# Deep Security 20 Guide

## for Azure Marketplace

# Legal notices

Privacy Policy

Trend Micro, Inc. is committed to protecting your privacy. Please read the Trend Micro Privacy Policy available at www.trendmicro.com.

**Document Number:** APEM209014/200622

**Publication Date:** 2/4/2026 4:47 PM

# Contents

# About Deep Security

## Deep Security 20 release strategy and lifecycle policy

Deep Security 20 is a long-term support (LTS) release. Its release management and lifecycle changes are designed to be more straighforward:

- Deep Security 20 updates include both new features and fixes.
- Feature releases (FR) are no longer available.

Even though Deep Security Manager supports older versions of Deep Security Agent, you should still upgrade agents when possible. New agent releases provide more security and protection, higher quality, performance improvements, and updates to stay in sync with OS releases. Regular software upgrades also ensure that, if an agent fix is required, you can update once, as opposed to installing multiple updates along a supported upgrade path. Each agent has an end-of-life date. For details, see Deep Security Agent LTS lifecycle date and Deep Security Agent FR lifecycle dates.

## Supported upgrade paths

Deep Security supports upgrades from the last two major releases for all Deep Security components, as long as the release that is subject to upgrade is still within its support period. See the support periods for LTS releases or for FR releases to ensure that the version being upgraded is supported.

You can upgrade to Deep Security 20 from the following versions until they reach their end-of-support dates:

- Deep Security 11 (LTS)
- Deep Security 12 (LTS)
- Deep Security 12 (FR)

You can also update any currently supported Deep Security 20 release to a more recent update release of it. Rolling back to a previous release is not supported.

## Deep Security 20 update schedule

Similar to previous LTS releases, Deep Security 20 updates are released monthly. If needed (such as due to critical fixes or vulnerabilities), more frequent releases are provided.

Each component may be released independently. Agents for different platforms (Windows, Linux, Unix) may also be released separately. An update can include one or more components and platforms. Typically, the global release process is completed within one week after the release date, at which point the update becomes available through the Download Center.

If you require a fix for a currently supported software release, then Trend Micro releases an update that can be directly applied during the support period. For example, if you had Deep Security 20 Update 2 and have an issue, then when the latest update is released (for example, Deep Security 20 Update 10), you could update directly from Update 2 to Update 10.

## LTS release support duration and upgrade best practices

The oftware updates process should be well-defined, regularly scheduled, and, ideally, automated, so all components are updated regularly.

The following table summarizes the updates release timeframe, the support duration of the released component, and considerations that should be taken when determining your upgrade strategy.

Deep Security 20 LTS updates span multiple years, with support periods changing in 2023: before 2023, support was based on the update's release year; since 2023, support is based on the specific release date. For example, all Deep Security 20 LTS updates released:

- in 2020 have standard support until December 31, 2023 and extended support until December 31, 2024.
- in 2021 have standard support until December 31, 2024 and extended support until December 31, 2025.
- in 2022 have standard support until December 31, 2025 and extended support until December 31, 2026.
- on July 25, 2023 have standard support until July 24, 2026 and extended support until July 24, 2027.
- on March 20, 2024 have standard support until March 19, 2027 and extended support until March 19, 2028.

| Component | Updates released | Support | Upgrade considerations |
|---|---|---|---|
| Deep Security Manager | LTS updates are released monthly | Before 2023: Standard support until 3 years after the year of release. Extended support until 4 years after the year of release.<br>In 2023 and later:<br>Standard support until 3 years after the release date. Extended support until 4 years after the release date. | Plan to upgrade regularly so that you are always using a supported release, and can upgrade to the latest software with a single upgrade. |
| Deep Security Agent | LTS updates are released monthly | Before 2023: Standard support until 3 years after the year of release. Extended support until 4 years after the year of release.<br>In 2023 and later:<br>Standard | LTS agents support upgrades from the last two major releases (for example, Deep Security Agent 11.0 to Deep Security Agent 20 LTS) that are still within their support period. Plan to upgrade regularly so that you are always using a supported release and are able to upgrade to the latest software with a single upgrade. |

| Component | Updates released | Support | Upgrade considerations |
|---|---|---|---|
| | | support until 3 years after the release date. Extended support until 4 years after the release date. | |
| Deep Security Agent (platforms where an older release of the agent is the latest agent for that platform) | LTS updates are released monthly | Platform-specific | If platform support is only provided by an older release of Deep Security Agent (for example, Windows 2000 uses a 9.6 agent and Red Hat Enterprise Linux 5 uses a 10.0 agent), use the latest agent for that platform and upgrade as updates are released. For details on which agent versions are supported for each platform, see "Agent platform compatibility" on page 389. |
| Deep Security Relay | LTS updates are released monthly | Same as agent | Deep Security Relay is simply a Deep Security Agent that has relay functionality enabled. The upgrade recommendations and support policies for agents also apply to relays. |

## Azure Marketplace software releases

Azure Marketplace is updated with the Deep Security 20 GA software release and every Deep Security 20 Update.

## Support services

The following table provides details about the artifacts supported during the Deep Security 20 lifecycle. Extended support is provided to all customers at no additional cost.

| Support item | LTS - standard support | LTS - extended support | LTS - limited support | Delivery mechanism |
|---|---|---|---|---|
| New features[1] | ✓ | ✓ | | LTS update |
| Small enhancements (no change to core functionality)[1] | ✓ | ✓ | | LTS update |
| Linux kernel updates | ✓ | On request | | Linux Kernel Support Package (LKP) |
| General bug fixes[1] | ✓ | ✓ | | LTS update |
| Critical bug fixes (system crash or hang, or loss of major functionality) | ✓ | ✓ | | LTS update or hotfix |
| Critical and high vulnerability fixes | ✓ | ✓ | | LTS update or hotfix |
| Medium and low vulnerability fixes | ✓ | ✓ | | LTS update |
| Anti-Malware pattern updates | ✓ | ✓ | ✓ | iAU (Active Update) |
| Intrusion Prevention, Integrity Monitoring, and Log Inspection rule updates | ✓ | ✓ | ✓ | iAU (Active Update) |
| Support for agents and Deep Security Manager on new versions of supported operating systems | ✓ | ✓ | | LTS update |

**Footnotes:**

[1] Agent platforms that are not supported are not included. See "Agent platform compatibility" on page 389.

# Agent platform support policy

Trend Micro recognizes that sometimes you must commit to an OS for many years. The agent platform support policy is designed to provide predictable support for the platform's lifespan.

- Many platforms are supported. See "Agent platform compatibility" on page 389.
- Platforms are supported until at least the OS vendor's end-of-extended-support date. Trend Micro might extend support beyond this date. However, once an OS vendor no longer supports its platform, there is a risk that some technical issues might not be fixable without the support of the OS vendor. Should this happen, Trend Micro notifies you immediately, but it could result in loss of functionality.
- Trend Micro notifies you in advance if it needs to end support for a platform.
- After General Availability (GA) of software, Trend Micro not shorten its support lifecycle, except possibly if the OS vendor stops supporting the platform.
- Consider how long the agent version is supported. For example, agent 11.0, 12.0, and so on (LTS releases) have 3 years of standard support and 4 years of extended support. If you are planning to use an OS for longer than that, then you must be prepared to regularly upgrade the agent so that you are always using an agent version that is currently supported.
- A new version of the agent is usually released for all supported platforms. However, to support older platforms, sometimes a deployment must include a previous release of the agent, and therefore its end-of-support dates are adjusted accordingly.

  For example, the newest agent for Windows 2000 is Deep Security Agent 9.6, so Deep Security Manager 11.0 supports it, even though the rest of the deployment uses Deep Security Agent 11.0. Therefore in this context, the older agent uses the EOL dates for Deep Security 11.0, not Deep Security 9.6.

To obtain the latest performance and security updates from your OS vendor, Trend Micro strongly encourages you to upgrade to the latest OS version for which an agent is available.

# Deep Security life cycle dates

## Deep Security LTS lifecycle dates

Subscribe via RSS

Refer to Trend Micro's latest End-of-Life Notice for more information on milestone definitions and standard timelines.

Deep Security Manager supports the use of older agent versions (see "Agent platform compatibility" on page 389), but Trend Micro encourages you to upgrade agents regularly. New agent releases provide additional security features and protection, better quality, performance improvements, and updates to stay in sync with releases from each platform vendor.

For more information, see "Deep Security 20 release strategy and lifecycle policy" on page 101. For information on feature releases, see "Deep Security FR life cycle dates" on page 114.

Products for the Japan region are handled under a region-specific policy. For more information, see End-of-Life Trend Micro Products and Versions.

### Deep Security LTS release lifecycle dates

The following table provides the dates for each Deep Security long-term support (LTS) release. These dates define the lifecycle for all components (manager, agents, relays, security updates) within the release, with the exception of any items listed in "Support extensions" on page 109.

| Version | Component | Platform | GA date | End of standard support | End of extended support (EOL) |
|---|---|---|---|---|---|
| Deep Security 9.0 | All | All | 11-Feb-2013 | 31-Dec-2017 | Extended support was introduced in Deep Security 10.0. See the Trend Micro End-of-Life Notice for terms and definitions.<br>These versions have reached EOL. |
| Deep Security 9.5 | All | All | 13-Aug-2014 | 17-Aug-2018 | |
| Deep Security 9.6 | All | All | 12-Aug-2015 | 12-Aug-2019 | |

| Version | Component | Platform | GA date | End of standard support | End of extended support (EOL) |
|---|---|---|---|---|---|
| Deep Security 10.0 | All | All | 09-Mar-2017 | 09-Mar-2020 | 09-Mar-2021 |
| Deep Security 11.0 | All | All | 22-May-2018 | 23-May-2021 | 22-May-2022 |
| Deep Security 12.0 | All | All | 20-Jun-2019 | 20-Jun-2022 | 20-Jun-2023 |
| Deep Security 20 (GA and all updates released in 2020) | All | All | 2020 | 31-Dec-2023 | 31-Dec-2024 |
| Deep Security 20 (all updates released in 2021) | All | All | 2021 | 31-Dec-2024 | 31-Dec-2025 |
| Deep Security 20 (all updates released in 2022) | All | All | 2022 | 31-Dec-2025 | 31-Dec-2026 |
| Deep Security 20 (all updates released in 2023 and later) | All | All | 2023 and later | Precisely 3 years after the release date | Precisely 4 years after the release date |

## Deep Security Virtual Appliance release life cycle dates

The Deep Security Virtual Appliance will reach end of extended support (EOL) on 31-Dec-2027, or VMware's end of support date for NSX-4.X, whichever comes first.

## Support extensions

The following table defines specific extensions to the life cycle dates listed above.

| Platform | Component | Version | Updated end of life (EOL) | More information |
|---|---|---|---|---|
| Windows 2000 | Agent | Deep Security 9.6 | 31-Dec-2025 1 | Trend Micro Server and Endpoint Protection Agent Minimum Windows Version Requirements for Updated Binaries After Mid-February 2023<br>Deep Security Windows 2000 Platform Support Update<br>Updated guidance on how to use Trend Micro Deep Security to protect Windows 2003, Windows XP, and Windows 2000 based systems<br>Support will continue, as per "Agent platform support policy" on page 106 |
| Windows 2003 | Agent | Deep Security 10.0 | 31-Dec-2025 1 | Trend Micro Server and Endpoint Protection Agent Minimum Windows Version Requirements for Updated Binaries After Mid-February 2023<br>Deep Security Windows 2003 Platform Support Update. |

| Platform | Component | Version | Updated end of life (EOL) | More information |
|---|---|---|---|---|
| | | | | Updated guidance on how to use Trend Micro Deep Security to protect Windows 2003, Windows XP, and Windows 2000 based systems<br>Support will continue, as per "Agent platform support policy" on page 106 |
| Windows XP | Agent | Deep Security 10.0 Update 25 or earlier | 30-Jul-2024 | Trend Micro Server and Endpoint Protection Agent Minimum Windows Version Requirements for Updated Binaries After Mid-February 2023<br>Updated guidance on how to use Trend Micro Deep Security to protect Windows 2003, Windows XP, and Windows 2000 based systems<br>Support will continue, as per "Agent platform support policy" on page 106 |
| Windows 7 | Agent | Deep Security 20.0.0 | 31-Dec-2026 | Starting in 2024, limited support will be provided, as per Platform support updates for Deep Security Agent version revision in January 2024 Update Release |
| Windows 2008 | Agent | Deep Security 20.0.0 | 31-Dec-2026 | Starting in 2024, limited support will be provided and conditional fixes will be available, as per |

| Platform | Component | Version | Updated end of life (EOL) | More information |
|---|---|---|---|---|
| | | | | Platform support updates for Deep Security Agent version revision in January 2024 Update Release |
| Windows 8.1 | Agent | Deep Security 20.0.0 | 31-Dec-2026 | Starting in 2024, limited support will be provided, as per Platform support updates for Deep Security Agent version revision in January 2024 Update Release |
| CloudLinux 5 (32- and 64-bit) | Agent | Deep Security 9.6 | 31-Dec-2025 1 | Support will continue, as per "Agent platform support policy" on page 106 |
| Cloud Linux 6 (32-bit) | Agent | Deep Security 10.0 | 31-Dec-2025 1 | Support will continue, as per "Agent platform support policy" on page 106 |
| Cloud Linux 6 (64-bit) | Agent | Deep Security 11.0 | 31-Dec-2025 1 | Support will continue, as per "Agent platform support policy" on page 106 |
| Debian 6 | Agent | Deep Security 9.6 | 31-Dec-2025 1 | Support will continue, as per "Agent platform support policy" on page 106 |
| Debian 7 | Agent | Deep Security 12.0 | 31-Dec-2025 1 | Support will continue, as per "Agent platform support policy" on page 106 |
| Debian 8 | Agent | Deep Security 20.0.0 | 31-Dec-2026 | Starting in 2024, limited support will be provided, as per Platform support updates for Deep Security Agent version revision in January 2024 Update Release |
| Oracle Linux 5 | Agent | Deep | 31-Dec- | Support will continue, as per |

| Platform | Component | Version | Updated end of life (EOL) | More information |
|---|---|---|---|---|
| | | Security 10.0 | 2025 [1] | "Agent platform support policy" on page 106 |
| Red Hat Enterprise Linux 5 | Agent | Deep Security 10.0 | 31-Dec-2025 [1] | Support will continue, as per "Agent platform support policy" on page 106 |
| SUSE Linux Enterprise Server 11 | Agent | Deep Security 12.0 | 31-Dec-2025 [1] | Support will continue, as per "Agent platform support policy" on page 106 |
| Ubuntu 10, 12 | Agent | Deep Security 9.6 | 31-Dec-2025 [1] | Support will continue, as per "Agent platform support policy" on page 106 |
| Ubuntu 14 | Agent | Deep Security 10.0 | 31-Dec-2025 [1] | Support will continue, as per "Agent platform support policy" on page 106 |
| CentOS 5 | Agent | Deep Security 10.0 | 31-Dec-2025 [1] | Support will continue, as per "Agent platform support policy" on page 106 |
| AIX 6.1 | Agent | Deep Security 20.0.0 | 31-Dec-2026 | Starting in 2024, limited support will be provided, as per Platform support updates for Deep Security Agent version revision in January 2024 Update Release |

**Footnotes:**

[1] This platform is currently supported using an older version of Deep Security Agent. Support for this platform will not be extended past this date. See also "Agent platform support policy" on page 106. For legacy OS support in the Japan region, see End-of-Life Trend Micro Products and Versions.

## Archive of past support extensions

| Platform | Component | Version | Updated end of life (EOL) | More information |
|---|---|---|---|---|
| All | Appliance | Deep Security 9.5 | 12-Aug-2019 | The Deep Security Virtual Appliance 9.5 embedded agent must be upgraded to version 9.6 to adopt this EOL date. If you do not do this, then an EOL date of **August 17, 2018** applies. Upgrading the embedded agent beyond version 9.6 will not extend the EOL date. |
| Windows 2000 | Agent | Deep Security 8.0 | 12-Aug-2019 | Deep Security Windows 2000 Platform Support Update<br>Updated the guidance on how to use Trend Micro Deep Security to protect Windows 2003, Windows XP, and Windows 2000 based systems |
| Solaris | Agent | Deep Security 9.0 | 31-Dec-2019 | |
| HP-UX | Agent | Deep Security 9.0 | 09-Mar-2020 | Only supported for use with Deep Security Manager 10.0. Support for HP-UX platform with Deep Security |
| AIX | Agent | Deep Security 9.0 | 31-Dec-2020 | |
| Windows XP Embedded | Agent | Deep Security 9.6 | 9-Mar-2021 | |
| SUSE Linux Enterprise Server 10 | Agent | Deep Security 9.6 | 23-May-2021 | Deep Security SuSE Enterprise Linux 10 Platform Support Update |

| Platform | Component | Version | Updated end of life (EOL) | More information |
|---|---|---|---|---|
| SP3, SP4 (32-bit and 64-bit) | | | | |

# Deep Security FR life cycle dates

Subscribe via RSS

Please refer to Trend Micro’s latest End-of-Life Policy for more information on milestone definitions and standard timelines.

**Note:** To reduce the number of software releases and simplify understanding of the support policy, Trend Micro is no longer releasing Feature Releases (FR) after the release of Deep Security 20. See "Deep Security 20 release strategy and lifecycle policy" on page 101.

Products for the Japan region are handled under a region-specific policy. For more information, see End-of-Life Trend Micro Products and Versions.

## Deep Security FR release life cycle dates

The following table presents the dates for each Deep Security feature release (FR). These dates define the life cycle for all components (manager, agents, relays, security updates) within the release, with the exception of any items listed in "Support extensions" on page 116.

| Version | Component | Platform | Build number | GA date | End of support |
|---|---|---|---|---|---|
| Deep Security 10.1 | All | All | 10.1.* | 11-Jul-2017 | 22-Nov-2018 |
| Deep Security 10.2 | All | All | 10.2.* | 24-Nov-2017 | 22-Nov-2018 |
| Deep Security 10.3 | All | All | 10.3.* | 18-Jan-2018 | 22-Nov-2018 |

| Version | Component | Platform | Build number | GA date | End of support |
|---|---|---|---|---|---|
| Deep Security 11.1 | All | All | 11.1.* | 16-Jul-2018 | 20-Dec-2019 |
| Deep Security 11.2 | All | All | 11.2.* | 10-Oct-2018 | 20-Dec-2019 |
| Deep Security 11.3 | All | All | 11.3.* | 07-Jan-2019 | 20-Dec-2019 |
| Deep Security 12 FR 2019-10-23 | Manager | All | 12.5.349 | 23-Oct-2019 | 23-Apr-2021 |
| Deep Security 12 FR 2019-12-12 | Manager | All | 12.5.494 | 12-Dec-2019 | 12-Jun-2021 |
| Deep Security 12 FR 2020-01-27 | Manager | All | 12.5.613 | 27-Jan-2020 | 27-Jul-2021 |
| Deep Security 12 FR 2020-03-09 | Agent | Windows | 12.5.0-713 | 09-Mar-2020 | 09-Sep-2021 |
| Deep Security 12 FR 2020-03-09 | Manager | All | 12.5.732 | 09-Mar-2020 | 09-Sep-2021 |
| Deep Security 12 FR 2020-04-02 | Agent | Linux | 12.5.0-814 | 02-Apr-2020 | 02-Oct-2021 |
| Deep Security 12 FR 2020-04-16 | Agent | Windows | 12.5.0-834 | 16-Apr-2020 | 16-Oct-2021 |
| Deep Security 12 FR 2020-04-29 | Manager | All | 12.5.855 | 29-Apr-2020 | 29-Oct-2021 |
| Deep Security 12 FR 2020-05-19 | Agent | Linux | 12.5.0-936 | 19-May-2020 | 19-Nov-2021 |
| Deep Security 12 FR 2020-06-17 | Manager | All | 12.5.985 | 17-Jun-2020 | 17-Dec-2021 |
| Deep Security 12 FR 2020-06-17 | Agent | All | 12.5.0-1033 | 17-Jun-2020 | 17-Dec-2021 |

## Support extensions

The following table defines specific extensions to the life cycle dates listed above.

| Version | Component | Platform | Updated end of life | More information |
|---|---|---|---|---|
| Deep Security 10.1, 10.2, 10.3 | Deep Security Agent Linux Kernel Updates | Linux | 22-Nov-2019 | Extending Linux kernel updates for Deep Security 10.x feature release agents |
| Deep Security 11.1, 11.2, 11.3 | Deep Security Agent Linux Kernel Updates | Linux | 31-Dec-2020 | Importing the kernel version package for Deep Security Agent operating system |

# About the Deep Security components

Trend Micro Deep Security provides advanced server security for physical, virtual, and cloud servers. It protects enterprise applications and data from breaches and business disruptions without requiring emergency patching. This comprehensive, centrally managed platform helps you simplify security operations while enabling regulatory compliance and accelerating the ROI of virtualization and cloud projects.

For information on the protection modules that are available for Deep Security, see "About the Deep Security protection modules" on the next page.

Deep Security consists of the following set of components that work together to provide protection:

- **Deep Security Manager**, the centralized web-based management console that administrators use to configure security policy and deploy protection to the enforcement components: the Deep Security Virtual Appliance and the Deep Security Agent.
- **Deep Security Virtual Appliance** is a security virtual machine built for VMware vSphere environments that agentlessly provides anti-malware and integrity monitoring protection modules for virtual machines in a vShield environment. In an NSX environment, the anti-malware, integrity monitoring, firewall, intrusion prevention, and web reputation modules are available agentlessly.

- **Deep Security Agent** is a security agent deployed directly on a computer which provides application control, anti-malware, web reputation service, firewall, intrusion prevention, integrity monitoring, and log inspection protection to computers on which it is installed.
- The Deep Security Agent contains a **Relay** module. A relay-enabled agent distributes software and security updates throughout your network of Deep Security components.
- **Deep Security Notifier** is a Windows taskbar application that communicates information on the local computer about security status and events, and, in the case of relay-enabled agents, also provides information about the security updates being distributed from the local machine.

# About the Deep Security protection modules

Trend Micro Deep Security has tightly integrated modules that easily expand your security capabilities:

- "Intrusion Prevention " below
- "Anti-Malware " on the next page
- "Firewall " on the next page
- "Web Reputation " on the next page
- "Integrity Monitoring " on the next page
- "Log Inspection " on page 119
- "Application Control" on page 119
- "Device Control" on page 119

## Intrusion Prevention

The Intrusion Prevention module inspects incoming and outgoing traffic to detect and block suspicious activity. This prevents exploitation of known and zero-day vulnerabilities. Deep Security supports "virtual patching": you can use Intrusion Prevention rules to shield from known vulnerabilities until they can be patched, which is required by many compliance regulations. You can configure Deep Security to automatically receive new rules that shield newly discovered vulnerabilities within hours of their discovery.

The Intrusion Prevention module also protects your web applications and the data that they process from SQL injection attacks, cross-site scripting attacks, and other web application vulnerabilities until code fixes can be completed.

For more information, see "Set up Intrusion Prevention" on page 804.

## Anti-Malware

The Anti-Malware module protects your Windows and Linux workloads against malicious software, such as malware, spyware, and Trojans. Powered by the Trend Micro™ Smart Protection Network™, the Anti-Malware module helps you instantly identify and remove malware and block domains known to be command and control servers.

For more information, see "Enable and configure Anti-Malware" on page 742.

## Firewall

The Firewall module is for controlling incoming and outgoing traffic and it also maintains firewall event logs for audits.

For more information, see "Set up the Deep Security firewall" on page 851.

## Web Reputation

The majority of today’s attacks start with a visit to a URL that’s carrying a malicious payload. The Web Reputation module provides content filtering by blocking access to malicious domains and known communication and control (C&C) servers used by criminals. The Web Reputation module taps into the Trend Micro Smart Protection Network, which identifies new threats quickly and accurately.

For more information, see "Configure Web Reputation" on page 794.

## Integrity Monitoring

The Integrity Monitoring module provides the ability to track both authorized and unauthorized changes made to an instance and enables you to receive alerts about unplanned or malicious changes. The ability to detect unauthorized changes is a critical component in your cloud security strategy because it provides visibility into changes that could indicate the compromise of an instance.

For more information, see "Set up Integrity Monitoring" on page 901.

## Log Inspection

The Log Inspection module captures and analyzes system logs to provide audit evidence for PCI DSS or internal requirements that your organization may have. It helps you to identify important security events that may be buried in multiple log entries. You can configure Log Inspection to forward suspicious events to an SIEM system or centralized logging server for correlation, reporting, and archiving (see "Forward Deep Security events to a Syslog or SIEM server" on page 1067).

For more information, see "Set up Log Inspection" on page 960.

## Application Control

The Application Control module monitors changes - "drift" or "delta" - compared to the computer’s original software. Once application control is enabled, all software changes are logged and events are created when it detects new or changed software on the file system. When Deep Security Agent detects changes, you can allow or block the software, and optionally lock down the computer.

For more information, see "Verify that Application Control is enabled" on page 1003.

## Device Control

The Device Control module regulates access to external storage devices connected to computers. Device Control helps prevent data loss and leakage and, combined with file scanning, helps guard against security risks.

For more information, see "Configure Device Control" on page 898.

# About this release

## What's new?

LTS releases of Deep Security are made available on an annual basis and include new functionality, enhancements for existing functionality, and bug fixes. LTS releases include long-term support, as described in "LTS release support duration and upgrade best practices" on page 102. Once an LTS release is made generally available, updates to LTS releases are restricted to only fixes and small enhancements.

With Deep Security 20, each component (manager, agent, appliance) can be released independently. Agents for different platforms (Windows, Linux, Unix) can also be released separately. An update may include one or more components and platforms.

Read:

- "What's new in Deep Security Manager?" below
- "What's new in Deep Security Agent?" on page 187

# What's new in Deep Security Manager?

## Deep Security Manager - 20.0.1138 (20 LTS Update 2026-01-28)

Release date: January 28, 2026

Build number: 20.0.1138

### New Features

**Support for SUSE Linux Enterprise Server 16**: Deep Security Manager now supports SUSE Linux Enterprise Server 16. DSA-13934

**Support for PostgreSQL 17**: Deep Security Manager now supports PostgreSQL 17. DSM-937

Support for Manager Instance Role (IAM Role) authentication for Amazon SNS event forwarding. DSM-1473

Support for OAuth 2.0 authentication for Microsoft Exchange Online SMTP. This adds a new authentication mode configured through **Administration > System Settings**. When enabled, Deep Security Manager securely manages token acquisition and refreshing via the Client Credentials Flow, replacing the deprecated basic authentication method. DSM-1415/DSM-1409

Support for inherited scan exception list. DSM-1001

### Enhancements

- Deep Security Manager copyright date is now set to year 2026. DSM-928

### Resolved issues

- Deep Security Manager nodes automatically shut down for an indefinite period of time due to the system time synchronization issues between nodes. PCT-85360/PCT-8942/DSM-1519

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. DSM-1546/DSM-1545

Highest Common Vulnerability Scoring System (CVSS) score: 7.5

Highest severity: High

## Deep Security Manager - 20.0.1123 (20 LTS Update 2025-12-09)

Release date: December 9, 2025

Build number: 20.0.1123

### New Features

**Support for Ubuntu Linux 24 with ARM architecture**: Deep Security Manager now supports Ubuntu Linux 24 with ARM architecture. DSA-12857

### Enhancements

- Deep Security Manager now supports file hash (MD5, SHA1, SHA256) in Spyware events. DSM-1429/DSA-13232

### Resolved issues

- System events could not always be exported to a CSV file with full description. This included certain 2205 events. PCT-77413/DSM-1465
- Users with expired passwords were not prompted to change their password upon the next login. PCT-77392/DSM-1395

## Deep Security Manager - 20.0.1112 (20 LTS Update 2025-11-12)

Release date: November 12, 2025

Build number: 20.0.1112

### New Features

**Support for Windows Server 2025**: Deep Security Manager now supports Windows Server 2025. DSM-929

**Support for Windows 11, version 25H2**: Deep Security Manager now supports Windows 11, version 25H2. DSA-12978/DSA-12967

**Support for Rocky Linux 10**: Deep Security Manager now supports Rocky Linux 10. DSA-12906/DSA-12903

### Enhancements

- The user is logged out when the password is changed. DSM-1344
- Any suspicious proxy user name is detected by the deployment script. DSM-1336
- The `activationCodes` field is not included in the `Describe a Tenant` API response. PCT-69880/DSM-1261

## Deep Security Manager - 20.0.1092 (20 LTS Update 2025-10-08)

Release date: October 8, 2025

Build number: 20.0.1092

### New Features

**Support for Red Hat Enterprise Linux 10**: Deep Security Manager now supports Red Hat Enterprise Linux 10. DSM-1335

### Resolved issues

- The AWS single-click upgrade banner was stuck in the "In progress" status. PCT-77674/DSM-1388

## Deep Security Manager - 20.0.1081 (20 LTS Update 2025-09-15)

Release date: September 15, 2025

Build number: 20.0.1081

### New Features

**Integration with Cisco Identity Services Engine (ISE)**: Deep Security Manager is now integrated with Cisco ISE for rapid threat containment. DSM-1000

### Enhancements

- The Deep Security Agent activation is now blocked if its system clock drifts forward more than the allowed threshold. PCT-54410/DSM-1006
- **Enable Census query** and **Enable Good file reputation query** settings were added to **Computer > Settings > General > Networking Setting for Census, Good File Reputation, and Predictive machine Learning Service**. PCT-36275/DSM-1201

### Resolved issues

- Some third-party Oracle Linux instances from the AWS Marketplace were not detected as a known platform by the AWS connector instance metadata. DSM-1284
- The Workload Security migration was failing due to the `VARCHAR(2000)` limit exceeded. PCT-62228/DSM-1112/DSM-1357
- In the SAML configuration, an unexpected incorrect input value replaced the original input value after the **Back** button had been clicked. DSM-1093/DSM-975

## Deep Security Manager - 20.0.1073 (20 LTS Update 2025-08-20)

Release date: August 20, 2025

Build number: 20.0.1073

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. DSM-1241

Highest Common Vulnerability Scoring System (CVSS) score: 8.8

Highest severity: High

## Deep Security Manager - 20.0.1059 (20 LTS Update 2025-07-09)

Release date: July 9, 2025

Build number: 20.0.1059

### Enhancements

- A new region AE-1 for UAE was added to the Deep Security Manager migration tool (**Support > Upgrade to Trend Vision One Endpoint Security**). DSM-1041

### Resolved issues

- The calendar in the **Smart Folder Editor** displayed the days of the week in the wrong order. DSM-1214

## Deep Security Manager - 20.0.1054 (20 LTS Update 2025-06-11)

Release date: June 11, 2025

Build number: 20.0.1054

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. DSM-975/DSM-923

Highest Common Vulnerability Scoring System (CVSS) score: 6.1

Highest severity: Medium

## Deep Security Manager - 20.0.1047 (20 LTS Update 2025-05-12)

Release date: May 12, 2025

Build number: 20.0.1047

### Enhancements

- Support for duplicate host merging during the Active Directory connector synchronization. PCT-51213/DSM-968
- Support for collecting syslog-related information via the Syslog Issues option on the Diagnostic Logging Wizard. DSM-902
- For Linux driverless mode, the Anti-Malware module status is now displayed instead of a warning. DSM-884

## Deep Security Manager - 20.0.1039 (20 LTS Update 2025-04-16)

Release date: April 16, 2025

Build number: 20.0.1039

### New Features

**VMware Cloud Director 10.6 support**: Deep Security Manager now supports VMware Cloud Director version 10.6. DSA-921

### Resolved issues

- Systems incorrectly used the `sts.cn-north-1.amazonaws.com` endpoint instead of the required China-specific endpoint `sts.cn-north-1.amazonaws.com.cn` when connecting to AWS China regions. PCT-55611/DSM-1042
- A new rule created for Integrity Monitoring, Log Inspection, Intrusion Prevention, or Firewall was logged as a rule update. PCT-53113/DSM-996
- Already applied Deep Security Rule Updates (DSRU) were deleted when purging spare DSRU. PCT-46867/DSM-918
- When a performance profile was switched to the one with a reduced thread pool size, a misleading error message was displayed. DSM-839/DSM-837
- The sending policy job count was incorrectly displayed on the taskbar. PCT-6652/DSM-347/WS-11383

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. VRTS-13713/DSM-912/WS-13713

Highest Common Vulnerability Scoring System (CVSS) score: 2.7

Highest severity: Low

## Deep Security Manager - 20.0.1027 (20 LTS Update 2025-03-12)

Release date: March 12, 2025

Build number: 20.0.1027

### Enhancements

- The Tomcat server version was updated in Deep Security Manager. VRTS-13896/DSM-955/DSM-947

### Resolved issues

- Migration of Deep Security Agents to Trend Vision One - Server & Workload Protection failed due to the incorrect public CA used during the migration. DSM-995/DSM-1023/WS-10344

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. DSM-885/DSM-632

Highest Common Vulnerability Scoring System (CVSS) score: 5.3

Highest severity: Medium

## Deep Security Manager - 20.0.1017 (20 LTS Update 2025-01-15)

Release date: January 15, 2025

Build number: 20.0.1017

### New Features

**Windows Server 2025 support**: Deep Security Agent now supports Windows Server 2025, including FIPS mode. DSA-7953

**Multi-tenancy support with enabled FIPS mode**: Deep Security Manager now supports multi-tenancy when Federal Information Processing Standard (FIPS) mode is enabled. DSM-846

### Enhancements

- The Deep Security Manager copyright information was updated to year 2025. DSM-412
- For newly-installed Deep Security Manager, the default baseline information is now stored in Deep Security Agent. For details, see Database performance issue due to lots of Integrity Monitoring baseline data. PCT-28475/PCT-19324/DSM-651
- Updated legacy descriptions for **Administration > System Settings > Proxies**. DSM-758/DSM-749
- The `EntityType` field was added to the Integrity Monitoring syslog message. PCT-39385/PCT-47161/DSM-911
- The procedure of testing AWS Security Token Service (STS) endpoint was improved to avoid issues with restricted Firewall rules. PCT-42974/DSM-942
- The Tomcat server version was updated in Deep Security Manager. VRTS-13877/VRTS-13889/DSM-947/DSM-914

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. DSM-812/DSM-809

Highest Common Vulnerability Scoring System (CVSS) score: 5.5

Highest severity: Medium

## Deep Security Manager - 20.0.1003 (20 LTS Update 2024-12-10)

Release date: December 10, 2024

Build number: 20.0.1003

### Enhancements

- CPU usage for real-time Anti-Malware can now be configured on Linux using the Deep Security Manager console. The options are unlimited, low, and extremely low CPU usage. DSM-881
- Unused system events no longer appear in the Deep Security Manager console (**Administration > System Settings > System Events**). PCT-3185/PCT-26855/PCT-34591/SEG-179061/DSM-279

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. DSM-874/DSM-886

Highest Common Vulnerability Scoring System (CVSS) score: 8.5

Highest severity: High

## Deep Security Manager - 20.0.993 (20 LTS Update 2024-11-13)

Release date: November 13, 2024

Build number: 20.0.993

### New Features

**Application Control support on Windows 10 and Windows 11**: Deep Security Manager 20.0.993 or later now supports Application Control on Windows 10 and Windows 11. DSM-819

### Enhancements

- Reduction in the recommendation scan elapsed time and memory usage. PCT-42518/DSM-896
- Custom input field to make troubleshooting more efficient. DSM-796
- Improved error message on the Trend Vision One Enrollment Token dialog. This message is displayed when the user enters an invalid token. DSM-731
- Recommendation scan does not run when the security module is disabled. PCT-11993/PCT-36524/DSM-464

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. DSM-879

Highest Common Vulnerability Scoring System (CVSS) score: 5.9

Highest severity: Medium

## Deep Security Manager - 20.0.979 (20 LTS Update 2024-10-16)

Release date: October 16, 2024

Build number: 20.0.979

### New Features

**Red Hat Enterprise 9 (PowerPC little-endian) support**: Deep Security Manager 20.0.979 or later now supports Red Hat Enterprise 9 (PowerPC little-endian).

### Enhancements

- Deep Security Manager now supports SAML single sign-on (SSO) when FIPS mode is enabled. PCT-17482/DSM-428

### Resolved issues

- If using a vCenter connector without NSX-v/T deployed, the Deep Security Manager logs would fail to record when Deep Security Manager checked for Deep Security Virtual Appliance versions. DSM-822

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. DSM-754

Highest Common Vulnerability Scoring System (CVSS) score: 5.3

Highest severity: Low

## Deep Security Manager - 20.0.967 (20 LTS Update 2024-09-18)

Release date: September 18, 2024

Build number: 20.0.967

### Enhancements

- Deep Security Manager performance profiles now have a new Higher Capacity option. PCT-1686/PCT-5853/PCT-6181/PCT-7244/PCT-15098/PCT-16008/PCT-18026/DSM-525
- The SAP Scanner status now provides more information and was moved next to the status of the other protection modules. DSM-572
- Improved some error messages to be more informative. DSM-788

### Resolved issues

- AWS connectors were missing the AWS GovCloud region as an option in Deep Security Manager 20.0.904 which would cause synchronization issues. PCT-26434/PCT-29880/PCT-30450/DSM-626
- The Support button link in the Deep Security Manager VM for Azure Marketplace console led to a 404 Page Not Found error. The Support button now links to Trend Bussiness Success Portal - Deep Security. DSM-801

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. DSM-735/DSM-741

Highest Common Vulnerability Scoring System (CVSS) score: 5.8

Highest severity: Low

## Deep Security Manager - 20.0.954 (20 LTS Update 2024-08-21)

Release date: August 21, 2024

Build number: 20.0.954

### New Features

**User mode solution**: User mode can now be enabled from the Deep Security Manager UI to provide event generation and protection through basic functions for Anti-Malware on systems that lack kernel support.

### Enhancements

- The path property for Application Control Trust Entities rules can now use wildcards in a Universal Naming Convention (UNC) path without requiring a drive letter. SF06976162/SEG-189907/WS-4290
- In the Deep Security Manager console for AWS and Azure marketplace, the **Contact Support** button (**Support > Contact Support**), which linked to the retired legacy support system, has been removed. To create a support case, please visit https://success.trendmicro.com/en-US/product/?name=deep-security. DSM-769
- The Application Control Software Changes page (**Actions**) now includes software change attributes or signer information for Signer Name, Issuer Common Name, Issuer Organizational Unit, Issuer Organization, Issuer Locality, Vendor, Product Name, Process Name, Install Path, and File Path. DSM-662
- Service Gateway can now be configured (from **Administration > System Settings > Proxies > Proxy Server Use**) as a proxy for Deep Security Manager (Software Updates, CSSS, News Updates, Product Registration and Licensing). DSM-518

### Resolved issues

- Updating Deep Security Agent sometimes caused Application Control software change events. SF07441007/PCT-9653/PCT-16914/WS-6246
- Application Control events generated by Trust Entities would display "None" in the RULESET column (**Events & Reports > Application Control Events**) even if they were associated with a ruleset. DSM-779
- The Kernel Support Package (KSP) was unexpectedly deleted on some systems. SF08057187/PCT-30396/PCT-36420/DSM-718

## Deep Security Manager - 20.0.940 (20 LTS Update 2024-07-17)

Release date: July 17, 2024

Build number: 20.0.940

### New Features

**Trend Vision One integration enhancement**: Intrusion Prevention System rules applied in Deep Security Manager can now be sent to Trend Vision One - Server & Workload Protection.

**Trend Vision One migration tool**: A tool is now available to help migrate from Deep Security Manager to Trend Vision One Endpoint Security - Server & Workload Protection.

### Enhancements

- Deep Security Manager now supports PostgreSQL 15 & 16, AWS Aurora PostgreSQL 15 & 16, and AWS RDS PostgreSQL 15 & 16. PCT-5186/PCT-32769/DSM-144

### Resolved issues

- Using Remote Desktop Protocol failed on some Windows Server 2022 systems. DSM-695
- Migrating on-premise policies or Deep Security Agents to Trend Vision One Endpoint Security using the migration tool resulted an `Invalid 'expires' attribute` entry in the `server0.log` file. This did not impact migration. DSM-657

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. VRTS-11981/DSM-517

Highest Common Vulnerability Scoring System (CVSS) score: 9.8

Highest severity: Critical

## Deep Security Manager - 20.0.926 (20 LTS Update 2024-06-19

Release date: June 19, 2024

Build number: 20.0.926

### Enhancements

- Custom actions can now be configured for Process Memory Scan. Process Memory Scan applies to real-time, on-demand and manual scans. This requires Deep Security Agent version 20.0.1-12510 or later. DSM-539/DSM-656

- The event level for agent events **1005: Upgrading Driver** and **1007: Driver Upgrade Succeeded** was changed from Warning to Info. DSM-440

### Resolved issues

- Deep Security Virtual Appliances would sometimes not show as upgradable, despite seeing **agent upgrade recommended** alerts for them in the management console. PCT-23179/PCT-27324/DSM-589
- When applying a new DSRU version, then rolling it back without restarting the DSM service, recommendation scan would incorrectly continue to use the new version. DSM-577

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. VRTS-11810/VRTS-12278/DSM-483/DSM-568

Highest Common Vulnerability Scoring System (CVSS) score: 7

Highest severity: High

## Deep Security Manager - 20.0.913 (20 LTS Update 2024-05-15)

Release date: May 15, 2024

Build number: 20.0.913

### Enhancements

- Advanced TLS Traffic Inspection configuration now has separate settings for inspecting inbound and outbound traffic. DSM-190
  **Note:** Enabling outbound traffic inspection requires additional configuration steps on the agent side.
- Deep Security Manager now supports configuring a Service Gateway proxy from the Trend Cloud One - Endpoint & Workload Security migration wizard. Using a Service Gateway proxy is only supported when all deployed Deep Security Agents are version 20.0.1-3180 or later. PCT-12854/DSM-367

- The "hostName" field now shows the device hostname when retrieving Service Gateway proxy information using the ProxyAPI. A new "ips" field is added to provide the device IP address information. DSM-533

### Resolved issues

- When a proxy was configured in policy, creating a new tenant template would cause Internal Server errors. Proxy settings were removed from policies when creating a new tenant template. PCT-4709/DSM-306
- Trend Vision One returned a HTTP 400 error when Deep Security Manager sent a request to update the certificate. DSM-593

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. VRTS-12054/PCT-25774/DSM-161/DSM-519

Highest Common Vulnerability Scoring System (CVSS) score: 7.5

Highest severity: High

## Deep Security Manager - 20.0.904 (20 LTS Update 2024-04-17)

Release date: April 17, 2024

Build number: 20.0.904

### New Features

**Cross-account AWS role registration**: Seed region and Security Token Service (STS) endpoint selection can now be done using the AWS connector wizard and AWS account properties page in Deep Security Manager.

### Enhancements

- Deep Security Manager now supports Oracle Database 23c. DSM-366
- Changed the Migration API default timeout for Cloud One Endpoint & Workload Security to 60 seconds. The previous default was 10 seconds, which sometimes led to timeout before

agents were transferred from Deep Security Manager. The timeout can be set between 10 and 1200 seconds (20 minutes) using the `settings.configuration.defaultWorkloadSecurityMigrationApiTimeout`. PCT-21902/PCT-22361/PCT-22860/PCT-22249/DSM-579
- Updated third-party licenses for Deep Security Manager. DSM-564
- Improved Azure connector performance for some system configurations. DSM-472

### Resolved issues

- Changes to the Deep Security Virtual Appliance OVF file's IP address (**Computer > Properties > NSX Configuration > General**) sometimes failed to be applied. PCT-20529/PCT-23331/DSM-545
- The public IP and network security group were not being displayed in the virtual machine summary for some Azure VM configurations. DSM-459
- Database connection issues sometimes caused Deep Security Manager to delete in-use Deep Security Agent installers. SEG-188888/PCT-7221/PCT-15200/DSM-348
- Deep Security Manager's console displayed Windows 10 Enterprise multi-session as "Windows Server 2019" when it should have displayed the platform as "Windows 10." SEG-131712/DS-69474/DSM-326

## Deep Security Manager - 20.0.893 (20 LTS Update 2024-03-20)

Release date: March 20, 2024

Build number: 20.0.893

### Enhancements

- Anti-Malware Manual Scan can now be configured from a policy on Deep Security Manager for Linux platforms. DSM-433

### Resolved issues

- Event Forwarding conditions `StringLike` and `StringNotLike` did not work for JSON formatted on multiple lines for a `Description`. SF07518120/PCT-12618/DSM-448
- Deep Security Manager sometimes displayed a Trend Micro Adversary Tactics and Techniques Detection pattern version (**Administration > Updates > Security > Patterns**) before it was available from the Trend Micro Update Server. DSM-439

## Deep Security Manager - 20.0.883 (20 LTS Update 2024-02-21)

Release date: February 21, 2024

Build number: 20.0.883

### New Features

- Deep Security Manager now supports dynamic updates of the XDR Device ID of the Trend Micro Endpoint Basecamp. DSM-250

### Enhancements

- The Web Reputation Service backend query now uses port 443 by default for new installations and new tenants. PCT-10486/DSM-445
- In the Anti-Malware configuration, the default values for Predictive Machine Learning and Windows Antimalware Scan Interface (AMSI) settings are now marked as recommended. PCT-3844/DSM-301

### Resolved issues

- Upgrading to Deep Security Agent 20.0.0-7943, 20.0.0-8137, 20.0.0-8268, or 20.0.0-8438 sometimes failed when Firewall, Web Reputation Service, or Intrusion Prevention System were enabled for Deep Security Manager. DSM-473

## Deep Security Manager - 20.0.879 (20 LTS Update 2024-01-17)

Release date: January 17, 2024

Build number: 20.0.879

### New Features

- Deep Security Manager now allows changing the IP address or fully qualified domain name (FQDN) for the NSX Manager. DSM-83/DSM-405

## Enhancements

- The Tomcat version was updated in Deep Security Manager. DSM-431/DSM-160
- A number of URLs on a verge of becoming invalid were updated on the Deep Security Manager Support website. DSM-352
- Deep Security Manager copyright information was updated to year 2024. DSM-133
- A dedicated banner is now displayed within Deep Security Manager to notify the users of Deep Security Virtual Appliance about the Deep Security Virtual Appliance EOL status. DS-76857/DSM-131
- Security updates for VRTS-10045, VRTS-10068, VRTS-10070. DSM-133
- Deep Security Manager copyright information was updated to year 2024. DSM-133
- Deep Security Manager can now force the removal of the service reference ID when the VMware vCenter connector is removed. This service reference ID is automatically created by VMware NSX-T to bind the Trend Micro service with the security profile. SEG-160298/DSM-49
- The out-of-date computer status is now representd by three separate statuses: **Out of Date (Anti-Malware Configuration Off)**, **Out of Date (Anti-Malware Offline)**, and **Out of Date (Agent Offline)**. This directly affects the functionality of the security pattern status widget, ensuring that the **Out-of-Date Advanced Search** results do not include Deep Security Agents with the statuses Agent Offline, Anti-Malware Configuration Off, and Anti-Malware Offline. DSM-135

## Resolved issues

- Azure Connector experienced synchronization issue for Azure Virtual Machine Scale Sets with Flexible orchestration mode. DSM-436
- Apex Central did not have the information and therefore could not forward it to syslog or display in its log view due to the MCP content not being updated to include the FileSHA1 of an infected file. SEG-192045/PCT-6042/DSM-435
- The value of the behaviorMonitoringEnabled property in the Antimalware Configuration API was missing, resulting in a disconnect between the UI and API. PCT-5360/DSM-411

## Known issues

- Upgrading to Deep Security Agent 20.0.0-7943, 20.0.0-8137, 20.0.0-8268, or 20.0.0-8438 sometimes fails when Firewall, Web Reputation Service, or Intrusion Prevention System are enabled for Deep Security Manager. DSM-473

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. DSM-402

Highest Common Vulnerability Scoring System (CVSS) score: 7.5

Highest severity: High

## Deep Security Manager - 20.0.864 (20 LTS Update 2023-12-12)

Release date: December 12, 2023

Build number: 20.0.864

### Enhancements

- Updated the Deep Security Manager UI to reflect Microsoft's product name change: Azure Active Directory is now Microsoft Entra ID. DSM-214
- Deep Security Manager reports (**Events & Reports > Generate Reports**) can now be generated using custom classifications by selecting **CUSTOM** from the classification list and filling in the name field. SF06301702/SEG-167348/DS-76507/DSM-8
- Deep Security Manager now limits Deep Security Virtual Appliance agent software upgrades to 20.0.0 versions. Note that 20.0.1 agent versions are not supported. DSM-311
- Upgrading Deep Security Agent for a limited support platform using the Use Latest Version for an Agent option (**Computers > Details > Action > Upgrade Agent Software**) now provides a warning that 20.0.1 agent versions are not supported for that platform. DSM-342/DSM-343/DSM-344

### Resolved issues

- After upgrading to Deep Security Manager 20.0.797, the Deep Security Component Summary widget display was blank in the Apex Central console. DSM-236
- Overrides for Application Control Trust Entities settings were not being removed after using **Remove** or **Remove All** (from **Computer** or **Policy > Overrides**). DSM-120

- SAP scans generated Get Events Failed errors when **Alert for all rules (Regardless of rule settings)** was enabled (**Alerts > Alert Configuration > Anti-Malware Alert > Alert Information > Options**). SF05087843/SEG-173393/DS-77098/DSM-28
- Deep Security Manager API searches using the `greater than` parameter sometimes returned incorrect results. DSM-325
- The **Schedule Agent Upgrade** screen sometimes displayed incorrect agent versions until Deep Security Manager was restarted. DSM-329

### Known issues

- Upgrading to Deep Security Agent 20.0.0-7943, 20.0.0-8137, 20.0.0-8268, or 20.0.0-8438 sometimes fails when Firewall, Web Reputation Service, or Intrusion Prevention System are enabled for Deep Security Manager. DSM-473

## Deep Security Manager - 20.0.854 (20 LTS Update 2023-11-15)

Release date: November 15, 2023

Build number: 20.0.854

### New Features

- Deep Security Manager now supports strong cipher suites when FIPS mode is enabled. DSM-211

### Enhancements

- Deep Security Manager now supports the 20.0.1 Deep Security Agent versioning revision planned for January 2024. DSM-121

### Resolved issues

- Using an Intrusion Prevention event containing a long note triggered an error with a message "Get Events Failed (Internal Server Error)". DSM-327
- The HostName lookup got stuck in some environments where the DNS setting was incomplete. DSM-307

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. VRTS-11238/DSM-290

Highest Common Vulnerability Scoring System (CVSS) score: 7.5

Highest severity: High

### Known issues

- Upgrading to Deep Security Agent 20.0.0-7943, 20.0.0-8137, 20.0.0-8268, or 20.0.0-8438 sometimes fails when Firewall, Web Reputation Service, or Intrusion Prevention System are enabled for Deep Security Manager. DSM-473

## Deep Security Manager - 20.0.844 (20 LTS Update 2023-10-18)

Release date: October 18, 2023

Build number: 20.0.844

### New Features

- Deep Security Manager now allows users to configure the agent Manual Scan from policy. DSM-16

### Enhancements

- In Events & Reports, the advanced search can now filter Intrusion Prevention events by "Flow" value.
  The "Flow" field is now added to Intrusion Prevention syslog events. SF06798790/SEG-177960/DS-77724/DSM-9
- Application Control global block by hash rules can now be configured using a MD5 or SHA-1 file hash. (Previously, only SHA-256 could be used.) SEG-108464/DS-74144/DSM-18
- Application Control Trust Entities rules that use the process name property can now be configured using wildcards in the Deep Security Manager UI. DS-75316/DSM-18
- Trust Entities process name properties can now use Universal Naming Convention (UNC) paths to files or peripheral devices on a local area network. DS-77133/DSM-18

- Trust Entities "Allow by target" rules can now use the process name property. DS-77364/DSM-18

## Resolved issues

- When configuring Role Properties, applying changes to the "Clear Warnings/Errors for" permission under the Computer Rights tab displayed the incorrect result in the console. DSM-195
- Application Control shared rulesets sometimes triggered policy updates to systems that did not support Application Control. DS-76766/DSM-18
- Software auto-authorized on agents by a Trust Entities rule are no longer automatically added to the shared rulesets. This will prevent software from remaining authorized if the corresponding trust entities rule is no longer applied. DS-74855/DSM-18

## Known issues

- Deep Security Notifier may fail to start when deployed as an Anti-Malware Protected Process Light (AM-PPL) in Windows. As a workaround, deploying the Notifier as an AM-PPL has been disabled by default. See Deep Security Notifier service is unable to start or stop. DSM-297

# Deep Security Manager - 20.0.833 (20 LTS Update 2023-09-20)

Release date: September 20, 2023

Build number: 20.0.833

## Enhancements

- The permission to clear warnings and errors "canClearWarningsAndErrors" can now be granted separately to roles. SF06516228/SEG-168657/DS-77463
- Changed the error message displayed when a user that doesn't have the necessary permissions tries to edit Device Control settings. SEG-180964/C1WS-14961/DSM-56
- Some default values for Real Time Anti-Malware configuration have changed: DS-77469/C1WS-13588/DSM-36
  - Predictive Machine Learning: Pass > **Quarantine**
  - Windows Antimalware Scan Interface (AMSI): Pass > **Terminate**

- When creating a Smart Folder, vCenter Power State is now a **Computer Property** option. DSM-6/DS-77643
- Smart Folder **Computer Property** options are now sorted in alphabetical order. DSM-6/DS-77643

### Resolved issues

- In the web console, AIX 7.3 agents did not display the OS version in the **Platform** field. DS-72424/DSM-128
- The **User Management > Roles > Role Properties** window did not load if a lot of computers were protected. SEG-170672/DS-76826/C1WS-12373/DSM-10
- The SHA256 hash value of files will now be included in SNS Anti-Malware events when SHA256 is selected in **Anti-Malware > Advanced > File Hash Calculation**. SEG-168652/DS-76448/C1WS-14048/DSM-7
- Deep Security Manager sometimes set a wrong date for Next Run Time while running the scheduled task, which lead to a Java DateTimeException and display of an internal server error. This could prevent the reservation task from working properly. SF07190612/SF07191522/SEG-192240/SEG-192321/DSM-169

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. VRTS-10326/DSM-158

Highest Common Vulnerability Scoring System (CVSS) score: 6.1

Highest severity: Medium

## Deep Security Manager - 20.0.817 (20 LTS Update 2023-08-23)

Release date: August 23, 2023

Build number: 20.0.817

### Enhancements

- The Deep Security Manager console now shows more information on the status of the Trend Micro LightWeight Filter Driver. DS-77465

- Add Device Control information to the Security Module Usage Report. DS-77319

## Deep Security Manager - 20.0.802 (20 LTS Update 2023-07-19)

Release date: July 19, 2023

Build number: 20.0.802

### Enhancements

- Updated Deep Security Manager to add SQL Server 2022 database support. SF06543523/SEG-169639/SEG-171432/DS-76501
- If the computer is a Podman Host, computer details now display the Podman version. DS-76683

### Resolved issues

- When creating a new Scheduled Task, the "Next Run Time" value displayed in the Scheduled Task list was incorrect. SF06593263/SEG-171126/DS-76900
- Upgrade Agent Software actions would sometimes fail on Amazon Linux platforms. DSM-14
- Deep Security Manager would sometimes fail to synchronize to a Vision One Service Gateway. SF06928392/SEG-182692/DSM-19

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. VRTS-6038/DSM-32/DSM-55

Highest Common Vulnerability Scoring System (CVSS) score: 7.5

Highest severity: High

## Deep Security Manager - 20.0.789 (20 LTS Update 2023-06-28)

Release date: June 28, 2023

Build number: 20.0.789

### New Features

**Trend Vision One Inventory support**: Deep Security Manager integration with Vision One now supports Endpoint Inventory, Inventory Group, and Inventory Compliance.

### Enhancements

- Deep Security Manager now supports PostgreSQL 14. SF06514546/SEG-169342/DS-76494
- Deep Security Manager now supports AWS Aurora PostgreSQL 14. DS-77594
- Deep Security Manager now supports VMware Cloud Director 10.4. SEG-152378/DS-74227
- Deep Security Manager now supports AWS RDS PostgreSQL 14. DS-76494
- Improved the processing of rules in recommendation scan. Recommendation scan does not work on Deep Security Manager versions earlier than 20.0.789 (20 LTS Update 2023-06-28) after applying 24-024.dsru. PCT-27452/PCT-27565

### Resolved issues

- The Deep Security Manager console sometimes froze when opening the agent migration pop-up window. SEG-180945/DS-78114

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. VRTS-9496/DS-77146

Highest Common Vulnerability Scoring System (CVSS) score: 4.3

Highest severity: Medium

## Deep Security Manager - 20.0.768 (20 LTS Update 2023-05-17)

Release date: May 17, 2023

Build number: 20.0.768

### New Features

**Device Control**: Deep Security Manager version 20.0.768 or later now supports Device Control for Windows Server platforms, helping to protect external storage devices connected to protected endpoints. This requires Deep Security Agent 20.0.0.6313 or later. For for information, see Supported features by platform.

### Resolved issues

- Deep Security Manager sometimes generated Tenant reports containing incorrect information for Deep Security Agents running in a multi-tenant environment. SF06301702/SEG-162798/DS-76311
- Deep Security Manager's dashboard sometimes failed to include events within the status and event history widgets. SF06492268/SEG-168155/DS-76201

## Deep Security Manager - 20.0.759 (20 LTS Update 2023-04-19)

Release date: April 19, 2023

Build number: 20.0.759

### Enhancements

- Agent Version Control is now available when configuring agent upgrade Scheduled Tasks. SF06094463/SEG-159727/DS-74710
- Due to product name changes, all mentions of Trend Micro Vision One were changed to Trend Vision One. DS-76215

### Resolved issues

- Under certain conditions, Deep Security events would incorrectly report that 'The component "Advanced Threat Scan Engine" has been removed'. SF05801044/SEG-147779/DS-75232
- Some lists in the management console were causing performance issues in environments with more than 50,000 hosts. SF05874881/SEG-149417/DS-72746
  The affected lists include, but are not limited to, the lists under System Event, Computer, Single Report, Scheduled Reports, Scheduled Task, Alert, and Dashboard.

## Deep Security Manager - 20.0.741 (20 LTS Update 2023-03-15)

Release date: March 15, 2023

Build number: 20.0.741

### New Features

**Service Gateway**: Deep Security Manager version 20.0.741 or later now supports Service Gateway, providing forward proxy functionality.

## Deep Security Manager - 20.0.737 (20 LTS Update 2023-02-23)

Release date: February 23, 2023

Build number: 20.0.737

### Enhancements

- Deep Security Manager 20.0.737 or later now supports Red Hat Enterprise Linux 9 (64-bit). SF06130289/SEG-157410/DS-74295
- Deep Security Manager now enforces certificate updates to RSA-2048 and SHA-256 for agents using unsupported certificates. Deep Security Agent version 20.0.0-6313 or later does not support SHA-1) For more details, see Upgrade the Deep Security cryptographic algorithm. DS-76297
- Updated Deep Security Manager to add API Smart Folder functionality. DS-75375

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. DS-75668/DS-75924

Highest Common Vulnerability Scoring System (CVSS) score: 8.1

Highest severity: High

## Deep Security Manager - 20.0.725 (20 LTS Update 2023-01-18)

Release date: January 18, 2023

Build number: 20.0.725

### Resolved issues

- Updated Deep Security Manager to include an OS (operating system) field for syslog forwarding if `settings.configuration.addPlatformInSyslogMessage` is set to true by console command. For more information, see Adding AWS instance ID or OS fields in syslog messages in Deep Security Manager (DSM). DS-73163

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. DS-74793

Highest Common Vulnerability Scoring System (CVSS) score: 7.5

Highest severity: High

## Deep Security Manager - 20.0.716 (20 LTS Update 2022-12-15)

Release date: December 15, 2022

Build number: 20.0.716

### Resolved issues

- When exporting the list of computers to CSV, the Docker Host and CRI-O Host field value was not included correctly. SF05232601/SEG-131041/DS-73391
- The Deep Security Manager would report Rocky Linux 8 as an unknown Linux OS when registered through the AWS connector. DS-71999

## Deep Security Manager - 20.0.711 (20 LTS Update 2022-11-16)

Release date: November 16, 2022

Build number: 20.0.711

### Enhancements

- Updated Deep Security Manager to include Project ID for computers using Google Cloud Platform. SF05811253/SEG-147466/DS-72694

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. DS-74218

Highest Common Vulnerability Scoring System (CVSS) score: 7.5

Highest severity: High

## Deep Security Manager - 20.0.703 (20 LTS Update 2022-10-19)

Release date: October 19, 2022

Build number: 20.0.703

### Enhancements

- With Multi-Factor Authentication enabled, changing an account password now requires verifying the user's MFA code (in addition to the user's old password). DS-73341
- Updated Deep Security Manager to notify users of trust entity ruleset changes in the computer's status bar. DS-70956
- Updated Deep Security Manager to allow using question marks in Application Control trust rule `paths` property fields to match a single additional character in the path. DS-71604
- Updated the Deep Security Manager's UI tooltip for trust entity rules to describe the latest wildcard functionality. DS-69964
- Updated Deep Security Manager to use the latest Simple Object Access Protocol (SOAP) components to protect against vulnerabilities affecting older versions. DS-73080

### Resolved issues

- Reports generated by Deep Security Manager **(Events & Reports > Generate Reports)** did not display Chinese language characters properly. SF05883379/SEG-149459/DS-72858

- Anti-Malware events sometimes displayed a blank file path with invalid Unicode encoding. 01746052/SEG-46912/DSSEG-3653
- Application Control rule permissions configured by administrators did not result in the corresponding functionality for users. As examples, a rule with its permissions set to Hide was still visible to users, and one with a Custom configuration preventing users from creating new rules did not prevent them from doing so. DS-68693
- In Trust Entity Management (**Policies > Common Objects > Application Control Rules > Trust Entities**), the horizontal scroll bar in the **Edit Trust Ruleset** window was covering rules displayed at the bottom of the window. DS-70435

## Deep Security Manager - 20.0.686 (20 LTS Update 2022-09-21)

Release date: September 21, 2022

Build number: 20.0.686

### Resolved issues

- If an Application Control shared ruleset was successfully created on a Deep Security Agent using the API, creating another shared ruleset with the API on the same agent would fail. DS-71034
- Deep Security Manager sometimes displayed the wrong state for items in an Anti-Malware Report (**Events & Reports > Generate Reports**). SF05780825/SEG-149707/DS-72871
- With Perform Ongoing Recommendation Scans set to Yes and an Ongoing Scan Interval set to 4 Weeks (**Computer** or **Policy > Settings > General > Recommendations**), Deep Security Manager executed the scans much more frequently than the set interval. SF05658685/SEG-148153/DSSEG-7707

## Deep Security Manager - 20.0.677 (20 LTS Update 2022-08-17)

Release date: August 17, 2022

Build number: 20.0.677

### New Features

**Windows Server 2022 support**: Deep Security Manager version 20.0.677 or later now supports Windows Server 2022.

### Enhancements

- Updated Deep Security Manager to encrypt user login details. DS-71448

### Resolved issues

- Under **Events & Reports > Firewall Events**, when using Action and Contains filters to search for Fail Open: Deny, the search results failed to display matching events. SF05740930/SEG-146282/DS-72636
- VMware vCloud accounts missing their OS type caused synchronization to fail. SF05830546/SEG-147983/DS-72518
- VMware vCloud connectors with more than 25 Virtual Data Centers only displayed 25 in Deep Security Manager. SEG-147252/DS-72376
- When Deep Security Relay were rehomed to a vCenter connector, they lost their original hostname in Deep Security Manager. SF05519505/SEG-140015/DS-72596
- Deep Security Manager sometimes generated unexpected Computer Updated system events. SF05496967/SEG-138407/DSSEG-7672

## Deep Security Manager - 20.0.664 (20 LTS Update 2022-07-21)

Release date: July 21, 2022

Build number: 20.0.664

### Enhancements

- Updated Deep Security Manager to include port 443 by default (along with ports 80 and 8080) for Ports to Monitor for Potentially Harmful Web Pages (**Computer** or **Policy > Web Reputation > Advanced**). This change prepares Web Reputation SSL inspection support on port 443 for future (not yet released) Deep Security Agent versions.
- Updated Deep Security Manager to add the `-disablemfa` parameter. This parameter allows users to disable Multi-factor authentication (MFA) when using the `dsm_c` command line to perform a password reset. DS-69590

### Resolved issues

- Deep Security Manager was sometimes unable to synchronize with Microsoft Active Directory (AD) users. SEG-138257/SF05452498/DS-70873

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. DS-71624

Highest Common Vulnerability Scoring System (CVSS) score: 9.8

Highest severity: Critical

## Deep Security Manager - 20.0.651 (20 LTS Update 2022-06-15)

Release date: June 15, 2022

Build number: 20.0.651

### Enhancements

- Updated Deep Security Manager to provide more information for Anti-Malware Engine Offline events, including an ID indicating the event's cause and a link in the description leading to recommended actions. Also, a system log entry for the event is now generated if SIEM is enabled. DS-70595
- Updated Deep Security Manager to save disk space by removing outdated versions of the agent installer package. DS-67840
- Updated Deep Security Manager to trigger event based tasks related to creating a computer when adding an active directory computer with the "Add Active Directory" wizard. DS-68877
- Updated Deep Security Manager to remove support for 8.0 and 9.0 Deep Security Agents, since these versions are past their EOL dates. For more information, see Deep Security LTS life cycle dates. DS-70332

## Deep Security Manager - 20.0.644 (20 LTS Update 2022-05-18)

Release date: May 18, 2022

Build number: 20.0.644

### Resolved issues

- Some rules did not display properly in Deep Security Manager when columns were sorted By Group (under **Policies > Common Objects > Rules** or under **Computers > Computers**). SEG-127353/DS-68348
- Agent activation sometimes became stuck in a loop which caused high memory consumption for Deep Security Manager. DS-71234

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases.DS-71244/DS-65171

Highest Common Vulnerability Scoring System (CVSS) score: 7.5

Highest severity: High

## Deep Security Manager - 20.0.635 (20 LTS Update 2022-04-21)

Release date: April 21, 2022

Build number: 20.0.635

### New Features

**Advanced TLS traffic inspection**: Deep Security Manager now provides an option to configure advanced TLS traffic inspection, removing the need to configure TLS credentials manually and adding support for more ciphers. You can verify the status of the feature by viewing the policy properties (Policy > Intrusion Prevention > General > Advanced TLS Traffic Inspection). For more information, see Enable Advanced TLS traffic inspection.

**Azure and GCP connector migration support**: Azure and GCP (Google Cloud Platform) connectors can now be migrated from Deep Security Manager to Trend Micro Cloud One - Workload Security. For more information, see Migrate cloud accounts to Workload Security.

### Resolved issues

- Deep Security Manager was not receiving the number associated with systemEventID errors for system configurations using Simple Network Management Protocol (SNMP).

SEG-122864/04711592/DS-67387

- Intrusion Prevention events containing number strings, such as IP addresses, sometimes resulted in Get Events Failed `NumberFormatException` errors in Deep Security Manager. SEG-120226/SF04838989/DSSEG-7216
- Deep Security Manager was sometimes unable to sync with vCloud. SEG-135846/SF05409802/DS-70336
- Deep Security Manager did not properly display Computer Moved events. DS-70669
- When a Deep Security Agent with an existing Application Control local ruleset was removed from Deep Security Manager, the ruleset for that agent still appeared in the manager (under **Policies > Application Control Rules > Software Rulesets**). DS-68173
- If the REST API was used to select the `critical-and-heuristic` parameter for Document Exploit Protection, Deep Security Manager would not display that selection for the malware scan configuration (under **Computer** or **Policy > Anti-Malware > General > Edit**). DS-67975

## Deep Security Manager - 20.0.619 (20 LTS Update 2022-03-22)

Release date: March 22, 2022

Build number: 20.0.619

### New Features

**FIPS mode for Amazon Linux 2**: Deep Security Manager version 20.0.619 or later now supports FIPS mode for AWS Marketplace deployment. This is supported for Deep Security Agent version 20.0.0-2971 or later.

### Enhancements

- Updated Deep Security Manager to use the term *protected* instead of *anonymous* when referring to Trend Micro Feedback being shared with the Smart Protection Network. DS-70101

### Resolved issues

- Deep Security Manager failed to migrate policies to Trend Micro Cloud One - Workload Security if a module's license had expired. DS-69595

- In a Security Module Usage Cumulative Report (**Events & Reports > Generate Reports**), Application Control usage hours were not being included properly under System Usage hours. DS-67494
- The Deep Security Manager Trust Entities **New Ruleset** window (**Trust Entities > Trust Ruleset > New**) had its **OK** and **Close** buttons blocked on some screen resolutions. DS-68838
- Behavior Monitoring status of Deep Security Agents for Linux was inconsistent on Deep Security Manager versions later than 20.0.312. With Behavior Monitor detection disable, the manager console sometimes still showed that it was enabled under the default settings for Anti-Malware real-time or advanced real-time scans. DS-69536
- There was a connectivity issue when a Deep Security Agent had FIPS mode enabled but Deep Security Manager did not. DS-70038

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. SEG-132505/SF05278860/DS-69608/DS-69764

Highest Common Vulnerability Scoring System (CVSS) score: 9.8

Highest severity: Critical

## Deep Security Manager - 20.0.605 (20 LTS Update 2022-02-16)

Release date: February 16, 2022

Build number: 20.0.605

### Enhancements

- Updated Deep Security Manager to allow users to toggle real time container protection (from **Computer** or **Policy Settings > General**). This setting is enabled by default. SEG-115751/DS-68963

### Resolved issues

- Filtering Smart Folders by Folder Name sometimes displayed results for folders or groups that no longer existed. SEG-120786/SF04858677/DSSEG-7220
- With event-based task settings enabled for NSX Security Group Change (**Administration > Event-Based Tasks**), Deep Security Manager would trigger auto-activation of a virtual machine if it was removed from an NSX Security Group. DS-36694
- Deep Security Manager displayed the wrong description for Move Failed (No Response) system events. DS-69407

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. VRTS-5866/DS-62223

Highest Common Vulnerability Scoring System (CVSS) score: 8.2

Highest severity: High

## Deep Security Manager - 20.0.585 (20 LTS Update 2022-01-17)

Release date: January 17, 2022

Build number: 20.0.585

### New Features

**Application Control Trust Entities**: This feature lets you configure trust rules to auto-authorize software changes in your environments, reducing the number of software changes and security events you need to manage manually. For details, see Application Control Trust Entities.

### Enhancements

- Deployment scripts used to install Trend Micro Endpoint Basecamp (required to forward security events to Trend Micro Vision One) have been updated with a new certificate issuer organization name.

### Resolved issues

- Moving Deep Security Agents to Workload Security would fail if Deep Security Manager was configured with a proxy that doesn't require authentication credentials. DS-68710

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. DS-68725, DS-67244

Highest Common Vulnerability Scoring System (CVSS) score: 9.1

Highest severity: Critical

## Deep Security Manager - 20.0.560 (20 LTS Update 2021-12-16)

Release date: December 16, 2021

Build number: 20.0.560

### New Features

**Trusted Certificates Detection Exceptions**: Deep Security Manager version 20.0.560 or later now allows you to configure Trusted Certificates Detection Exceptions (from a policy's **Details & Anti-Malware & Advanced** tab) to exclude files from Anti-Malware scanning based on their digital certificate. This is currently supported for Deep Security Agent version 20.0.0-3445 or later on Windows platforms only. For more information, see Exclude files signed by a trusted certificate.

### Resolved issues

- Deep Security Manager was unable to retrieve security settings from groups containing more than 1000 computers. SF05006314/SEG-124719/DS-67938
- Deep Security Manager was sending suspicious objects to Deep Security Agent even after the objects' expire time had ended. DS-67917
- Deep Security Manager was not displaying virtual machines that had been upgraded to VMware Cloud Director 10.3 or 10.3.1, even though they were still connected. SEG-123585/SF04968350/DS-67513

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. DS-68162/DS-65579

Highest Common Vulnerability Scoring System (CVSS) score: 7.5

Highest severity: High

## Deep Security Manager - 20.0.543 (20 LTS Update 2021-11-18)

Release date: November 18, 2021

Build number: 20.0.543

### Enhancements

- Updated Deep Security Manager to hide the Trend Micro Vision One promotion banner for 24 hours after being dismissed by a user. DS-55349
- You can now use Azure application certificate authentication when adding an Azure connector. For details, see "Add a Microsoft Azure account to Deep Security" on page 602. DS-63762
- Improved migration from Deep Security Manager to Workload Security in the following ways:
  - Updated Deep Security Manager to handle connectivity issues better during migration to Workload Security, preventing the console UI from being blocked or stuck in a loading loop. DS-67841
  - Updated Deep Security Manager so that the Computer Group list for Deep Security Agents being migrated to Workload Security no longer displays computer groups generated by connectors. DS-67776
  - Updated Deep Security Manager Move Failed system events to include additional event details from the Workload Security side. DS-67921
  - Updated Deep Security Manager to check for inactivated computers with the same hostname as computers being migrated to Workload Security. If a matching hostname

is found, the manager now updates the existing computer instead of marking the task as Move Failed. DS-67527

- Updated Deep Security Manager's policy migration page (**Support > Migrate to Workload Security > Configurations**) to note that Rule Updates must be up to date before migration, and that common objects in Workload Security are overwritten if they have the same name as migrated objects. DS-67777
- Updated Deep Security Manager to remove the Migrate to Workload Security option (shown when right-clicking a computer) for computers that are not migratable. DS-67666

### Resolved issues

- Software Update sometimes failed if the kernel support package and the agent installer were both the same version. DS-67547
- Deep Security Manager system events sometimes had No Description in the description field. DS-66878
- Deep Security Manager sometimes received alerts for agents that had not been activated. DS-64523
- After an update, Deep Security Manager kept a copy of the previous version's online help files. SEG-120770/SF04858311/DS-66969
- In Deep Security Manager's **Computers** tab, the LAST COMMUNICATION column sometimes did not sort correctly. SEG-120751/SF04862693/DS-67579
- Deep Security Manager was unable to migrate agent/appliance initiated agents (AIA) with certain configurations over to Workload Security. SEG-124938/DS-67861
- When the Migrate With Settings Overridden at Computer Level option was selected, Deep Security Manager incorrectly tried to migrate rule assignments, which could cause the migration to Workload Security to fail. DS-67528
- For Deep Security Managers using an Oracle Database, any computers requesting migration to Workload Security would have their status show Moving even if the migration was successful. DS-67930
- Deep Security Manager sometimes encountered a runtime exception that would prevent computers from moving to Workload Security during migration. DS-67932

## Deep Security Manager - 20.0.513 (20 LTS Update 2021-10-14)

Release date: October 14, 2021

Build number: 20.0.513

### New Feature

**Migrate to Workload Security using the Deep Security Manager UI**: Deep Security Manager now supports moving agents and policy configurations to Trend Micro Cloud One Workload Security using the Deep Security Manager UI. This includes the following:

- Migrate agents using the UI
- Migrate configurations using the UI
- Migrate agents with settings overridden at the computer level
- Move multiple agents at the same time with a single BatchComputerMoveTask API call

For more information, see Migrate to Workload Security.

### Resolved issues

- While syncing Trend Micro Vision One (XDR) status, Deep Security Manager sometimes failed to synchronize the Sandbox as a Service status at the same time. DS-66122

## Deep Security Manager - 20.0.503 (20 LTS Update 2021-09-23)

Release date: September 23, 2021

Build number: 20.0.503

### New Feature

**Control kernel package updates**: This update introduces a new way to manage your kernel support packages. Deep Security Manager now provides an option to automatically update the kernel package when an agent restarts on Linux. For details, see "Disable optional Linux kernel support package updates" on page 410.

### Enhancements

- Updated Deep Security Manager to integrate with Trend Micro Vision One for Threat Intelligence (previously known as Connected Threat Defense). DS-61106

- Updated Deep Security Manager to allow the removal of Integrity Monitoring baseline data using a console (dsm_c) command. Removing baseline data does not affect the protection you receive from Integrity Monitoring, but does remove the following:

- The option to View Baseline data from the manager console
- The ability to use Trusted Common Baseline as a source of Auto-Tagging
- The ability to generate an Integrity Monitoring Baseline Report

As baselines have grown larger and workloads have become more dynamic, the ability to support the Integrity Monitoring baseline in the Deep Security Manager console has become increasingly challenging. We are committed to evolving the design of Integrity Monitoring to meet the performance and operational needs of our customers. Through discussions with our customers, it was determined that in its current form, Integrity Monitoring was not always delivering the value to offset the performance and operational overhead required to maintain baseline data. For more details on disabling baseline data, see Database performance issue due to lots of Integrity Monitoring baseline data. DS-60498

## Resolved issues

- Deep Security Agent automatic upgrades sometimes failed if Deep Security Manager had Upgrade on Activation and Event-based Tasks enabled at the same time. SEG-105646/SF04249597/DS-62190
- The Deep Security Manager console command to add a trusted certificate sometimes failed for LDAPS server certificates. SEG-116063/SF04716472/DS-65277
- Some API key fields used to migrate to Workload Security were missing from the Workload Security Links API document. DS-66022
- In environments with multiple vCenter connectors undergoing frequent vMotion, Deep Security Manager sometimes encountered a deadlock causing Engine Offline errors for Anti-Malware, Firewall, and Intrusion Prevention. SEG-115729/SF04696226/DS-65311
- Deep Security Manager sometimes couldn't retrieve a computer's information, causing VMware NSX synchronization to fail. SEG-117202/DS-65610
- Deep Security Virtual Appliance IPv6 addresses sometimes displayed in the Deep Security Manager console even if the IPv6 was not available in the environment. SEG-118810/SF04806948/DS-66263
- Deep Security Manager Scheduled Reports (**Events & Scheduled Reports**) with a Using Policy computer filter sometimes still showed all computers in the generated reports. SF04676734/SEG-116345/DS-65336

- Deep Security Agent upgrade failures sometimes occurred if Default Real-Time Scan File List or Directory List exclusions were created with duplicate names in Deep Security Manager. DS-65746

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. VRTS-5934/DS-63325/DS-65607

Highest Common Vulnerability Scoring System (CVSS) score: 7.5

Highest severity: High

## Deep Security Manager - 20.0.482 (20 LTS Update 2021-08-25)

Release date: August 25, 2021

Build number: 20.0.482

### Enhancements

- Updated Deep Security Manager to support PostgreSQL 12 and PostgreSQL 13 in FIPS mode. For more information see FIPS 140-2 support. DS-63876
- Updated Deep Security Manager's Workload Security Link API to support URLs containing "https" when attempting to Migrate to Workload Security. DS-65095

### Resolved issues

- Deep Security Manager Scheduled Tasks (**Administration > Scheduled Tasks**) configured to run daily would sometimes run hourly. SEG-108098/DS-64247
- In Deep Security Manager's Computers page, the LAST MANUAL SCAN FOR MALWARE and LAST SCHEDULED SCAN FOR MALWARE columns sometimes did not sort properly.
- Tenants were sometimes unable to update their license if the primary tenant enabled a proxy server with credentials (**Administration > System Settings > Proxies > Deep Security Manager (Software Updates, CSSS, News Updates, Product Registration and Licensing)**).

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. VRTS-5932/DS-63442/DS-51695/ VRTS-5930/DS-63071/ VRTS-5929/DS-63072

Highest Common Vulnerability Scoring System (CVSS) score: 6.5

Highest severity: Medium

## Deep Security Manager - 20.0.463 (20 LTS Update 2021-07-22)

Release date: July 22, 2021

Build number: 20.0.463

### Enhancements

- Updated Deep Security Manager to include two different action options in the Anti-Malware Scan Interface (AMSI): Customers can now select either Pass or Terminate. DS-63691
- Updated Deep Security Manager to support migrating policies to Workload Security using the new MigratePolicy API command. This command automates the process of migrating the Deep Security Policies from their current on-premise manager to a Cloud One Workload Security tenant. DS-63316
- Updated Deep Security Manager to check if the virtual machine's IP address is reachable during the rehoming process for vCenter. DS-63514

### Resolved issues

- Deep Security Manager was sometimes unable to send emails on systems with more than one network interface card (NIC). DS-63254
- Deep Security Agents using agent-initiated activation (AIA) sometimes went offline following a certificate update. DS-58106
- When generating an Agent Version Report (**Events & Reports > Generate Reports**), the report generated as if All Computers was selected in the Computer Filter section regardless of which option was actually selected. DS-64133

- Filtering a Smart Folder by Tag was not working properly for new events added with Auto-Tagging (**Events & Reports > Events > (Select an event type) > Auto-Tagging**). DS-61210
- When a virtual machine (on vCenter) had multiple IP addresses, Deep Security Manager was sometimes unable to select the correct IP address. SEG-109694/SF04486485/DS-63235
- Deep Security Manager would sometimes re-download an outdated Kernel Support Package (KSP) that had previously been deleted. SEG-101335/04121383/DS-60849

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. DS-64012/ VRTS-5931/DS-63070

Highest Common Vulnerability Scoring System (CVSS) score: 6.8

Highest severity: Medium

## Deep Security Manager - 20.0.447 (20 LTS Update 2021-06-28)

Release date: June 28, 2021

Build number: 20.0.447

### New Feature

**Re-parent agents**: Deep Security Manager now supports moving agents to Trend Micro Cloud One Workload Security using the new MoveAgent API command. This command automates the process of re-parenting an activated Deep Security Agent from its current on-premise manager to a Workload Security tenant. If re-parenting is unsuccessful, the agent will re-activate with its on-premise manager, retaining its previous configuration.

Due to feature differences between the Deep Security and Workload Security managers, move tasks may be refused to prevent unexpected behaviors. You should disable the following before moving agents:

- FIPS 140-2: Deep Security Manager will refuse move tasks if FIPS 140-2 support is enabled.

- Deep Security Virtual Appliance: Computers protected by Deep Security Virtual Appliance (agentless or combined mode) will refuse move tasks.
- SAP NetWeaver integration: Agents with SAP NetWeaver integration will accept move tasks. However, after being moved to Workload Security, the SAP NetWeaver integration will not be available until it is supported on Workload Security.

## Enhancements

- Updated Deep Security Manager to add PostgreSQL 12 and PostgreSQL 13 database support. DS-59911
- Removed the Windows logo that was displayed next to Predictive Machine Learning in the Deep Security Manager UI. Predictive Machine Learning is currently supported by all Windows agents, as well as Linux agents version 20.0.0-2395 or later. DS-62929
- Updated Deep Security Manager to note which agent versions support Behavior Monitoring Pass action: Deep Security Agent 20.0.0-1559 or later on Windows and Deep Security Agent 20.0.0-1822 or later on Linux. DS-62937
- Updated the Activity Data Forwarding description (**Administration > System Settings > Trend Micro Vision One**) to provide more information on script deployment. DS-63278
- Updated the Endpoint Basecamp deployment script (**Administration > System Settings > Trend Micro Vision One > Activity Data Forwarding**) to improve support on some platforms, and updated script deployment error messages to be more descriptive. SEG-109629/DS-63157

## Resolved issues

- In Deep Security Manager's **Tenants** page (**Administration > Tenants**), some columns were being sorted based only on the first digit of the number of events or jobs, instead of being sorted based on the entire number. SEG-107657/DS-62544
- Deep Security Manager had high memory consumption when querying databases with a large number of security profiles. SEG-103097/SF04265571/DS-61490
- Anti-Malware Real-Time Scan Configuration policies sometimes did not reset to their inherited value properly. DS-63835
- System event messages sometimes contained information referencing the wrong operating system. SF04443281/SEG-111629/DS-64089

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases.DS-63110/DS-61049

Highest Common Vulnerability Scoring System (CVSS) score: 5.8

Highest severity: Low

## Deep Security Manager - 20.0.414 (20 LTS Update 2021-05-24)

Release date: May 24, 2021

Build number: 20.0.414

### Enhancement

- Updated Deep Security Manager to enhance the Identified Files download mechanism, including the ability to download from agent-initiated Deep Security Agents, and a new File Status field on identified files to indicate download progress. DS-60741

### Resolved issues

- Under some configurations an internal error prevented users from generating a Deep Security Best Practice Guide Report.SF04154114/SEG-99975/DS-60897
- An account permissions issue sometimes caused Trend Micro Vision One registration to fail or display the wrong status (under **Administration > System Settings > Trend Micro Vision One**). DS-61893
- Deep Security Manager sometimes had connectivity issues preventing computers from importing properly and preventing Deep Security Relays from activating or deactivating. DS-58417
- Deep Security Manager sometimes incorrectly prevented users with an Auditor role from viewing Firewall Rules (**Policies > Rules > Firewall Rules**). SF04220398/SEG-102016/DS-60847
- Deep Security Manager links to Japanese language content failed to load in setups using an air gapped Online Help package (**Administration > Updates > Local**). 04442246/SEG-108814/DS-63080

- Deep Security Manager sometimes stopped processing scheduled tasks if the database connection was unstable. DSSEG-6689/DS-62963

## Deep Security Manager - 20.0.393 (20 LTS Update 2021-04-27)

Release date: April 27, 2021

Build number: 20.0.393

### Enhancements

- Updated Deep Security Manager to add a message to an event's description if the event is purged by one of the Automatically Delete Events Older Than options (**Administration > System Settings > Storage**). DS-59349
- Updated Deep Security Manager to increase the number of >Maximum TCP Connections (**Computers > Computers > Details > Settings > Advanced**) to 1000000 by default. DS-61032

### Resolved issues

- Deep Security Manager version upgrade sometimes failed when a key value contained special characters. SEG-99875/SF04106715/DS-60581
- Anti-Malware Scheduled Scan was not working under some configurations. DS-54952
- The Deep Security Manager console's load time was sometimes slower than normal when many policies existed and/or were assigned to roles. SEG-90429/SF03787758/DS-58871
- The Automatically Delete Server Logs Older Than setting (**Administration > System Settings > Storage**) appeared for tenants when it should have only appeared for the primary tenant. DS-58669
- The View Renewal Instructions URL was broken in **License Properties** (**Administration > Licenses > View Details**). SEG-104258/SF04308332/DS-61343
- Deep Security Manager was sometimes unable to synchronize with AWS Connectors. SEG-102091/SF04198233/DSSEG-6726
- Deep Security Manager was unable to validate credentials for some AWS connectors when their region data changed unexpectedly in the database. SEG-97924/DS-60541
- Deep Security Manager was sometimes unable to access existing Real-Time Malware Scan Configurations (**Policies > Common Objects > Other > Malware Scan Configurations**). SEG-86700/SF03646616/DS-55577

- A Data Pruning malfunction (**Administration > System Settings > Storage**) sometimes led to a large number of events, causing performance issues between the Deep Security Manager and database. SEG-97589/SF04073627/DS-61356
- System Event Reports in Deep Security Manager (**Events & Reports > Generate Reports**) were sometimes generated with data missing. DS-61752
- Deep Security Manager was sometimes unable to generate a password-protected Single Report or password-protected Scheduled Reports (**Events & Reports > Generate Reports**). SEG-105241/SF04341549/DS-61718
- Updating the password for an Azure Connector (**Computers > Computers > right-click Azure Connector > Properties > Connection**) sometimes did not work, causing the account to lose its connection to Deep Security Manager. DS-60479
- Deep Security Manager sometimes could not remove a vCenter Connector that had NSX installed. DS-61101
- Deep Security Manager's Anti-Malware Protection Status on the **Dashboard** sometimes displayed incorrect information. SEG-103625/SF04271447/DS-61598
- Application Control hours were not being calculated when generating a Security Module Usage Cumulative Report (**Events & Reports > Generate Reports**). SEG-100505/SF04174981/DS-60675

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. DS-51780/DS-61318

Highest Common Vulnerability Scoring System (CVSS) score: 8.2

Highest severity: Medium

## Deep Security Manager - 20.0.366 (20 LTS Update 2021-03-24)

Release date: March 24, 2021

Build number: 20.0.366

## New Feature

**Deploy Trend Micro Endpoint Basecamp for Trend Micro Vision One (XDR)**: After onboarding to Trend Micro Vision One (XDR), you can now select the **Trend Micro Endpoint Basecamp Agent Deployment Script** (**Support > Deployment Scripts**) to automatically deploy it along with your Deep Security Agent on Linux or Windows platforms.

## Enhancements

- Updated Deep Security Manager to make error messages, and the actions required to troubleshoot them, clearer during Trend Micro Vision One (XDR) registration. DS-61057

## Resolved issues

- Deep Security Manager System Event Reports (**Events & Reports > Generate Reports**) sometimes had no data in the section for Most Active Computers Ranked by Number of System Events. DS-28985
- **Malware Scan Status** on the **Dashboard** sometimes displayed the wrong data. DS-57263
- Deep Security Manager's Security Updates Overview (**Administration > Updates > Security**) sometimes showed No Scheduled Task even if there was one in **Administration > Scheduled Tasks**. SEG-97381/DS-60271
- Entering certain terms in the Computers search field (in the **Computers** tab) would cause the search to fail and display an Internal server error. SEG-98108/SF03976840/DS-60133
- A user with View-Only privileges was able to make changes to Deep Security Manager's Application Control Ruleset actions. SEG-81133/03347924/DS-61041

## Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. DS-61209/VRTS-4382/03116764/DS-49429

Highest Common Vulnerability Scoring System (CVSS) score: 7.5

Highest severity: High

# Deep Security Manager - 20.0.344 (20 LTS Update 2021-02-23)

Release date: February 23, 2021

Build number: 20.0.344

## Enhancements

- Updated Deep Security Manager's Anti-Malware default real-time scan exclusions to enhance performance. DS-55169
- Updated Deep Security Manager UI to rename Trend Micro XDR as Trend Micro Vision One. DS-60273
- Updated Deep Security Manager to add deployment script support for CentOS 8 and RedHat 8. DS-60413
- Updated Trend Micro Vision One tab Learn More links to point to content based on the language of a user's locale (EN/JP). DS-60487
- Updated the Deep Security Software page to fix some incorrect links. DS-60494
- Updated Deep Security Manager to add 2 Days as an option for Inactive Agent Cleanup (**Administration > Agents > Inactive Agent Cleanup**). SEG-91358/SF03711833/DS-59591
- Updated Deep Security Manager to improve vCenter connectivity when a Deep Security Agent's IP is unreachable, and when Manager-Initiated communication is enabled. DS-58526
- Updated Deep Security Manager to add support for ports 32767-65535. SEG-98840/SF04119337/DS-60122
- Updated the Deep Security Manager's XDR Basecamp (XBC) deployment script UI to provide a link to the latest platform support info on the online help center. DS-60206

## Resolved issues

- When a VM was managed through both the **Computers > Add Active Directory** and **Add Azure Account** options, issues with host updates and rehoming occurred. SEG-97266/SF03911224/DS-59853
- Deep Security Manager's Anti-Malware Protection Status Widget (in the **Dashboard** tab) sometimes failed to display data. DS-48046
- Deep Security Manager integration with an SAML identity provider sometimes failed if all roles didn't match the expected format. SEG-90158/SF03783432/DS-57687

## Deep Security Manager - 20.0.321 (20 LTS Update 2021-01-26)

Release date: January 26, 2021

Build number: 20.0.321

### Enhancements

- Updated Deep Security Manager to display the correct deployment script when it is selected from the **Platform** menu (**Administration > System Settings > Trend Micro Vision One**). DS-59825
- Updated Deep Security Manager to support agentless mode for NSX-T on VMWare Cloud Director version 10.2 or later. DS-54044

### Resolved issues

- Running multiple Check for Security Update scheduled tasks at the same time sometimes resulted in updates being skipped. DS-59715

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. DS-59917

Highest Common Vulnerability Scoring System (CVSS) score: 6.1

Highest severity: Medium

## Deep Security Manager - 20.0.313 (20 LTS Update 2021-01-18)

Release date: January 18, 2021

Build number: 20.0.313

### New Feature

**Trend Micro Endpoint Basecamp Agent**: Trend Micro Endpoint Basecamp (XBC) Agent integrates XDR tools and functionality into Deep Security, following Trend Micro Vision One onboarding. For more information see "Integrate with Trend Vision One (XDR)" on page 1682.

## Enhancements

- Updated vCenter to make changing an NSX Manager simpler by using the **Remove NSX Manager** button (**Properties > NSX Manager**) rather than editing the **Manager Address:** field. DS-58377
- Updated the Deep Security Manager so that, by default, Trend Micro Vision One is enabled after the onboarding experience and after migrating to a paid license. DS-58788
- Removed the **News** button from Deep Security Manager. For the latest news on product changes, see What's new? DS-58808
- Aligned package naming for Deep Security Manager and Deep Security Agent on the Download Center. DS-56806
- Updated Deep Security Manager to include the option to log Trend Micro Vision One issues (**Administration > System Information > Diagnostic Logging...**). DS-58533
- Updated Deep Security Manager's Default Real-Time Scan Configuration (**Computers > Details > Anti-Malware > General > Real-Time Scan > Malware Scan Configuration**) to enable Behavior Monitoring and Predictive Machine Learning by default. Later versions of Deep Security Agents (Windows agent 20.0.0.1559 or later, and Linux agent 20.0.0-1822 or later) will have Use Custom Actions set to Pass by default, and will log Anti-Malware Events. Earlier versions of agents will have Behavior Monitoring and Predictive Machine disabled if their **Possible Malware** Action to Take is set to Pass. DS-59282
- Updated the Deep Security Manager to make Trend Micro Vision One related settings and features consistent after the onboarding. DS-58788
- Updated the Deep Security Manager to improve Search Computer API and List Computer API performance. DS-56722

## Resolved issues

- When the Deep Security Manager installer detected at least 16 GB of RAM on the operating system, it was not automatically allocating 8 GB of RAM to the Java Virtual Machine as is recommended for best performance. SEG-87319/03645194/DS-55701
- The Deep Security Manager was unable to communicate with agents in some environments, causing agent offline issues. SEG-86783/SF03637359/DS-56400
- Anti-Malware Scan scheduled tasks that timed out sometimes restarted instead of triggering a Scheduled Task Skipped event as expected. DS-59252

- The Deep Security Manager console command used to set a preferred IP address for Deep Security Agents with multiple IPs was sometimes not working, causing some agents to be unable to connect. DS-58878
- Deep Security Manager version update install was failing under some configurations. SEG-95357/SF03988405/DS-59222
- Deep Security Manager installed an incorrect version of the relay in some cases. DS-59634
- The Deep Security license check for Trend Micro Vision One registration was sometimes failing. DS-59645
- After changing the settings for a policy (**Policies > Details > Settings > General**), the **Reset all settings to Inherent** button did not work for Automatically Send Policy Changes to Computers or Perform Ongoing Recommendation Scans. DS-56830
- Links were sometimes not clickable in the Computer Status of the **Dashboard** tab, and for Agent/Appliance Upgrade Recommended (New Version Available) alerts opened in the List View of the **Alerts** tab. DS-57968

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. DS-33781/DS-58415/DS-58917/DS-51741/DS-59636

Highest Common Vulnerability Scoring System (CVSS) score: 9.8

Highest severity: Critical

## Deep Security Manager - 20.0.262 (20 LTS Update 2020-11-26)

Release date: November 26, 2020

Build number: 20.0.262

### New Features

**Integrate with Trend Micro Vision One**: Trend Micro Vision One applies effective expert analytics and global threat intelligence using data collected across multiple vectors - email, endpoints, servers, cloud workloads, and networks. For more information, see "Integrate with Trend Vision One (XDR)" on page 1682.

**Custom actions for Behavior Monitoring and Machine Learning**: This release provides the ability to specify custom actions for Behavior Monitoring and Predictive Machine Learning.

### Enhancements

- The **Computer Description** field for Smart Folders can be used as a search criteria. SEG-85288/DS-55034

### Resolved issues

- In the Smart Folder Editor, the computer type was listed as Undefined instead of Physical Computers. DS-32765
- On the vCenter connector properties page, when a user clicked **Remove NSX Manager** and then re-registered the NSX-T manager, the network-related features displayed **Not supported (NSX license limited)**. DS-56411
- An internal server error occurred when AWS was added to a Smart Folders sub-folder with the **Version** condition selected. DS-50785
- When Log Inspection or Intrusion Prevention rules were added, the Web Application Firewall sometimes blocked the page. DS-56448

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. DS-57603

Highest Common Vulnerability Scoring System (CVSS) score: 3.7

Highest severity: Low

## Deep Security Manager 20.0.198 (20 LTS Update 2020-10-19)

Release date: October 19, 2020

Build number: 20.0.198

### Enhancements

- Enhanced the description of the Activation Failed event to specify why the event occurred. DS-29719

### Resolved issues

- If you installed standalone agents on VMware VMs, and then you subsequently added vCenter to Deep Security Manager, you would see duplicate computer records in the manager for one VM. DS-55316
- The settings on **Policies > Settings > Advanced** could not be changed because the **Inherited** option could not be deselected. DS-56309
- The **Administration > Updates > Security** page took a long time to load.

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. DS-54102/DS-53674

Highest Common Vulnerability Scoring System (CVSS) score: 6.5

Highest severity: Medium

## Deep Security Manager 20.0.174 (20 LTS Update 2020-09-16)

Release date: September 16, 2020

Build number: 20.0.174

### New features

#### Improved management and quality

**Agent Version Report**: The **Agent Version Report** has been created in order for you to view a summary of how many agents are using a specific agent version, the percentage of total agents each version is using and an overview of how many agents are online and how many are offline, all of which are broken down based on the Deep Security Agent's platform (OS). To generate the report, go to **Events & Reports > Generate Reports > Single Report > New > Agent Version Report**.

**Azure Government improvement**: Azure Government resources can be added through the Deep Security Manager Azure connector (**Computers > Add > Add Azure Account**). For more information, see How do I protect Azure Government instances?.

**Database encryption**: The process of encrypting the communication between Deep Security Manager and your database has been simplified. For more information, see "Encrypt communication between the Deep Security Manager and the database" on page 1506.

## Enhancements

- Reduced the time it takes to validate GCP service accounts when changing your GCP Account Properties configuration. Previously, this took a long time when there were a large number of auto-generated GCP projects. SEG-81743/SF03452889/DS-53515
- Updated the pager numbers, phone numbers and mobile numbers listed on the **User Properties** window (click your email at the top of the console and select **User Properties**) so they can be configured to exceed more than 30 digits.
- Updated the My User Summary on the console and the User and Contact Report (**Events & Reports > Generate Reports > Single Report**) to reflect the logins that have occurred in the last 30 days. SEG-81216/03407489/DSSEG-5897
- Added support for VMware Cloud Director (vCloud) 10.1.1 (with NSX-V only).
- Improved the "Scheduled report sending failed" error message by adding a more thorough description. For more information, see Troubleshoot: Scheduled report sending failed. SEG-77886/03221276/DS-54615
- Updated the **New Malware Scan Configuration Properties (Policies > Common Objects > Malware Scans > New)** default settings to match the default settings for the **Default Malware Scan Configuration Properties**.

## Resolved issues

- The **Computer Status** widget on Deep Security Manager's dashboard did not display the correct number of managed computers. DS-53294
- The Deep Security Agent trusted certificates were not automatically renewed. SEG-79146/SF03240076/DS-52488
- The AWS Contract License Exceeded alert sometimes occurred even though the number of protected computers did not exceed the limit. SEG-82932/SF03491496/DSSEG-5974
- Imported VMs in vClouds were unable to activate. SEG-75542/03189161/DS-53447
- The console sometimes showed the incorrect Log Inspection status. /DS-54630

- Some Intrusion Prevention rules were designed to operate exclusively in Detect Only mode, however you were able to change their behavior on the policy and computer pages. DS-54667
- An incorrect number of overrides were displayed on **Computer/Policy Editor > Overrides**. SEG-83802/03513073/DS-54710
- There was a rights issue with Scheduled Tasks that caused incorrect behaviors to occur when creating them. SEG-78610/SF03320936/DS-53292
- The MasterAdmin could not create a scheduled task for all computers. DS-55522
- Ransomware Event History on the dashboard displayed incorrect information. DS-55494

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases.DS-52678 /DS-21167 /DS-53059

Highest Common Vulnerability Scoring System (CVSS) score: 7.0

Highest severity: High

### Notices

Red Hat Enterprise Linux 5 and 6 are no longer supported platforms for Deep Security Manager. For a list of supported Deep Security Manager platforms, see "Deep Security Manager requirements" on page 384.

## Deep Security Manager 20 (long-term support release)

Release date: July 30, 2020

Build number: 20.0.60

### Action required if you use cross-account roles to add AWS accounts to Deep Security using the API /rest/cloudaccounts/aws

To better align with AWS best practices and improve AWS account security, Trend Micro have made a change to the process of adding a new AWS account into Deep Security using cross-account roles. Previously, when using a cross-account role for authentication, Deep Security required two pieces of information: a role ARN, and an external ID trusted by the role. This has now changed to a new process where Deep Security provides the external ID, and requires that the role provided has included this external ID in its IAM trust policy. This change provides stronger security in shared Deep Security environments, and ensures that strong external IDs are always used. For details on the new process of adding cross-account roles using manager-generated external ID, see "Add an AWS account using a cross-account role" on page 587.

**Action Required**:

Switch your external ID to a manager-generated one: "Update the external ID" on page 594.

If you are using cross-account roles with the API `/rest/cloudaccounts/aws`, see Action required if you are using cross-account roles with the API /rest/cloudaccounts/aws.

## New features

### Updated platform support

- Red Hat Enterprise Linux 8 (64-bit)
- Windows Server 2019 (64-bit)
- Oracle 18 database support
- Oracle 19c database support
- PostgreSQL 11 database support
- SQL Server 2019 database support

**Google Cloud Platform**: Google Cloud Platform (GCP) has been integrated with Deep Security. You can now view new GCP instances that come online or are removed, and which instances have protection. If you are using multiple clouds on-premise and in your data center, Deep Security can provide visibility for all of your environments. This feature is available for VMs that have Deep Security Agent 12.0 or later installed. For details, see "Add a Google Cloud Platform account" on page 614.

**End of Support for Red Hat Enterprise Linux 6**: Red Hat Enterprise Linux 6 is no longer a supported platform for Deep Security Manager. Upgrade your operating system.

### Improved Security

**Continuous Anti-Malware protection for NSX-T environments**: Deep Security Manager now sends guest VMs' Anti-Malware real-time configuration to all Deep Security Virtual Appliances that are under the same cluster. The effect is that the appliances can now maintain the protection of guest machines that use the Anti-Malware real-time feature during and after a vMotion migration from one ESXi host to another under the same cluster. This feature only applies to NSX-T environments.

**Agent version control**: Agent version control gives you and your security operations team control over the specific versions of the Deep Security Agent that can be used by features like deployment scripts and upgrade on activation. This provides increased control over the Deep Security Agent used in your environment. For more information, see "Configure agent version control" on page 1367.

### Improved management and quality

**Differentiate between Red Hat and CentOS platforms**: Deep Security Manager can distinguish between a Red Hat and CentOS platforms and operations.

**Visibility, Protection, and Management on Google Cloud Platform (GCP)**:

- VMs are organized into projects, which lets you easily see which GCP VMs are protected and which are not.
- Assign policies automatically based on the GCP Instance Labels, GCP Network Tags, and other instance attributes while auto-scaling up.
- Group related GCP instances in Smart Folders based on the GCP instance labels, GCP network tags, and other instance attributes to simplify the management.

**Automate Google and AWS accounts via REST API**: As you move to more automated deployments, having APIs to perform common tasks becomes a greater requirement Deep Security provides REST APIs to allow you to automate the adding of both AWS and Google Cloud accounts into Deep Security.

**Actionable recommendations for Anti-Malware issues**: In order for you to understand what is happening in the Anti-Malware system, many Anti-Malware events have been updated to provide more details on why a cancellation or failure has occurred. These events can occur for manual, quick, or scheduled Anti-Malware scans. The enhanced detail is provided in the events with Deep Security Manager as well as provided through SIEM or AWS SNS.

**Search Cloud Instance Metadata**: Added the ability to do a simple search or advanced search for Cloud Instance Metadata on the Computers page. This allows you to easily find workloads with specific labels, network tags, and more.

**Instance Metadata Service Version 2 (IMDSv2) support**: IMDSv2 is supported in this release. For details, see "How does Deep Security Agent use the Amazon Instance Metadata Service?" on page 1691

**Upgrade on activation**: Deep Security Manager now has options (**Administration > System Settings > Agents > Automatically upgrade Linux/Windows agents on activation**) that enable you to automatically upgrade the Deep Security Agent on Linux and Windows computers to the version specified in **Administration > System Settings > Updates > Software > Agent Version Control** when the agent is activated or reactivated. For details, refer to "Automatically upgrade agents on activation" on page 1388.

**Enhanced visibility of scheduled scan tasks and event based tasks**: Scheduled scan tasks and event-based tasks have been improved by providing scan visibility as well as specific reasons for each uncompleted Anti-Malware scan and recommended actions to resolve the scan.

**Reporting improvements to allow chargeback to cloud accounts**: The Security Module Usage Report now includes the Cloud Account ID (AWS Account ID, Azure Subscription ID or GCP Project ID) for protected instances.

**Multiple vCenters**: You can add multiple vCenters in the Deep Security Manager, and associate them to the same NSX-T Data Center. An overwrite warning message is displayed if you are using NSX Data Center for vSphere (NSX-V), which does not support the use of multiple vCenters, or if the NSX-T Manager has being registered with another Deep Security Manager cluster.

## Enhancements

UI improvements:

- Added file hash values to Anti-Malware events that are exported to CSV (**Events & Reports > Anti-Malware Export > Export to CSV**). SEG-61890/SF02510024/DS-53441</p>
- Updated the descriptions related to memory on the System Information page so they're more accurate and easier to understand.
- Improved the description of Behavior Monitoring events by including the reason the event occurred.
- Added a **GCP Network Tag** column to the **Computers** tab.
- Added GCP information such as Instance ID, Labels, Network tags, and more, to **Computer Editor > Overview > General**.
- Added the **Cloud Instance Metadata** field to the **Computers** page.
- Added a progress bar to **Administration > User Management > Roles > New > Computer Rights > Selected Computers** to indicate the status of the computers list that's loading.
- If there are a lot of agent events in a single heartbeat, they will be split into multiple "Event Retrieved" events.

- Enhanced the Relay management experience by providing possible solutions for the "Empty Relay Group Assigned" alert in the alert's description and removing the relay count for tenants that are using the Primary Tenant Relay Group.
- Added "Database Type" and "Database Server" columns to **Administration > Tenants**.
- Added the "Kernel Unsupported" system event to indicate if your computer has been upgraded to an unsupported kernel.
- Added a reason ID for the "Manual Malware Scan Cancellation complete" system event. The reason ID is displayed in REST API calls, SNS information and SIEM information.
- Added the "TrendMicroDsPacketData" field to Firewall events that are syslog forwarded via the Deep Security Manager.
- Added the **Validate the signature on the agent installer** checkbox on **Support > Deployment Scripts**. For more information, see "Check digital signatures on software packages" on page 494.
- Improved the "License Changed" event description by specifying if the plan ID is for Azure Marketplace billing.
- Renamed the **Service Token** setting to **Data Source GUID** on **Administration > System Settings > Managed Detection and Response**.
- Added a "Agent GUID" column to the **Computers** page so you can search computers by the Agent GUID.
- Included a search bar under **Administration > Updates > Software > Local**.
- When creating a smart folder, you can now select "Version" as the filter criteria to filter computers based on their Agent version.
- Added the ability to hide all empty AWS regions, VPCs, subnets, and directories, reducing clutter and increasing load speed on the **Computers** page.
- Aggregated identical agent events in a single heartbeat under a single event.
- Modernized the **Policies > Lists > Port Lists** page.
- When creating a smart folder, you can now select "Task(s)" as the filter criteria, which filters for values displayed in the "Task(s)" column on the Computers page. For example, you could create a smart folder that lists all computers that contain "Scheduled Malware Scan Pending (Offline)" as the task. Additionally, if you are using the Deep Security API to search for computers, you can now search on the value of the tasks/agentTasks and tasks/applianceTasks fields.
- Deep Security Manager now prevents you from importing duplicate Trusted Certificates.

- Redesigned the **Computers > Add Account** synchronization scheduling to handle many more connectors per tenant, reduce idle thread time, and sync connectors with invalid credentials less frequently.
- By default, the "My User Summary" widget on the Dashboard only displays information about sign-ins that have occurred within the last 24 hours.
- You can choose not to send packet data back to the Deep Security Manager by going to **Administration > Agents> Data Privacy** and selecting **No**.
- Deep Security Manager diagnostic packages have the ability to be encrypted. To encrypt your package and logs, go to **Administration > Create Diagnostic Package > Enable AES 256 encryption** and enter a password.

  > **Note:** Encrypted zips cannot be extracted using the default ZIP extraction tool available in Windows, it needs to be extracted by 3rd party tools like 7Zip, WinZip etc.

- Redacted potentially sensitive information from the diagnostic packages and logs.

Event-based tasks:

- Improved the capability of event-based tasks by adding support for GCP security automation with account name, labels, network tags and more in the task conditions.
- Introduced "Cloud Vendor" in the event-based tasks conditions in order to limit a task's scope for a specific public vendor (for example, AWS or GCP).

Commands:

- Added the following command:

  ```
  dsm_c -action changesetting -name
  com.trendmicro.ds.antimalware:settings.configuration.maxSelfExtractRTSc
  anSizeMB -value 512
  ```

  When Deep Security Agent could not determine the type of the target file, the scan engine loaded the file to memory to identify if it was a self-extract file. If there were many of these large files, the scan engine consumed lots of memory. Using the command above, the file-size limitation is set to 512MB for loading target files. When the file-size exceeds the set limitation, the scan engine will skip this process and scan the file directly.

  To implement this enhancement:

1. Run the command in Deep Security Manager to change the value in the database.
2. Send the policy to your target Deep Security Agent to deploy the setting.

- Added the ability for the Deep Security Administrator to hide unresolved recommendation scan results from the Intrusion Prevention, Integrity Monitoring and Log Inspection tab in the policy pages. To hide the unresolved recommendation scan results, use the following commands

  Intrusion Prevention:

  ```
  dsm_c -action changesetting -name
  com.trendmicro.ds.network:settings.configuration.showUnresolvedRecommen
  dationsInfoInPolicyPage -value false
  ```

  Integrity Monitoring:

  ```
  dsm_c -action changesetting -name
  com.trendmicro.ds.integrity:settings.configuration.showUnresolvedRecomm
  endationsInfoInPolicyPage -value false
  ```

  Log Inspection:

  ```
  dsm_c -action changesetting -name
  com.trendmicro.ds.loginspection:settings.configuration.showUnresolvedRe
  commendationsInfoInPolicyPage -value false
  ```

Enhanced scheduled tasks:

- **Task enabled** has been renamed to **Enable task** on the last screen of the Create Scheduled Task wizard
- Synchronize cloud account now indicates it only supports vCloud and Azure connectors
- Computer/group selection details now display in list view for Anti-Malware scans and Intrusion Prevention tasks

Virtual Appliance:

- Added the ability to auto-activate guest VMs protected by the Deep Security Virtual Appliance in an NSX-T environment.
- Added the "VMware NSX Policy Configuration Conflict" system event. This event is generated when Deep Security Manager detects that a NSX-T group is configured with different security policies for Endpoint Protection and Network Introspection (E-W).

- Updated Deep Security Manager to allow vCloud accounts to be added even if the virtual machine hardware information is missing.
- When you upgrade the Deep Security Virtual Appliance SVM in NSX-T Manager, Deep Security Manager will now detect that a new SVM is now protecting guest VMs, and will auto-activate those VMs after the upgrade.
- Upgraded the vCloud Connector in Deep Security Manager supports vCloud 9.7 and vCloud 10.0.
- Added the ability to sync Deep Security Manager policies to NSX-T environments.
- Improved the experience when deleting vCenter Connectors with NSX-T Manager. Previously, you had to manually remove the NSX-T component as a service profile, endpoint rules and service deployments, or the vCenter deletion would fail.
- Deep Security Manager can now connect to NSX-T Data Center using LDAP account credentials. Previously, only local NSX-T account credentials could be used.

Other:

- When Anti-Malware actions fail, the results will be displayed in the Syslog result field.

## Resolved issues

- When the **Hide Unlicensed modules** option was selected on **Administration > User Management > Users > customer's current account > Settings**, all of the modules were hidden. SEG-77037/03228448/DS-51202
- When the **Alert on any Computer** action was selected for Intrusion Prevention, Firewall, Integrity Monitoring or Log Inspection rules, the computers were not automatically updated with the new policy. SEG-66986/SF02684105/DSSEG-5201
- Sometimes, you couldn't edit a smart folder. SEG-74078/SF03120830/DSSEG-5450
- When the **Alert on any Computer** action was selected for Intrusion Prevention, Firewall, Integrity Monitoring or Log Inspection rules, the computers were not automatically updated with the new policy. DS-50216/SEG-77260
- Anti-Malware events that were marked as "Pass" were not properly counted on the dashboard or under Anti-Malware events. DS-49364/SEG-70872
- When an agent activated with no AWS metadata but then provided it on a later heartbeat, the cloud provider was not updated, which caused the computer to never be rehomed properly. DS-50713/SEG-77150

- When you did an advanced search on the Computers page for **Status Light > Equals > Managed [Green]**, then selected **Export to CSV**, the CSV file did not contain the listed computers. DS-49936/SEG-74140
- Azure accounts could not be added in Azure Government regions because the login endpoint was changed. This only applies to Azure Marketplace deployments. DS-52399
- For tenants, the Security Module Usage Report was only visible if you had access to the default Full Access role. (SEG-70494/SF02940195/DS-47492)
- The sign-up page did not render properly in Internet Explorer. (SEG-73072/SF03075345/DS-48944)
- When several emails with large bodies were queued, they were loaded all at once instead of in batches, which caused a large amount of memory to be used. (SEG-71863/SF03024164/DS-49833)
- When the "Untagged" filter was selected on the dashboard, some widgets continued to display tagged items. (SEG-63290/SF02585007/DS-43795)
- Tenants in a multi-tenant setup could move their relays to the primary tenant relay group. This would cause the relays to disappear from their Relay Management page. Tenants are now prevented from moving their relays to the primary tenant relay group. (SEG-57715/02322762/DS-47509)
- Performance issues occurred when there were 1,000s of requests to download the same SVG file because the file was not cached. (SEG-64280/DS-45002)
- AIA hosts with the same Virtual UUID fail when "Activate a new Computer with the same name" was selected. (SEG-66346/02725330/DS-45423)
- In some multi-tenant environments, you could not log in as a tenant. For more information, see Known issues in Deep Security 9.0. (SF02873892/SEG-68674/DS-46391)
- When Integrity Monitoring was enabled but Anti-Malware was disabled, a warning message would appear indicating "Security Update: Pattern Update on Agents/Appliance Failed". (SEG-68454/SEG-67859/DS-32205)
- In the **Malware Scan** configurations window, the content of the **Advanced** tab was displayed in the **General** tab. (SEG-64701/SF02657864/DS-44176)
- Deep Security Manager had issues loading the computers trees on some pages when there were a lot of computers and folders. (SEG-58089/SF02345427/DS-44424)
- AWS connectors sometimes failed to synchronize. (SEG-66472/DS-45029)
- The column names in the CSV output of the "Security Module Usage Report" were partially misaligned with the data columns.(SEG-66717/SF02619240/DS-45130)

- In the Malware Scan Configuration window (**Computers/Policies > Anti-Malware > General > Manual Scan > Edit > Advanced** and select **Scan Compressed File**) the **Maximum number of files to extract** setting could not be set to 0, meaning unlimited. (SEG-65997/02685854/DS-45081)
- Deep Security Manager with PostgreSQL sometimes stopped forwarding events to AWS SNS. (SEG-67362/SF02798561/DS-45594)
- When Deep Security Manager was deployed in an environment with a large number of hosts and protection rules, the manager would sometimes load data for all hosts, even if the user only requested data from some of the hosts. (SF02552257/SEG-62563/DS-43188)
- When booting up, Deep Security Manager validates the database schema of the events tables. Logs always said that the schema was updated, even if no update was actually required. (DS-43196)
- Active Directory synchronization sometimes would not finish. (SEG-52485/DS-38203)
- When a custom Anti-Evasion posture was selected in a parent policy (in the policy editor **Settings > Advanced > Network Engine Settings > Anti-Evasion Posture > select 'Custom'**), that setting did not appear in the child policies. (SF02434648/SEG-60410/DS-41597)
- On Linux systems, the default maximum number of the concurrent opened files did not meet Deep Security Manager's needs, resulting in the manager failing to acquire file handles. As a result, features in Deep Security Manager failed randomly and a "Too many open files" message appeared in logs. (SEG-59895/DS-43192)
- The "Activity Overview" widget sometime displayed the incorrect database size. (SF02449882/SEG-63362/DS-43946)
- When sorting the "Alert Configuration" page by the "ON" column, the number of alerts was sometimes incorrect. (SF02578797/SEG-63560/DS-43685)
- Certain smart folder search criteria caused an IllegalStateException error. (SF02436019/SEG-60330/DS-41369)
- The memory usage percentage display on the "Manager Node Status" dashboard widget did not match the last recorded system memory usage percentage. (SF02218013/SEG-55761/DS-39149)
- In Deep Security Manager, under **Policies > Intrusion Prevention Rules > Application Types > (select DNS client) > Properties > General**, the Port setting would change to "Any" after any updates to the port list. (SEG-55634/DS-39444)
- Reconnaissance alerts could not be disabled because the option was not available. (SEG-49907/DS-35122)

- Some Azure Virtual Machine types categorized incorrectly. (SF01885266/SEG-48561/DS-33951)
- Users of AWS Marketplace metered-billing would see an error reported in system events when the billing job was processed. (SF1899351/SEG-48580/DS-33955)
- Integrity Monitoring detailed change and recommendation reports was not running against smart folders. (SF2056260/SEG-51781/DS-35886)
- When the Computers page was grouped by status, it sometimes didn't display the correct total number of computers for each group. (SF01655622/SEG-44858/DS-37769)
- When Deep Security Manager was connected to both a case-sensitive Microsoft SQL database and VMware NSX, the Deep Security Manager upgrade readiness check would sometimes fail and block the upgrade. (SF02060051/SEG-52044/DS-38405)
- Scheduled task scans could be initiated by a user for computer groups that they do not have access to in their roles, which caused an error to occur. (SF02119582/SEG-53275/DS-38892)
- Deep Security Agent sometimes went offline when duplicate virtual UUIDs were stored in the database. (SF01722554/SEG-41425/DS-39272)
- False alerts regarding the license expiration were occasionally raised. (SF01484611/SEG-41437/DS-33831)
- Using a local key secret containing the $ symbol stopped the upgrade or fresh install of Deep Security Manager. (SF02013831/SEG-57243/DS-39526)
- Deep Security used an open source library called SIGAR that is no longer maintained or supported. This can cause applications to crash and other unintended issues in the future. (SF02184158/SEG-54629/DS-39394)
- When an invalid or unresolvable SNMP server name was configured in **Administration > System Settings > Event Forwarding > SNMP**, it caused SIEM & SNS to also fail. (SF02339427/SEG-57996/DS-39865)
- Forwarding events "via Deep Security Manager" with SIEM event forwarding would not work if the Deep Security Manager hostname was not obtained through DNS resolution. (SEG-50655/DS-37374)
- The events exported via AWS SNS did not contain the HostOwnerID, which corresponds to the AWS Account ID. (SF02420860/SEG-59870/DS-41089)
- In the computer or policy editor in Deep Security Manager, under **Anti-Malware > General > Real-Time Scan > Schedule > Edit**, the **Assigned To** tab was sometimes empty, even

when the schedule was assigned correctly to computers and policies. (SF02374723/SEG-58761/DS-41036)

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Responses. (DS-45446/DS-44955/DS-43627/DS-28754/DS-32322/DS-33833/DS-26068)

Highest Common Vulnerability Scoring System (CVSS) score: 9.8

Highest Severity: Critical

- Updated the JRE to the latest Java Update (8.0.241/8.43.0.6).
- Updated third-party libraries used by Deep Security Manager. (DS-24214)
- Upgraded Apache Tomcat to 8.5.53. (VRTS-4652)

### Known issues

- If you are using an Oracle database, this upgrade will take longer than usual due to a database schema change. For more information about Deep Security Manager upgrades, see Upgrade Deep Security Manager.
- When a new Deep Security Virtual Appliance is deployed, the VM name is displayed as "Trend Micro_Custom - <version>", if you're using a local web server to store the Deep Security Virtual Appliance software package. This has no effect on the integrity of the appliance.
- Due to issues discovered during internal testing with SQL 2008, Trend Micro now blocks upgrades to Deep Security feature release when SQL 2008 is the Deep Security Manager database. Microsoft SQL Server 2008 is no longer supported by Microsoft and therefore is no longer being tested and supported for use as a database for the latest releases of Deep Security Manager. For more information from Microsoft, see End of support for SQL Server 2008 and SQL Server 2008 R2. For the full list of databases supported for use with Deep Security Manager, see "Deep Security Manager requirements" on page 384 system requirements. (DS-36715)

## What's new in Deep Security Agent?

Linux

## Deep Security Agent - 20.0.3-860 (20 LTS Update 2026-01-21)

Release date: January 21, 2026

Build number: 20.0.3-860

### New features

**Endpoint Event Viewer**: Access Endpoint Event Viewer to view all security and system events across managed computers with filtering by period, severity, event origin, and action. This is only supported for Trend Vision One - Server & Workload Protection.

### Enhancements

- During periods of high activity, Deep Security Agent can now discard non-critical background events to improve system stability without impacting security. PCT-83049/DSA-14187

### Resolved issues

- Deep Security Agent crashed when syslog hostnames were longer than 64 characters. PCT-87531/DSA-14252
- When Web Reputation Service was enabled, system memory usage continuously increased. PCT-80352/DSA-13866
- Deep Security Agent sometimes crashed when processing HTTP/2 packets that were formatted differently from what the agent expected. PCT-85552/DSA-13755
- After Deep Security Agent restarted, Intrusion Prevention Detection sometimes stopped working. PCT-82352/DSA-13755

## Deep Security Agent - 20.0.2-29810 (20 LTS Update 2025-12-24)

Release date: December 24, 2025

Build number: 20.0.2-29810

### Resolved issues

- Application Control failed to retain the inventory when a ruleset update was applied. For details, see Trend Vision One™ Server & Workload Protection, Cloud One Workload Security, and Deep Security Application Control may fail to save the inventory when updating rules. DSA-13750

## Deep Security Agent - 20.0.2-29760 (20 LTS Update 2025-12-09)

Release date: December 09, 2025

Build number: 20.0.2-29760

### New features

**Ubuntu 24.04 (AWS Arm-based Graviton 2) support**: Deep Security Agent 20.0.2-29760 or later supports Ubuntu 24.04 (AWS Arm-based Graviton 2). This requires Deep Security Manager 20.0.1123 or later.

### Enhancements

- Firewall and Intrusion Prevention System events now display process and user info if that data is available. This is being rolled out gradually to all customers. DSA-13741
- Strong cipher (`app.relay.strongciphers=true`) and minimum Transport Layer Security (TLS) version (`app.relay.restrictRelayMinimumTLSProtocol=TLSv1.2`) can now be set in the Deep Security Agent configuration file for agents using Deep Security Relay. DSA-2163
- Advanced Threat Scan Engine has been updated to version 25.560. DSA-12306

### Resolved issues

- Deep Security Agent was unable to start on some Red Hat Package Manager (RPM)-based Linux distributions using a newer RPM library (rpm-4.16.1.3-39.el9.x86_64 or above / rpm-4.19.1.1-20.el10.x86_64 or above). For more details, see Unable to start Trend Micro™ Deep Security™ Agent (DSA) and Trend Vision One™ XDR for Endpoints after updating Red Hat Enterprise Linux (RHEL) version 9 or 10 system package. PCT-84361/V1E-116239

- Uploading logs using the File Collection or Custom Script functions failed on some systems. This issue only affected Trend Vision One. V1E-115291
- Application Control blocked some applications from being executed through a shell when they should have been allowed. PCT-83681
- After upgrading to Deep Security Agent 20.0.2.22850 or 20.0.2.26670, the enhanced recommendation scan would disable and not automatically re-enable. When this issue occurred, the system reverted to using classic recommendation scan after 36 hours to ensure continued functionality. This issue only affected Endpoint & Workload Security. WS-13982

## Security updates

This release contains updates to third-party libraries. DSA-13181/DSA-13204

## Known issues

- Application Control fails to retain the AC inventory when a ruleset update is applied.

  **Recommended actions:**
  - If you have agents running Application Control that have not been upgraded to version 20.0.2-29760, do not upgrade these agents.
  - If you have agents running Application Control that have already been upgraded to version 20.0.2-29760, perform the following actions in order:
    a. Disable Application Control's block mode for all 20.0.2-29760 agents that have Application Control enabled.
    b. Downgrade all agents that have Application Control enabled to a previous agent version.
    c. Re-enable Application Control block mode for these agents, if desired.

  For more information see Trend Vision One™ Server & Workload Protection, Cloud One Workload Security, and Deep Security Application Control may fail to save the inventory when updating rules. DSA-13750

## Deep Security Agent - 20.0.2-26670 (20 LTS Update 2025-11-12)

Release date: November 12, 2025

Build number: 20.0.2-26670

### New features

**User-based Firewall**: Firewall rules can now be configured based on user account. This feature is being rolled out gradually to all customers.

**Enhanced HTTP/2 support**: The Intrusion Prevention System engine now supports inbound HTTP/2 connections. This feature will be rolled out gradually through backend updates to ensure stability and performance enhancements. (This release also includes fixes aimed at improving HTTP/2 handling and security. PCT-77306/DSA-13105)

**Rocky Linux 10 support**: Deep Security Agent 20.0.2-26670 and later now supports Rocky Linux 10, including SELinux, Secure Boot, and FIPS mode support.

**Debian Linux 13 support**: Deep Security Agent 20.0.2-26670 and later supports Debian Linux 13 including Secure Boot support and FIPS mode support. This requires Deep Security Manager 20.0.1112 or later.

**Red Hat Enterprise Linux 8 (64-bit IBM Z) Anti-Malware on-demand scan support:**: Deep Security Agent 20.0.2-26670 and later supports only the Anti-Malware on-demand scan for Red Hat Enterprise Linux 8 (64-bit IBM Z). This requires Deep Security Manager 20.0.1112 or later. Security updates are not provided for this platform.

**Red Hat Enterprise Linux 9 (64-bit IBM Z) Anti-Malware on-demand scan support:**: Deep Security Agent 20.0.2-26670 and later supports only the Anti-Malware on-demand scan for Red Hat Enterprise Linux 8 (64-bit IBM Z). This requires Deep Security Manager 20.0.1112 or later. Security updates are not provided for this platform.

### Resolved issues

- Files that were unscannable using `dsa_scan` were being automatically classified as infected. DSA-10037
- Advanced TLS Traffic Inspection caused Docker container crashes in environments running Linux Kernel version 6.11 to 6.14. DSA-13372

### Known issues

- Advanced TLS Traffic Inspection sometimes causes malfunctions in Docker containers running in Linux Kernel version 6.11 to 6.14. DSA-13371

## Deep Security Agent - 20.0.2-22850 (20 LTS Update 2025-10-08)

Release date: October 08, 2025

Build number: 20.0.2-22850

### Resolved issues

- A network device issue caused some systems to crash. PCT-74972/DSA-12698
- Multiple processes updating the `dsa_filter` driver at the same time sometimes caused a system crash. PCT-76239/DSA-12697

## Deep Security Agent - 20.0.2-20480 (20 LTS Update 2025-09-17)

Release date: September 17, 2025

Build number: 20.0.2-20480

### New features

**Oracle Linux 10**: Deep Security Agent 20.0.2-20480 or later now supports Oracle Linux 10, including SELinux, Secure Boot, and FIPS mode support. This requires Deep Security Manager 20.0.1081 or later.

### Enhancements

- Log Inspection now supports glob character in directory names. PCT-8309

### Resolved issues

- Deep Security Agent running with Application Control enabled led to a memory leak on some systems. DSA-12148
- Using Advanced TLS Traffic Inspection in Deep Security Agent caused high CPU usage when certain third-party software was also running on a system. PCT-55552/DSA-11921
- Running the podman system service interfered with Deep Security Agent functionality on some systems. (When getting podman information using the command line, the agent is unaffected.) PCT-16544/PCT-47917/PCT-63773/DSA-4452

## Deep Security Agent - 20.0.2-17500 (20 LTS Update 2025-08-13)

Release date: August 13, 2025

Build number: 20.0.2-17500

### Enhancements

- All `Agent-PGPCore*` and `Agent-Core*` files are now removed from the app folder after completing a Deep Security Agent upgrade. DSA-10996

### Resolved issues

- Integrity check of Kernel Support Package files sometimes failed if multiple copies were downloaded at nearly the same time. PCT-66493/DSA-11495
- Deep Security Agent sometimes crashed when establishing a heartbeat connection. PCT-66595/DSA-11386
- Deep Security Agent was sometimes unable to install a Kernel Support Package (KSP) if its Linux kernel version was no longer supported by the latest KSP imported to Deep Security Manager. PCT-66447/DSA-11366

## Deep Security Agent - 20.0.2-14431 (20 LTS Update 2025-07-09)

Release date: July 09, 2025

Build number: 20.0.2-14431

### New features

**Red Hat Enterprise Linux 10**: Deep Security Agent 20.0.2.14431 or later now supports Red Hat Enterprise Linux 10, including SELinux, Secure Boot, and FIPS mode support. This requires Deep Security Manager 20.0.1054 or later.

### Enhancements

- When Advanced TLS Traffic Inspection is enabled, Deep Security Agent now injects packets to speed up the connection as long that connection is not blocked. PCT-63207/DSA-10919

### Resolved issues

- The Intrusion Prevention System, Web Reputation Service, and Firewall protection modules displayed an offline status even when disabled. PCT-66070/PCT-66493/PCT-67224/DSA-11160
- On demand scans could not be started manually until an automatic scan had been triggered, after either an activation or a restart of Deep Security Agent. WS-12581
- Enhanced Recommendation Scan failed if unexpected process values were encountered. WS-12572
- A file descriptor leak sometimes caused the engines for Anti-Malware, Web Reputation Service, and Integrity Monitoring to go offline. PCT-70783/DSA-11618

## Deep Security Agent - 20.0.2-12010 (20 LTS Update 2025-06-11)

Release date: June 11, 2025

Build number: 20.0.2-12010

### Enhancements

- Enabled by default, Web Reputation Service now uses Server Name Indication (SNI) queries when determining the risk level of a website.
- Activity Monitoring now supports JavaServer Page (JSP) files. V1E-54751

### Resolved issues

- Deep Security Agent sometimes crashed during SSL handshake. PCT-55526/DSA-9902
- With Vision One Endpoint Security Version Control Policy enabled, Deep Security Agent protection module deployment sometimes failed, resulting in a 5102 "No such file or directory" error. DSA-10398

### Security updates

This release contains updates to third-party libraries. DSA-10530

## Deep Security Agent - 20.0.2-9811 (20 LTS Update 2025-05-14)

Release date: May 14, 2025

Build number: 20.0.2-9811

### New features

**Red Hat Enterprise Linux 9 (AWS Arm-based Graviton 2)**: Deep Security Agent 20.0.2-9810 or later now supports Red Hat Enterprise Linux 9 (AWS Arm-based Graviton 2), including SELinux support. This requires Deep Security Manager 20.0.1047 or later.

### Enhancements

Web Reputation Service now points to a 403 Forbidden rather than a 200 OK page when blocking an http proxy connection to a suspicious or malicious site. PTC-60576/DSA-10325

### Resolved issues

- Deep Security Agent configurations using advanced TLS caused some systems to freeze. PCT-63207/DSA-10380
- The URL column for **Web Reputation Events** was sometimes missing information. PCT-60576/DSA-10090
- With Intrusion Prevention System enabled, some systems received a UBSAN out of range error for an operation that was safely in range. PCT-63329/DSA-10353
- Improved the handling of Deep Security Agent diagnostic packages to avoid including some incomplete data. DSA-10270
- Deep Security Agent was sometimes unable to download kernel support packages from Deep Security Relay when Kernel Package Update was configured to No. For more details, see Deep Security Agent (DSA) reports "Protection Module Deployment Failed (Event ID 5102)" PCT-61830/DSA-10249
- The operating system was unable to load Deep Security Agent Anti-Malware kernel modules due to incompatible environment tools. PCT-34454/PCT-41680/PCT-46866/DSA-9349
- Offline Scheduled Scan sometimes used the Server & Workload Protection time zone when it should have used the Deep Security Agent time zone, causing Weekly and Daily scans to trigger at the wrong time, and causing high CPU usage for Monthly scans when triggered on the last day of a month. PCT-55169/DSA-9303
- If a security update failed, Deep Security Agent sometimes stopped multiple system services. PCT-62050/DSA-10168

## Deep Security Agent - 20.0.2-7600 (20 LTS Update 2025-04-16)

Release date: April 16, 2025

Build number: 20.0.2-7600

### New features

**Dynamic Intelligence Mode**: Dynamic Intelligence Mode enables Deep Security Agent to automatically adjust monitoring levels to optimize security responses based on detected threats, user behavior, and system configuration.

### Resolved issues

- Updating the Kernel Support Package stopped Web Reputation Service from working and caused Intrusion Prevention System to encounter a rules compilation failure. DSA-6398
- The Anti-Malware Engine sometimes crashed after a pattern update. DSA-9208
- Scheduled scans sometimes triggered on the wrong date or at the wrong time when "Enable agent to trigger scheduled scans for malware" was enabled. PCT-21726/DSA-6938

## Deep Security Agent - 20.0.2-4961 (20 LTS Update 2025-03-12)

Release date: March 12, 2025

Build number: 20.0.2-4961

### New features

**Version Control Policy**: Deep Security Agent now supports Version Control Policy advanced settings, which allows Trend Vision One version control policies to manage kernel support updates for any endpoint with the Trend Micro Endpoint Basecamp (XBC) agent installed. For more information, see Version Control Policies.

This is currently in pre-release, and is only supported for Trend Vision One - Server & Workload Protection. DSA-9384

### Enhancements

- The `dsa_scan` command now includes a `scanLargeFile` option for managing larger files. DSA-8825

### Resolved issues

- SAP Scanner sometimes incorrectly classified CSV files if they were larger than 4096 bytes. PCT-51974/DSA-9139

- Deep Security Agent experienced reduced performance when using TLS 1.3 with some network protocols. DSA-6959

### Known issues

- Updating the Kernel Support Package stops Web Reputation Service from working and causes Intrusion Prevention System to encounter a rules compilation failure. For more information and details on a workaround for this issue, see Web Reputation Service (WRS) not working and Intrusion Prevention System (IPS) rules compilation failure in Trend Micro™ Deep Security™. DSA-6398

## Deep Security Agent - 20.0.2-1390 (20 LTS Update 2025-01-15)

Release date: January 15, 2025

Build number: 20.0.2-1390

### New features

**User-based Firewall events**: Firewall events now include username whenever possible. This feature is in preview and is only available to certain customers at this time.

### Enhancements

- Deep Security Agent now queues packets to handle them in sequence, improving performance. DSA-6916

### Resolved issues

- Deep Security Agent sometimes had connectivity issues when Advanced TLS Traffic Inspection was enabled. DSA-8577

### Security updates

This release contains updates to third-party libraries. DSA-7696/DSA-7697/DSA-8042

## Deep Security Agent - 20.0.1-25771 (20 LTS Update 2024-12-10)

Release date: December 10, 2024

Build number: 20.0.1-25771

### New features

**Version Control Policy**: Deep Security Agent now supports Version Control Policy, which allows Trend Vision One version control policies to manage agent and component updates for any endpoint with the Trend Micro Endpoint Basecamp (XBC) agent installed. For more information, see Version Control Policies. This is currently in pre-release, and is only supported for Trend Vision One - Server & Workload Protection.

**Quarantine auto-cleanup**: Deep Security Agent will now automatically purge parts of files in the quarantine folder if its disk space usage exceeds the maximum amount. Max disk space usage (1024 MB by default) is configurable from **Computer** (or **Policy) > Anti-Malware > Advanced > Identified Files**. This feature is only available for Cloud One Workload Security at this time.

### Enhancements

- Deep Security Agent 20.0.1.25771 or later supports FIPS mode for Ubuntu 22.04. DSA-7699
- Deep Security Agent now supports Advanced TLS Traffic Inspection for Intrusion Prevention on Apache Tomcat servers running OpenJDK 8 on 64-bit Linux operating systems. DSA-8244
- Deep Security SAP Scanner can now report results to SAP applications when it identifies password-protected compressed files attached to an email in Microsoft Outlook Item (MSG) format. SF07873657/PCT-23367/DSA-7716
- Anti-Malware's Behavior Monitoring detection level and prevention level can now be configured. DSA-6796
- Deep Security Agent now detects if its relay proxy is Trend Vision One Service Gateway Forward Proxy Service, and uses the Service Gateway domain allow list to decide whether the connection should use the relay proxy or not. SF07267852/PCT-29311/DSA-6274

- Trend Cloud One - Endpoint & Workload Security can now install Trend Vision One Endpoint Security agent via Deep Security Agent. DSA-7532
- Deep Security Agent now supports additional options to fine-tune detection sensitivity for Anti-Malware, Behavior Monitoring, and Predictive Machine Learning for real-time scan. This enhancement is only available in Trend Cloud One - Endpoint & Workload Security. DSA-6062
- Improved detection and protection against malicious processes that can be launched through a memory file descriptor (memfd). DSA-6009

### Resolved issues

- Events including packet data were being logged with an incorrect packet size. PCT-45556/DSA-8074
- Some systems with Anti-Malware enabled encountered a memory leak. DSA-8243
- Some systems encountered a memory issue that caused Anti-Malware to stop working. PCT-46330/DSA-8156
- Deep Security SAP Scanner would incorrectly report scan failures when two or more files with the same content were included in a compressed file. PCT-38781/DSA-7324
- Deep Security Agent had higher than usual CPU usage if Integrity Monitoring was disabled following an Integrity Monitoring scan. SF07991055/PCT-31459/DSA-6195
- Rebooting caused some systems to hang if agent self-protection was enabled. PCT-27574/PCT-29800/DSA-6007
- When SAP was enabled, duplicate exclude paths were sometimes created and would remain even after SAP was disabled. DSA-7595

### Security updates

This release contains updates to third-party libraries. DSA-7124

## Deep Security Agent - 20.0.1-23340 (20 LTS Update 2024-11-13)

Release date: November 13, 2024

Build number: 20.0.1-23340

### Enhancements

- Deep Security Agent 20.0.1-23340 or later adds additional support for Red Hat Enterprise Linux 9 (PowerPC little-endian). For details, see supported features by platform for Deep Security 20 LTS or Trend Cloud One - Endpoint & Workload Security. DSA-7234
- Web Reputation Service can now use Server Name Indication (SNI) queries when determining the risk level of a website. DSA-7314
- Connection timeout for the Predictive Machine Learning service was extended to nine seconds to reduce the number of "Census, Good File Reputation, and Predictive Machine Learning Service Disconnected" events (Event ID 945). DSA-5321

### Resolved issues

- When Application Control was operating in block mode, files in some directories were being allowed to run when they should have been blocked. PCT-38516/DSA-7613
- When Deep Security Agent had Advanced TLS Traffic Inspection enabled using Transport Layer Security (TLS) 1.3, some systems encountered a kernel panic crash. PCT-43009/DSA-7787
- Some systems running Deep Security Agent encountered an operating system crash caused by retrieving an invalid memory address. PCT-33865/DSA-6335

## Deep Security Agent - 20.0.1-21510 (20 LTS Update 2024-10-16)

Release date: October 16, 2024

Build number: 20.0.1-21510

### New features

**Red Hat Enterprise Linux 9 (PowerPC little-endian) support**: Deep Security Agent 20.0.1-21510 or later supports Anti-Malware, and SAP Scanner for Red Hat Enterprise

Linux 9 (PowerPC little-endian). This requires Deep Security Manager 20.0.979 or later.

### Enhancements

- Advanced Threat Scan Engine has been updated to version 24.5. DSA-7354
- Deep Security Agent now supports wildcard `*` use in Anti-Malware process path exclusions, which is being rolled out gradually for Linux platforms. DSA-6384

### Resolved issues

- High CPU usage would occur when both Application Control and FIPS were enabled. DSA-6842
- When the SAP Scanner library re-established connections to Deep Security Agent, the scan requests sent from the SAP Scanner library would sometimes be rejected. SF08196066/PCT-34824/DSA-7608
- Deep Security SAP Scanner would sometimes crash when scanning for files in certain formats, like CSV. PCT-41353/DSA-7609

## Deep Security Agent - 20.0.1-19250 (20 LTS Update 2024-09-18)

Release date: September 18, 2024

Build number: 20.0.1-19250

### New features

**Ubuntu 24.04 support**: Deep Security Agent 20.0.1-19250 or later supports Ubuntu 24.04 including Secure Boot support. This requires Deep Security Manager 20.0.954 or later.

### Enhancements

- Updated Deep Security Agent to improve compatibility with older versions of the SAP Scanner. SF08196066/PCT-34824/DSA-6819
- Deep Security Agent now supports the Alibaba Cloud connector type. DSA-6018

### Resolved issues

- Deep Security Agent caused high CPU usage on systems with both Application Control and FIPS enabled. DSA-6842
- Anti-Malware engine did not start correctly during Deep Security Agent startup on systems using XDR Endpoint Sensor. DSA-7158
- An issue detecting the operating system information sometimes prevented Deep Security Agent from installing on Rocky Linux 9. PCT-26151/DSA-5630

### Security updates

This release contains updates to third-party libraries. DSA-6156/DSA-6942

## Deep Security Agent - 20.0.1-17380 (20 LTS Update 2024-08-21)

Release date: August 21, 2024

Build number: 20.0.1-17380

### Enhancements

- Web Reputation Service "Smart Protection Server Disconnected" events now include FQDN or IP address information in the description field. DSA-5408
- SAP Scanner now classifies Society for Worldwide Interbank Financial Telecommunication (SWIFT) messages as text files. SF07895338/PCT-24359/DSA-5790
- SAP Scanner now associates JavaScript with compatible file extensions. For details, see Supported MIME types. SF08102626/PCT-31518/DSA-6192

### Resolved issues

- Anti-Malware engine sometimes crashed. DSA-5536
- SAP Scanner incorrectly classified valid CSV files if the data was formatted on a single line. SF07967718/PCT-26844/DSA-6102

- SAP Scanner sometimes incorrectly identified image files as ASP scripts. SF07764878/PCT-20406/DSA-6122
- Kernel Support Package (KSP) did not reload automatically after being imported. DSA-6159
- Deep Security Agent could not load the policy if some policy configuration fields contained curly brackets. DSA-6189
- Deep Security Agent failed to activate if the hostname contained non-ASCII characters. PCT-32214/DSA-6268
- Deep Security Agent sometimes failed to shut down completely if integrating with Trend Micro Endpoint Basecamp (XBC) agent. SF08143019/PCT-32915/DSA-6347
- Deep Security Agent incorrectly created a temporary directory named `/opt/ds_agent@tmp` during installation. DSA-6412
- When Intrusion Prevention was enabled for Deep Security Agent, some third-party applications had connectivity issues if they were reusing a source port. SF07685331/PCT-20541/DSA-5596
- When Anti-Malware accessed files on a Cluster Shared Volume, the Hyper-V host crashed. SF05713918/SF05850687/SF07038125/SEG-146660/SEG-148664/SEG-186072/PCT-41910/PCT-5467/DSSEG-7664

### Known issues

- Deep Security Agent Application Control causes high CPU usage. PCT-36414
- Anti-Malware engine is not starting correctly during Deep Security Agent startup on systems using XDR Endpoint Sensor. DSA-7158

## Deep Security Agent - 20.0.1-14610 (20 LTS Update 2024-07-17)

Release date: July 17, 2024

Build number: 20.0.1-14610

### New features

**SUSE Linux Enterprise Server 15 (AWS Arm-based Graviton 2) support**: Deep Security Agent 20.0.1-14610 or later supports SUSE Linux Enterprise Server 15 (AWS Arm-based Graviton 2). This requires Deep Security Manager 20.0.926 or later. DSA-4836

### Enhancements

- SAP Scanner now associates the following MIME types with compatible file extensions. For details, see Integrate with SAP NetWeaver.
  - TrueType Font (TTF). SF08102626/PCT-31518/DSA-6049
  - Java Archive (JAR). SF08102626/PCT-31518/DSA-6044
  - Apple QuickTime File Format (QTFF). SF07967718/SF07840151/PCT-22825/PCT-26844/DSA-5887/DSA-5567
  - Microsoft Advanced Systems Format (ASF). SF07967718/PCT-26844/DSA-5886

### Resolved issues

- Deep Security Agent still tried to test connections for Service Gateways. DSA-5814
- A Deep Security Agent restart sometimes caused Application Control to report drift events. SF07813110/PCT-25731/DSA-5798
- Deep Security Agent was only able to use the primary IP address for Service Gateway. DSA-4513
- Integrity Monitoring real-time scans sometimes failed to generate events. SF07269768/PCT-21721/DSA-5877
- Switching from User Mode to Kernel Mode (**Computer** or **Policy > System > General > Choose whether to use Drivers for System Protection**) sometimes caused Deep Security Agent to lose real-time Anti-Malware protection. DSA-6090

## Deep Security Agent - 20.0.1-12510 (20 LTS Update 2024-06-19)

Release date: June 19, 2024

Build number: 20.0.1-12510

## Enhancements

- Deep Security Agent 20.0.1-12510 or later adds additional support (including SAP Scanner) for Red Hat Enterprise Linux 8.6 (PowerPC little-endian). For details, see supported features by platform for Deep Security 20 LTS or Trend Cloud One - Endpoint & Workload Security. DSA-4835
- Advanced TLS Traffic Inspection now supports separate configurations for "Inspect Inbound TLS/SSL Traffic" and "Inspect Outbound TLS/SSL Traffic". For detailed configuration steps, see https://help.deepsecurity.trendmicro.com/20_0/on-premise/intrusion-prevention-ssl-traffic.html#EnableTLS.

## Resolved issues

- When Anti-Malware had only basic functions, some systems would hang. DSA-4821
- When Anti-Malware was enabled, Deep Security Agent sometimes failed to shut down completely. PCT-26090/DSA-5492

## Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-12022/DSA-5484

Highest Common Vulnerability Scoring System (CVSS) score: 5.5

Highest severity: Medium

## Known issues

- There is a performance impact when **Inspect Inbound TLS/SSL Traffic** and **Inspect Outbound TLS/SSL Traffic** are enabled at the same time in Advanced TLS Inspection settings. For details, see Performance impact of bi-directional TLS inspection in Deep Security. DSA-5959

- Switching from User Mode to Kernel Mode (**Computer** or **Policy > System > General > Choose whether to use Drivers for System Protection**) sometimes causes Deep Security Agent to lose real-time Anti-Malware protection. DSA-6090
- Switching to User Mode (**Computer** or **Policy > System > General > Choose whether to use Drivers for System Protection**) sometimes causes Deep Security Agent to lose real-time Anti-Malware protection. DSA-6104

## Deep Security Agent - 20.0.1-9400 (20 LTS Update 2024-05-16)

Release date: May 16, 2024

Build number: 20.0.1-9400

### New features

**User mode solution**: User mode can now be enabled from the Trend Cloud One - Endpoint & Workload Security or Deep Security Manager UI to provide event generation and protection through basic functions for Anti-Malware on systems that lack kernel support.

### Enhancements

- SAP Scanner now supports the `SCANLOGPATH` parameter. For details, see Integrate with SAP NetWeaver. PCT-21958/DSA-4924
- Updated Deep Security Agent to improve the priority for configurations using a proxy. DSA-4817/PCT-21750
- Deep Security Agent can now retrieve Service Gateway settings from the Trend Micro Endpoint Basecamp (XBC) agent. DSA-4841/V1E-13468

### Resolved issues

- Deep Security Agent security updates sometimes failed after reconfiguring proxy settings. PCT-18382/DSA-5390
- Using Deep Security Agent with Web Reputation Service enabled prevented some Application Performance Monitoring (APM) applications from functioning correctly. SF04072723/SEG-97952/PCT-15716/DSA-4750

- Deep Security Agent Anti-Malware and network drivers were unable to load on systems using Security-Enhanced Linux (SELinux) enforcing mode with its default policies. PCT-14630/DSA-4917
- Deep Security Agent was sometimes unable to detect Linux system firewall port settings, which prevented the agent Firewall from allowing ports required for it to function. SF07650853/PCT-16253/DSA-4849
- Anti-Malware on-demand scans sometimes used file descriptors incorrectly, which resulted in "Bad file descriptor" log errors. DSA-4051
- Anti-Malware engine sometimes crashed. PCT-25789/DSA-4051

### Security updates

This release contains updates to third-party libraries. DSA-4187

### Known issues

- This release excludes the Deep Security Agent package for Oracle Linux 6 (32-bit) as it reports the Anti-Malware Engine status incorrectly. DSA-5557
- Switching from User Mode to Kernel Mode (**Computer** or **Policy > System > General > Choose whether to use Drivers for System Protection**) sometimes causes Deep Security Agent to lose real-time Anti-Malware protection. DSA-6090
- Switching to User Mode (**Computer** or **Policy > System > General > Choose whether to use Drivers for System Protection**) sometimes causes Deep Security Agent to lose real-time Anti-Malware protection. DSA-6104

## Deep Security Agent - 20.0.1-7380 (20 LTS Update 2024-04-24)

Release date: April 24, 2024

Build number: 20.0.1-7380

### New features

**User mode solution**: This feature provides basic Anti-Malware functions through Fanotify and eBPF on systems that lack kernel support. Deep Security Agent cannot protect runtime container workloads in this mode.

### Enhancements

- Deep Security Agent 20.0.1-7380 or later adds additional support (including SAP Scanner) for SUSE Linux Enterprise Server 12 (PowerPC little-endian). For details, see supported features by platform for Deep Security 20 LTS or Trend Cloud One - Endpoint & Workload Security. DSA-2626
- Deep Security Agent 20.0.1-7380 or later adds additional support (including SAP Scanner) for SUSE Linux Enterprise Server 15 (PowerPC little-endian). For details, see supported features by platform for Deep Security 20 LTS or Trend Cloud One - Endpoint & Workload Security. DSA-2630
- Deep Security Agent now supports Trend Vision One Service Gateway exclusions. This is only supported for Trend Cloud One - Endpoint & Workload Security users at this time. V1E-17754
- Deep Security Agent can have its proxy configuration set by the Trend Vision One Proxy Manager. V1E-14557

### Resolved issues

- Deep Security Agents running in cloud environments sometimes could not be activated for Trend Cloud One - Endpoint & Workload Security. DSA-4861
- When SAP Scanner was enabled, system events for "SAP: Anti-Malware module is not ready" or "SAP: Virus Scan service is not working correctly" sometimes displayed during Deep Security Agent upgrade. These system event messages were triggered by the restart of Deep Security Agent modules. There was no functional impact. DSA-4603
- Deep Security Agent caused high CPU usage on some systems using TLS inspection with the `tm_netagent` process running. PCT-22031/DSA-4805
- After enabling Trend Micro Service Gateway Generic Caching Service (GCS) from Trend Vision One, Deep Security Manager and Trend Cloud One - Endpoint & Workload Security displayed the "Check Status Failed" error when communicating with Deep Security Agent. DSA-4763
- The local Smart Protection Server sometimes showed an incorrect number of Deep Security Agents. DSA-3780

## Deep Security Agent - 20.0.1-4540 (20 LTS Update 2024-03-20)

Release date: March 20, 2024

Build number: 20.0.1-4540

### New features

**CPU Usage Control**: This feature provides three predefined modes to throttle CPU usage of Anti-Malware Real-Time Scan (**Computer > Settings > General > CPU Usage Control**). This is only supported for Trend Cloud One - Endpoint & Workload Security customers at this time. DSA-2465

### Enhancements

- SAP Scanner is now supported on Deep Security Agent 20.0.1-4540 or later for Red Hat Enterprise Linux 9. DSA-4213
- The SAP Scanner status for Deep Security Agent is now displayed in the console. DSA-3329
- The Deep Security Agent version is now displayed in the SAP Scanner library. SF07483850/PCT-10077/DSA-3304

### Resolved issues

- Some systems encountered higher than normal CPU usage and performance issues if Deep Security Agent lost its connection to the Smart Protection Server. SF07552865/PCT-12430/DSA-3784
- Deep Security Agent incorrectly classified the MIME type of `.dwg` files generated by AutoCAD, from AutoCAD 2004 to AutoCAD 2024. SF07027236/SEG-186079/PCT-5797/DSA-2901

### Known issues

- When SAP Scanner is enabled, system events may cause a message "SAP: Anti-Malware module is not ready" or "SAP: Virus Scan service is not working correctly" to be displayed temporary during the Deep Security Agent upgrade. This is caused by the restart of Deep Security Agent modules. There is no functional impact. DSA-4572

- After enabling Trend Micro Service Gateway Generic Caching Service (GCS) from Trend Vision One, Deep Security Manager and Trend Cloud One - Endpoint & Workload Security display "Check Status Failed" error when communicating with Deep Security Agent. For details, see Deep Security Agent reports "Check Status Failed" after enabling Service Gateway Generic Caching Service. DSA-2756

## Deep Security Agent - 20.0.1-3180 (20 LTS Update 2024-02-29)

Release date: February 29, 2024

Build number: 20.0.1-3180

### Enhancements

- Deep Security Scanner (SAP) now reports files containing Microsoft Office Macros as Active Content, while previously they were identified as Malware. PCT-5979/DSA-3911

### Resolved issues

- Migration of agents from on-premise Deep Security Manager to Trend Cloud One - Endpoint & Workload Security using Trend Vision One Service Gateway failed. This issue could also occur when migrating using other proxy services. PCT-16649/DSA-4144
- The expected MIME type for `.msg` files by the Deep Security Agent SAP Scanner was incorrect. PCT-5797/DSA-4050
- Enabling Intrusion Prevention or Web Reputation Service in Deep Security Agent sometimes resulted in a TLS inspection process (tm_netagent) error log rotation issue. DSA-3965
- Deep Security Agent could not start because a keyword in its system configuration was incorrectly interpreted. SEG-156447/PCT-8768/DSA-3897
- Smart Scan hung during its update because the IPv6 configuration could not be detected automatically. DSA-3287

- When Deep Security Agent is installed on a system with Fanotify enabled, the Anti-Malware process restarting or stopping sometimes caused the system to freeze. PCT-6047/SEG-190061/DSA-4474

### Known issues

- The Application Control Trust Entities block by target trust rule sometimes does not work properly when running a copy of an executable file. PCT-11105/DSA-3324

## Deep Security Agent - 20.0.1-690 (20 LTS Update 2024-01-17)

Release date: January 17, 2024

Build number: 20.0.1-690

### New features

**Command line scan**: Deep Security Agent now supports on-demand scans triggered using `dsa_scan` from a command line interface.

This is currently only available to Trend Cloud One - Endpoint & Workload Security customers. For more information, see Command-line basics. V1E-6993

### Enhancements

- From 2024 onward, Deep Security Agent versioning is being revised from 20.0.0 to 20.0.1. This requires Deep Security Manager 20.0.883 or later. DSA-3584.

  For details, see Preparedness of DSM/DSA for Supporting 20.0.1 Linux Kernel Support Package (KSP).

### Resolved issues

- Deep Security Agent was sometimes unable to connect to the local Smart Protection Server. DSA-3564
- When FIPS mode was disabled, Deep Security Agent used the OpenSSL configuration specified by the system environment variables rather than the config specified by the agent. PCT-4914/DSA-2651/DSA-2737/DSA-2738

- Deep Security Agent would incorrectly log network errors when the SAP scanner was enabled. DSA-3548
- Files added to the SAP Scanner allow list without including a file extension were being blocked when they should have been allowed. SF06565062/SEG-170933/DS-77132/DSA-3424
- When using Deep Security Agent on a system with Fanotify enabled, quarantining a file sometimes caused the system to freeze. PCT-6047/SEG-190061/DSA-2473

### Known issues

- Updating to Deep Security Agent 20.0.1-690 from some 20.0.0 versions sometimes fails when using Deep Security Relay on Trend Cloud One - Endpoint & Workload Security. For details, see Failed remote upgrade of self-deployed Workload Security relay from 20.0.0-3445 or later to version revision 20.0.1 DSA-3317
- With the release of Deep Security Agent 20.0.1-690, Trend Micro is changing the version number of the Kernel Support Package (KSP) from 20.0.0 to 20.0.1. This may cause issues downloading the latest kernel driver on some agent versions. To maintain kernel support after the KSP revision, it is suggested that users upgrade to Deep Security Agent 20.0.0-8453 or later. For details, see Kernel driver download issues with Deep Security Agent (DSA) Linux. DSA-3588
- Enabling Intrusion Prevention or Web Reputation Service in Deep Security Agent might result in a TLS inspection process (`tm_netagent`) error log rotation issue. For details, see TLS inspection process error log rotation problem in Deep Security. DSA-3773

## Deep Security Agent - 20.0.0-8453 (20 LTS Update 2024-01-17)

Release date: January 17, 2024

Build number: 20.0.0-8453

### Resolved issues

- Upgrading to Deep Security Agent 20.0.0-7943, 20.0.0-8137, 20.0.0-8268, or 20.0.0-8438 sometimes failed when Firewall, Web Reputation Service, or Intrusion Prevention System were enabled.

  This issue is resolved for Trend Cloud One - Endpoint & Workload Security, but continues to affect Deep Security Manager 20.0.854, 20.0.864, and 20.0.879. For details, see Failure to install or upgrade to Deep Security Agent version 20.0.0-7943 to 20.0.0-8438 for Linux when Network Modules are enabled. DSA-3834

### Enhancements

- Updated Deep Security Agent to support 20.0.1 Kernel Support Packages. In order to continue Linux Kernel support in 2024, upgrade to Deep Security Agent to 20.0.0-8453+. For details, see Platform support updates for Deep Security Agent (DSA) version revision in January 2024 Update Release. DSA-1217

### Known issues

- Deep Security Agent is sometimes unable to connect to the local Smart Protection Server. This issue is fixed in 20.0.1-690. For details, see Deep Security Agent (DSA) connection issues with Smart Protection Server (SPS) when using proxy. DSA-3564

## Deep Security Agent - 20.0.0-8438 (20 LTS Update 2023-12-12)

Release date: December 12, 2023

Build number: 20.0.0-8438

### New features

**Debian 12 support**: Deep Security Agent 20.0.0-8438 or later supports Debian 12 including Secure Boot support. This requires Deep Security Manager 20.0.864 or later. DSA-1408

### Enhancements

- Remove some file types from the scanning list to avoid high CPU and disk consumption. SF07099651/SEG-188688/DSA-2010
- Agent self-protection now protects the Advanced TLS Traffic Inspection process (tm_netagent) preventing local users with administrator privileges from stopping it. DSA-1042/DSA-1043
- Telemetry now reports the IPv4 and IPv6 address of all network interfaces. V1E-4543

### Resolved issues

- When using a local Smart Protection Server and a configured proxy, Web Reputation Service would sometimes improperly send traffic through the proxy. Web Reputation Service now sends queries to the local Smart Protection Server directly. DSA-2981
- A memory leak would occur when loading large Suspicious Object lists. SF06904914/SEG-182231/DSA-1370

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. DSA-2722

Highest Common Vulnerability Scoring System (CVSS) score: 9.8

Highest severity: Critical

### Known issues

- Enabling Intrusion Prevention or Web Reputation Service in Deep Security Agent might result in a TLS inspection process (`tm_netagent`) error log rotation issue. For details, see TLS inspection process error log rotation problem in Deep Security. DSA-3773

- Upgrading to Deep Security Agent 20.0.0-8438 sometimes fails when Firewall, Web Reputation Service, or Intrusion Prevention System are enabled.

  This issue is resolved in Deep Security Agent 20.0.0-8453 or later for Trend Cloud One - Endpoint & Workload Security, but continues to affect Deep Security Manager 20.0.854, 20.0.864, and 20.0.879. For details, see Failure to install or upgrade to Deep Security Agent version 20.0.0-7943 to 20.0.0-8438 for Linux when Network Modules are enabled. DSA-3834
- Deep Security Agent is sometimes unable to connect to the local Smart Protection Server. This issue is fixed in 20.0.1-690. For details, see Deep Security Agent (DSA) connection issues with Smart Protection Server (SPS) when using proxy. DSA-3564

## Deep Security Agent - 20.0.0-8268 (20 LTS Update 2023-11-21)

Release date: November 21, 2023

Build number: 20.0.0-8268

### New Features

- Deep Security Agent now supports Trend Micro Service Gateway Generic Caching Service (GCS). DSA-2035
- Deep Security Agent now supports FIPS mode for Debian 10 and Debian 11. This requires Deep Security Manager 20.0.854 or later. DSA-1955

### Resolved issues

- Deep Security Anti-Malware sometimes did not function as expected after the system had resumed from sleep mode (S0 low-power idle mode of the working state, also known as modern standby). SF07326571/PCT-5476/DSA-2485
- Deep Security Manager displayed the status of the VM protected by the Deep Security Virtual Appliance as Offline, after the Deep Security Virtual Appliance had been upgraded to version 20.0.0-7943 or 20.0.0-8137. The Deep Security Virtual Appliance itself was functioning properly and displayed the status as Managed

(Online). SF07317008/SF07313849/SF07331882/PCT-4330/PCT-4607/PCT-4899/DSA-2259
- Deep Security Agent incorrectly classified MIME type of `.xml` files generated by Microsoft Word, Excel, PowerPoint, as well as `.dwg` files generated by AutoCAD and R2000. SF07027236/SEG-186079/DSA-2202

### Known issues

- Linux virtual machines froze when trying to update the Smart Scan pattern. As a workaround, you can add the `/opt/ds_agent/lib/libvmpd_scanctrl.so=icrc_try_update=0` key to the `ds_am.ini` file and restart the DSA service. SF07031242/PCT-5795/DSA-2616
- Enabling Intrusion Prevention or Web Reputation Service in Deep Security Agent might result in a TLS inspection process (`tm_netagent`) error log rotation issue. For details, see TLS inspection process error log rotation problem in Deep Security. DSA-3773
- Upgrading to Deep Security Agent 20.0.0-8268 sometimes fails when Firewall, Web Reputation Service, or Intrusion Prevention System are enabled.

  This issue is resolved in Deep Security Agent 20.0.0-8453 or later for Trend Cloud One - Endpoint & Workload Security, but continues to affect Deep Security Manager 20.0.854, 20.0.864, and 20.0.879. For details, see Failure to install or upgrade to Deep Security Agent version 20.0.0-7943 to 20.0.0-8438 for Linux when Network Modules are enabled. DSA-3834

## Deep Security Agent - 20.0.0-8137 (20 LTS Update 2023-10-26)

Release date: October 26, 2023

Build number: 20.0.0-8137

### New features

**Miracle Linux 9 support**: Deep Security Agent 20.0.0-8137 or later supports Miracle Linux 9, including FIPS mode and Secure Boot support. This requires Deep Security Manager 20.0.844 or later.

### Known issues

- Upgrading to Deep Security Agent 20.0.0-8137 sometimes fails when Firewall, Web Reputation Service, or Intrusion Prevention System are enabled.

  This issue is resolved in Deep Security Agent 20.0.0-8453 or later for Trend Cloud One - Endpoint & Workload Security, but continues to affect Deep Security Manager 20.0.854, 20.0.864, and 20.0.879. For details, see Failure to install or upgrade to Deep Security Agent version 20.0.0-7943 to 20.0.0-8438 for Linux when Network Modules are enabled. DSA-3834
- Deep Security Manager displays the status of guest VMs protected by the Deep Security Virtual Appliance 20.0.0-7943 as Offline or Check Status Failed (Activation Required). SF07317008/SF07313849/SF07331882/PCT-4330/PCT-4607/PCT-4899/DSA-2259

## Deep Security Agent - 20.0.0-7943 (20 LTS Update 2023-09-26)

Release date: September 26, 2023

Build number: 20.0.0-7943

### New features

**Red Hat Enterprise Linux 8.6 (PowerPC little-endian) on-demand scan support**: Deep Security Agent 20.0.0-7943 or later supports only the Anti-Malware on-demand scan feature for Red Hat Enterprise Linux 8.6 (PowerPC little-endian). This requires Deep Security Manager 20.0.817 or later. Security updates are currently unsupported for this platform.

**SUSE Linux Enterprise Server 12 (PowerPC little-endian) on-demand scan support**: Deep Security Agent 20.0.0-7943 or later supports only the Anti-Malware on-demand scan feature for SUSE Linux Enterprise Server 12 (PowerPC little-endian). This requires Deep Security Manager 20.0.817 or later. Security updates are currently unsupported for this platform.

**SUSE Linux Enterprise Server 15 (PowerPC little-endian) on-demand scan support**: Deep Security Agent 20.0.0-7943 or later supports only the Anti-Malware on-demand scan feature for SUSE Linux Enterprise Server 15 (PowerPC little-endian). This requires Deep Security Manager 20.0.817 or later. Security updates are currently unsupported for this platform.

> **Note:**
> Security updates are not supported on PowerPC platforms at this time. The Advanced Threat Scan Engine (ATSE) status does not display correctly and the following alerts are expected on RHEL 8.6, SUSE 12, and SUSE 15:
>
> - Security Update: Security Update Check and Download Failed (Agent/Appliance error)
> - Status: Out of Date

### Enhancements

- New commands exist to get proxy information from the command line:
  `dsa_query -c GetProxyInfo`
  `dsa_query -c GetProxyInfo details=true`
  DSA-864
- All Trend Micro public keys that are used to validate kernel module signatures are now included by default in the Deep Security Agent packages. SF06915385/SEG-185980/DSA-1569
- In order to display agent pattern updates properly, Deep Security Agent 20.0.0-7943 or later requires Deep Security Manager 20.0.759 or later. For more information, see Incompatible Agent / Appliance Version error in Deep Security Agent 20.0.0-7943. SEG-190866/SEG-191017/DSA-1531

### Resolved issues

- Deep Security Agent ignored the file if the exclusion list for the file or folder contained an empty path from Deep Security Manager. PCT-1066/DSA-1873

### Known issues

- Enabling Intrusion Prevention or Web Reputation Service in Deep Security Agent might result in a TLS inspection process (`tm_netagent`) error log rotation issue. For details, see TLS inspection process error log rotation problem in Deep

Security. DSA-3773

- Upgrading to Deep Security Agent 20.0.0-7943 sometimes fails when Firewall, Web Reputation Service, or Intrusion Prevention System are enabled.

  This issue is resolved in Deep Security Agent 20.0.0-8453 or later for Trend Cloud One - Endpoint & Workload Security, but continues to affect Deep Security Manager 20.0.854, 20.0.864, and 20.0.879. DSA-3834
- Deep Security Manager displays the status of guest VMs protected by the Deep Security Virtual Appliance 20.0.0-7943 as Offline or Check Status Failed (Activation Required). SF07317008/SF07313849/SF07331882/PCT-4330/PCT-4607/PCT-4899/DSA-2259

## Deep Security Agent - 20.0.0-7719 (20 LTS Update 2023-08-29)

Release date: August 29, 2023

Build number: 20.0.0-7719

### New features

**Miracle Linux 8 support**: Deep Security Agent 20.0.0-7719 or later now supports Miracle Linux 8, including FIPS mode. This requires Deep Security Manager 20.0.817 or later.

### Enhancements

- Deep Security Agent no longer updates the Smart Scan agent pattern when Smart Scan is disabled, saving network bandwidth. SEG-186625/DSA-1063
- Deep Security Agent now downloads fewer incremental pattern updates, saving network bandwidth. (Agents configured as a Deep Security Relay still download all pattern updates.) DSA-1000
- The "blocking page" Web Reputation Service redirects users to when they try to access a blocked URL can now be viewed in Czech or Polish. DSA-444
- Advanced Threat Scan Engine has been updated to version 22.6. DSA-453

### Resolved issues

- Stopping the Deep Security Agent service (ds_agent) took longer than usual on some systems. SEG-187365/DSA-1212
- Deep Security Agent sometimes performed security updates even if none were scheduled. SEG-187449/DSA-1064
- Deep Security Agent caused high CPU usage on some systems. SEG-185563/DSA-756
- TLS Inspection Package updates sometimes caused the `ds_nuagent` service to stop unexpectedly. DSA-1319

## Deep Security Agent - 20.0.0-7476 (20 LTS Update 2023-07-25)

Release date: July 25, 2023

Build number: 20.0.0-7476

### Enhancements

- Updated the dsa-connect service to improve CPU performance. C1WS-12970
- Deep Security Agent 20.0.0-7476 now supports FIPS mode for Red Hat Enterprise Linux 9. DS-77642
- Updated Deep Security Agent Scanner (SAP) to accept up to 512 parallel client connections established by SAP NetWeaver. Note that the previous connection limit was 256. SF06983349/SEG-184190/DS-78229

### Resolved issues

- Smart Protection Servers would sometimes lose connectivity with Web Reputation Service. SF06423462/SEG-166651/DSSEG-7858

## Deep Security Agent - 20.0.0-7303 (20 LTS Update 2023-06-28)

Release date: June 28, 2023

Build number: 20.0.0-7303

## New features

**Amazon Linux 2023 support:** Deep Security Agent 20.0.0-7303 or later now supports Amazon Linux 2023, including FIPS mode. This requires Deep Security Manager 20.0.789 or later.

> **Note:** At time of release, Amazon Linux 2023 is not yet certified for FIPS. See the Amazon Linux 2023 release notes for the latest support information.

**Amazon Linux 2023 (AWS Arm-based Graviton 2):** Deep Security Agent 20.0.0-7303 or later now supports Amazon Linux 2023 on AWS Graviton 2. This requires Deep Security Manager 20.0.789 or later.

**Advanced TLS Traffic Inspection** now supports Oracle Linux 9 (64-bit), Red Hat Enterprise Linux 9 (64-bit), and Ubuntu 22.04 (64-bit).

## Enhancements

- Deep Security Agent now supports IPv6 addresses using either CIDR or double colon notation, such as fe80:0:0:0:0:0:0:1/24 or fe80::01. SF04849178/SEG-122076/DS-67280
- Web Reputation Service now automatically monitor the ports used by the OS proxy configuration. DS-77233
- Removed unnecessary proxy scheduled tasks from the Deep Security Virtual Appliance. This should prevent `Timed out waiting for relay to msg` and `Error creating task...` errors in the logs. SF06844880/SEG-179554/DS-77440

## Resolved issues

- When Secure Boot is enabled but the signing key has not been loaded, the system would crash when Anti-Malware used the fanotify facility. SF06464888/SEG-167771/DS-76161
- Intrusion Prevention (IPS) might not read the correct payload value, which can result in rule malfunctions. DS-74647

- The Deep Security Agent would report "dsa-connect has not provided status" on every heartbeat, even when Endpoint Sensor was not in use. C1WS-14696
- Deep Security Relay 20.0.0-7119 failed to provide security and software updates when using the improved Relay. SF06935222/SEG-183184/DS-78201
- The Deep Security Agent connection count could overflow under certain conditions. DS-76902
- Some MQTT messages would be sent repeatedly and cause dsa-connect to get stuck in a shutdown loop. DS-76709

## Deep Security Agent - 20.0.0-7119 (20 LTS Update 2023-05-29)

Release date: May 29, 2023

Build number: 20.0.0-7119

### Enhancements

- MQTT connection credentials were entered in the Deep Security Agent log file (`ds_agent.log`) in certain scenarios. SEG-174560/C1WS-13282
- Deep Security Agent crashed some systems when they were out of memory. SF06704797/SEG-175243/DSSEG-7875
- Agent self-protection now secures the Advanced TLS inspection process (`ds_nuagent`), preventing local users with administrator privileges from stopping it. DS-74080

  Systems running Red Hat Enterprise Linux 7 (64-bit) with SELinux may require some manual configuration to avoid permission issues following this update. For details, see BPF permission denied for ds_nuagent with RedHat 7 SELinux enforcing mode in Deep Security.
- Deep Security Agent now runs within a predefined group and accept outbound traffic. DS-77415

### Resolved issues

- Deep Security Agent only reported a single Anti-Malware event for an infected compressed file, even if it contained multiple infected files. DS-76339
- After replacing a connection, Deep Security Agent reported metrics as though it was still connected to the old connection for up to 4 minutes. DS-77453
- When Anti-Malware was enabled, Deep Security Agent caused high CPU usage on some systems. DS-77758

## Deep Security Agent - 20.0.0-6912 (20 LTS Update 2023-05-02)

Release date: May 02, 2023

Build number: 20.0.0-6912

### New features

**Red Hat Enterprise Linux Workstation 7 support**: Deep Security Agent 20.0.0-6912 or later now supports Red Hat Enterprise Linux Workstation 7, including Secure Boot support. This requires Deep Security Manager 20.0.759 or later.

**AlmaLinux 9 support**: Deep Security Agent 20.0.0-6912 or later now supports AlmaLinux 9, including Secure Boot support. This requires Deep Security Manager 20.0.759 or later.

### Enhancements

- Updated Deep Security Agent to make the connection timeout for proxy probing configurable by adding a line to `ds_agent.ini`. SF06664116/SEG-173848/DS-77182

  Example proxy probing line in `ds_agent.ini` config file:
  `dsa.proxymanager.ProbeTimeoutInSec=120`
- Deep Security Agent installer now prevents the agent from updating if it detects SHA-1 was used to sign the certificate on the agent installer. This prevents the agent from updating and becoming unresponsive, since Deep Security Agent

20.0.0-6313 and higher requires RSA-2048 and SHA-256. For more information on certificate upgrade, see Upgrade the Deep Security cryptographic algorithm. DS-76499

- Updated Deep Security Agent to improve MQTT connection quality and reduce the occurrence of connection timeouts. DS-76840
- Deep Security Agent now includes path and PID (process ID) for Anti-Malware events. SF05682761/SEG-147452/DS-72909

### Resolved issues

- When connecting through a proxy with FIPS mode enabled, Deep Security Agent sometimes had connectivity issues with IoT devices. SEG-174776/DS-77197
- Deep Security Agent's Anti-Malware module sometimes failed to restart following an IPC (inter-process communication) timeout. DS-76889/SEG-169218
- A compatibility issue between the Deep Security Agent network driver and some third-party products caused systems to crash. SEG-156743/DS-75377
- Deep Security Virtual Appliance sometimes crashed when connecting by HTTPS to a Smart Protection Server. SEG-169451/DS-76968
- Deep Security Agent sometimes reported the network driver status incorrectly after the driver had restarted. C1WS-12896
- When Web Reputation Service was enabled, Deep Security Agent caused some systems to shutdown unexpectedly. SF06680505/SEG-174730/DSSEG-7866
- Files added to the SAP Scanner allow list without including a file extension were being blocked when they should have been allowed. SF06565062/SEG-170933/DS-77132
- Deep Security Agent sometimes crashed when shutting down after downloading new plugins from the relay. DS-76961
- Deep Security Agent caused some systems to reboot unexpectedly. SF06584000/SEG-171147/DSSEG-7851

## Deep Security Agent - 20.0.0-6658 (20 LTS Update 2023-03-22)

Release date: March 22, 2023

Build number: 20.0.0-6658

## New features

**Oracle Linux 9 support**: Deep Security Agent 20.0.0-6658 or later with Deep Security Manager 20.0.737 or later now supports Oracle Linux 9, including FIPS mode and Secure Boot support.

**Service Gateway**: Deep Security Agent 20.0.0-6658 or later with Deep Security Manager 20.0.741 or later now supports the Service Gateway feature, providing forward proxy functionality.

## Enhancements

- When an Application Control Trust Entities path rule uses a wildcard without specifying a filename, the wildcard now applies to all files in any directory matching the rule's path. Note that previously, the globstar (`**`) wildcard would apply to a path rule's directory and subdirectories, as opposed to the single star (`*`) wildcard which would only match within the path rule's directory. DS-75133
- Web Reputation Service now includes OS platform metadata. DS-75453
- Anti-Malware events generated by the SAP Scanner now include file hashes. DS-75648/SEG-165491
- Application Control now checks web browser execution of .HTML, .HTM, and .JS files. DS-75102
- Deep Security Agent now sends full command lines for processes to Deep Security Manager, improving the Recommendation Scan's rule recommendations. Note that previously, the agent only sent the first 2048 characters of each process's command line. C1WS-11728
- Deep Security Agent 20.0.0-6658 or later with Deep Security Manager 20.0.737 or later now supports Secure Boot for Ubuntu 22.04. DS-73729
- Deep Security Agent 20.0.0-6658 or later now supports the Proxy Manager for Trend Micro Vision One (XDR) Threat Intelligence - User-Defined Suspicious Object (UDSO). DS-75365

- Updated Deep Security Agent's logging system to provide additional information and tracing to debug customer issues more efficiently. The agent now generates five (5) log files (`dsa-connect-X.log`) that are 2MB each instead of the agent's previous three 1MB log files. C1WS-9598

The logger supports an on-demand JSON config file (either `dsa-connect.ini` or `dsa-connect.conf`) with the following configurable options:

- Debug: Enable the debug log messages. The default value is false.
- Count: Number of log files to generate. The default value is 5.
- Size: Maximum size of each log file in bytes. The default value is 2097152.

Example config file:

```
{
"Debug": true,
"Count": 5,
"Size": 2097152
}
```

- Deep Security Agent can now have a maximum of 1024 process tasks when deployed on RedHat or SUSE. PCT-25908/DSA-5507

## Resolved issues

- When the Advanced TLS Traffic Inspection "Inspect TLS/SSL traffic" option was set to "No" from the console (**Computer** or **Policy > Intrusion Prevention > General > Advanced TLS Traffic Inspection**), driver-side SSL packets were sometimes still being processed. DS-76160
- The Deep Security Agent kernel support package download was sometimes interrupted, generating "Agent Integrity Check Failed" warnings and "Kernel Unsupported" errors. SEG-169497/DS-76545
- Deep Security Agent's Intrusion Prevention System sometimes failed to block "TCP Congestion Flags" properly. DS-76182
- Anti-Malware Behavior Monitoring had a driver issue causing kernel warnings on some systems. SF06254724/SEG-163042/ORCA-762
- When Anti-Malware Smart Scan was enabled, an IPC connectivity issue caused some systems to crash. SEG-169132/C1WS-10821

- Deep Security Agent security updates were failing due to a file handle issue that prevented files from being removed during an update. DS-75907
- A process thread timeout caused the Anti-Malware Engine to restart unexpectedly on some systems. SF06524736/SEG-169218/DS-76656
- When a SOCKS proxy was used, Deep Security Agent failed to provide a Web Reputation Services rating for HTTP URLs. DS-73482/DS-73364
- Deep Security Agent upgrade sometimes failed because of a missing signature in the agent package. SF06045259/SEG-154576/DS-73668
- Deep Security Agent was incorrectly generating system events showing that the Advanced Threat Search Engine (ATSE) component had been removed on some systems. SEG-147779/DS-75463
- Updated Deep Security Agent to increase the MQTT timeout from 30 minutes to 2 hours to help resolve connection issues on some systems. C1WS-11835
- Deep Security Agent was unable to connect to the Anti-Malware Smart Scan service on some systems. SEG-168468/DS-76433
- Deep Security Agent caused performance issues on systems generating a large number of container environment Application Control events. SF06538377/SEG-169605/DS-76594

## Deep Security Agent - 20.0.0-6313 (20 LTS Update 2023-01-31)

Release date: January 31, 2023

Build number: 20.0.0-6313

### New feature

**Agent self-protection**: This feature helps prevent users on the local system from tampering with the agent. For more information, and help configuring agent self-protection, see Enable or disable agent self-protection.

**Rocky Linux 9 support**: Deep Security Agent 20.0.0-6313 or later with Deep Security Manager 20.0.716 or later now supports Rocky Linux 9, including FIPS mode and Secure Boot support. DS-73727

## Enhancements

- Deep Security no longer supports certificates signed with the SHA-1 algorithm. The agent now requires SSL/TLS certificates issued using SHA-256 to communicate with the Deep Security Manager. C1WS-5676

- With Anti-Malware and Behavior Monitoring enabled, Deep Security Agent 20.0.0-6313 or later with Deep Security Manager 20.0.716 or later now monitors for suspicious behavior to improve protection against MITRE attack scenarios. DS-73644
- Deep Security Agent 20.0.0-6313 or later with Deep Security Manager 20.0.711 or later now supports FIPS mode for Oracle Linux 8. DS-73778

## Resolved issues

- When Application Control was enabled, Deep Security Agent's status sometimes became stuck at "Application Control Ruleset Update In Progress". DS-74627
- For component updates, Deep Security Agent would attempt with and without use of a proxy and generate an event for each attempt. To make event reporting more straightforward, this behavior has been changed so that after a successful update the agent only shows the final successful event. SF06207160/SEG-160085/DSSEG-7765
- Deep Security Agent crashes and issues connecting with Deep Security Manager caused Anti-Malware Offline events. SF06061098/SEG-154701/DS-74665
- With Web Reputation Enabled, some characters entered in console commands were not being parsed properly. For example, an underscore (`_`) entered in a command was replaced with a dash (`-`), and an uppercase Z was replaced with a lowercase z. DS-74335
- Application Control sometimes failed to block programs running in namespace mode. SF05929869/SEG-151363/DS-74116
- Integrity Monitoring sometimes failed to create events after running certain console commands (for example, `passwd` or `mv` commands). 05718251/SEG-148552/DS-72643
- Older Application Control events were not being removed from the database as intended, causing the `events.db` file size to increase indefinitely. SF06172729/SEG-159548/DS-74706

- When Integrity Monitoring event generation is interrupted by a process or system crash, it could lead to incorrect events being created. SF05508030/SEG-138756/DS-72470

### Known issues

- Deep Security Agent is having connectivity issues on some systems, resulting in "Event ID 9012, Smart Protection Server Disconnected for Smart Scan" error messages. For more details including temporary workaround instructions, see Smart Protection Server disconnected messages appear in Deep Security. SF06512673/SEG-168468

## Deep Security Agent - 20.0.0-5953 (20 LTS Update 2022-11-22)

Release date: November 22, 2022

Build number: 20.0.0-5953

### New feature

**Agent self-protection**: This feature helps prevent users on the local system from tampering with the agent. For more information, and help configuring agent self-protection, see Enable or disable agent self-protection.

### Enhancements

- Deep Security Agent 20.0.0-5953 or later with Deep Security Manager 20.0.711 or later now supports FIPS mode for Oracle Linux 8.

### Resolved issues

- Application Control sometimes failed to block programs running in namespace mode. SF05929869/SEG-151363/DS-74116
- Integrity Monitoring sometimes failed to create events after running certain console commands (for example, `passwd` or `mv` commands). 05718251/SEG-148552/DS-72643

- Older Application Control events were not being removed from the database as intended, causing the `events.db` file size to increase indefinitely. SF06172729/SEG-159548/DS-74706
- When Integrity Monitoring event generation is interrupted by a process or system crash, it could lead to incorrect events being created. SF05508030/SEG-138756/DS-72470

## Deep Security Agent - 20.0.0-5761 (20 LTS Update 2022-10-21)

Release date: October 21, 2022

Build number: 20.0.0-5761

### New feature

#### Enhanced platform support

- SAP Scanner support for Oracle Linux 7: Deep Security Agent for Oracle Linux 7 now supports SAP Scanner. VO-1849

### Enhancements

- Updated Deep Security Agent to include additional metadata, such as `UserAgent` and `Referrer`, for Web Reputation Services. DS-72196
- Updated Deep Security Agent to include the Integrity Monitoring database in the agent diagnostic package. DS-73293
- Updated Deep Security Agent to support NULL cipher when inspecting TLS traffic with Intrusion Prevention. DS-71085
- Deep Security Agent now can be deployed without additional dependency on System V packages. DS-73588

### Resolved issues

- With Log Inspection enabled, Deep Security Agent sometimes generated "Abnormal Restart Detected" events. SF05951130/SEG-151372/DS-73737

- If the Deep Security Agent service stopped while running Application Control in Maintenance Mode, executable files created after the service stopped were not being auto-approved as intended. SF05961688/SEG-152045/DS-73570
- With Advanced TLS traffic inspection enabled, Deep Security Agent had a memory issue that prevented some applications from running. SEG-150631/DS-74039
- Software, if renamed or copied while Application Control had Maintenance Mode enabled, would remain authorized in the software inventory under its original filename or location. DS-74015
- Virtual Machines using vMotion sometimes deactivated unexpectedly and displayed an "Offline (Activation required)" status. SEG-153050/DS-73807
- The TLS inspection support package failed to download on Deep Security Agents using Edge Relay. DS-73789
- On RedHat Enterprise Linux computers, Anti-Malware being enabled would sometimes cause a system crash. SEG-155143/DS-74008

## Deep Security Agent - 20.0.0-5512 (20 LTS Update 2022-09-22)

Release date: September 22, 2022

Build number: 20.0.0-5512

### Enhancements

- Updated Deep Security Agent kernel device module files to comply with Security-Enhanced Linux (SELinux) requirements. DSSEG-7378
- Deep Security Agent now reports host information with additional details. DS-72609
- Deep Security Agent now reports host metadata for installed software with additional details. DS-72608
- Updated Deep Security Agent to add multi-thread support for On-Demand scan and Scheduled Scan. DS-72797/DS-72798
- Deep Security Agent with Deep Security Manager 20.0.677 or later now supports the automatic update of Advanced TLS Traffic Inspection as operating system

libraries change (**Computer** or **Policy > Settings > TLS Inspection Package Update**). DS-72828

### Resolved issues

- Trust Entities settings were not being re-applied after turning Application Control off and back on again. SF05930535/SEG-152439/DS-73312
- When installed on a system that uses secure boot without importing the required sign key, Deep Security Agent generated an Anti-Malware Engine error code with "Reason ID: 13" when it should have generated the code with "Reason ID: 11". For details on Reason IDs, see Warning: Anti-Malware Engine has only Basic Functions. DS-72891
- Deep Security Agent reported host metadata in an unexpected format. DS-73411

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-8100/VRTS-8101/DS-73087/DS-72528

Highest Common Vulnerability Scoring System (CVSS) score: 7.0

Highest severity: High

## Deep Security Agent - 20.0.0-5394 (20 LTS Update 2022-08-29)

Release date: August 29, 2022

Build number: 20.0.0-5394

### New features

**Ubuntu 22.04 (AWS Arm-based Graviton 2) support**: Deep Security Agent 20.0.0-5394 or later with Deep Security Manager 20.0.677 or later is now supported on Ubuntu 22.04 (AWS Arm-based Graviton 2).

## Enhancements

- The Deep Security Agent process now restarts automatically if the file descriptor count is abnormally high, and a counter was added to track how many times this event occurs. SF05212995/SEG-130431/DS-72616
- Application Control now detects software changes for executables with non executable extensions. DS-70805
- Updated Deep Security Agent to add support for inspecting packets using dynamic ports in a TLS connection. DS-71078
- Updated Deep Security Agent to add more metrics for Advanced TLS Inspection. DS-72833

## Resolved issues

- When TLS inspection was done on a UDP connection with dynamic ports, the operating system would sometimes crash. SEG-151169/DS-73043
- Log Inspection Engine would go offline when using '$' character in match or regex fields together with variables. SEG-146965/SEG-146966/DS-72325
- Anti-Malware would sometimes leak file descriptors. SF05212995/SEG-130431/DS-72979
- When assigning a policy with real-time Anti-Malware turned off to a new guest VM, it would sometimes turn off real-time Anti-Malware for all other guest VMs registered to the same Deep Security Virtual Appliance. SEG-146057/DS-72856
- Application Control would still block access to network files while in maintenance mode. SF04922652/SEG-131710/DS-72037
- When Application Control is enabled, Adobe plugins were generating unexpected security events. SF05823607/SEG-148570/DS-72679
- Deep Security Agent would return "revision mismatch (-10039)" errors when loading certain configuration files during an agent update. DS-72499
- Deep Security Agent would report detected software changes before Application Control inventory scan was completed. DS-72071
- Patched third-party libraries. Before patch, the Deep Security Virtual Appliance agent would sometimes crash. SF05559993/SEG-140234/DS-72510

### Known issues

- When executing multiple custom script tasks, new tasks are currently overwritten by previous unfinished tasks. You can execute custom script tasks one by one to bypass this issue. Note that this issue will be fixed in a future release. DS-72699

## Deep Security Agent - 20.0.0-5137 (20 LTS Update 2022-07-26)

Release date: July 26, 2022

Build number: 20.0.0-5137

### New features

**Advanced TLS Traffic Inspection**: Deep Security Agent 20.0.0-5137 or later adds Advanced TLS Traffic Inspection support to platforms that run system updates or package updates. Note that this feature is currently only supported for Trend Cloud One - Workload Security. Support for Deep Security Manager (On-Premise) will be added later.

**Red Hat 9 support**: Deep Security Agent 20.0.0-5137 or later with Deep Security Manager 20.0.651 or later now supports Red Hat 9.

**Amazon Linux 2 support**: Deep Security Agent 20.0.0-5137 or later with Deep Security Manager 20.0.651 or later now supports Amazon Linux 2 for AWS Graviton 3.

### Enhancements

- Updated Deep Security Agent to add Anti-Malware support for Red Hat OpenShift. DS-72368
- Updated Deep Security Agent to reduce CPU usage and improve container performance for real-time Anti-Malware scanning. Previously, all files were scanned during read/write. Now, Anti-Malware file scanning during write is deferred (the file is added to a queue and scanned in the background). DS-65581
- Deep Security Agent Scanner (SAP) now generates infection reports with additional details. DS-71660

- Updated Deep Security Agent to improve the "zero-config" SSL process for outbound connections. DS-70715
- Updated Deep Security Agent to improve Trust Entities functionality. Trust rule wildcard support now includes globstar `\*\*` which matches many sub directories. Single star `\*` now only matches within your current directory. Existing rules that used a single star `\*` to match many folders no longer work and need to be changed to use a globstar `\*\*`. DS-71817

## Resolved issues

- Deep Security Agent Scanner (SAP) sometimes displayed duplicate Anti-Malware events for .SAR file types. DS-71879
- Deep Security Agent SAP scanner could not detect the MIME (.TTF) files. DS-55897
- Intrusion Prevention rules with certain setting combinations failed to compile. DS-71889
- Deep Security Agent had connectivity issues on some systems. DS-72219

## Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-7102/VRTS-7070/VRTS-7041/VRTS-7039/DSSEG-7636

Highest Common Vulnerability Scoring System (CVSS) score: 4.4

Highest severity: Medium

## Known issues

- When executing multiple custom script tasks, new tasks are currently overwritten by previous unfinished tasks. You can execute custom script tasks one by one to bypass this issue. Note that this issue will be fixed in a future release. DS-72699

## Deep Security Agent - 20.0.0-4959 (20 LTS Update 2022-07-04)

Release date: July 4, 2022

Build number: 20.0.0-4959

### New features

**Ubuntu 22.04**: Deep Security Agent 20.0.0-4959 or later now supports Ubuntu 22.04. This requires Deep Security Manager 20.0.651 or later.

**FIPS mode on Ubuntu 20.04**: Deep Security Agent 20.0.0-4959 or later now supports FIPS mode for Ubuntu 20.04.

### Enhancements

- Deep Security Agent 20.0.0-4959 or later with Deep Security Manager 20.0.0-414 or later now has improved Anti-Malware support on systems using Fanotify. Previously, "Anti-Malware Engine Offline" events interrupted Anti-Malware function on these systems. Now, an Anti-Malware with basic functions event is recorded and users maintain basic file scanning function, but not advanced scan mechanisms such as Predictive Machine Learning. DS-68552

### Resolved issues

- Deep Security Agent Scanner (SAP) had a connectivity issue preventing it from loading the correct libraries on some systems. DS-71623
- Deep Security Agent Scanner library sometimes caused SAP applications to crash. DS-71849
- Anti-Malware was unable to remove immutable or append-only files on some systems. VRTS-7110/DS-52383
- Using the command line (`dsa_control -b`), Deep Security Relay failed to extract the bundle file required to update in a closed network environment. SF05715642/SEG-144571/DSSEG-7600

- With Log Inspection enabled, upgrades to Deep Security Agents 20.0.0-4726 encountered "Get Events Failed" and "Command Not Found" alerts. SF05738607/SEG-145679/DS-72117
- When Anti-Malware is enabled alongside Integrity Monitoring, Deep Security Agent caused high CPU usage. SF05169148/SEG-129522/DS-69594
- With Anti-Malware enabled, Deep Security Agent sometimes crashed operating systems that were undergoing an ISO backup. SF05532786/SEG-139280/DS-71299
- Updated Deep Security Agent to immediately report its status to Deep Security Manager when Application Control's maintenance mode is enabled on the agent. DS-71617
- Deep Security Agent sometimes created unclear error log entries referencing "invalid" or "badly-formed" proxy URLs. SEG-144613/DS-71866

## Deep Security Agent - 20.0.0-4726 (20 LTS Update 2022-05-31)

Release date: May 31, 2022

Build number: 20.0.0-4726

### Enhancements

- Updated Deep Security Relay to record its status and other metrics for potential troubleshooting. DS-65763

### Resolved issues

- Trust Entities "allow by target" rules sometimes blocked processes they weren't intended to block. SF04922652/SEG-131710/DS-71060
- Deep Security Agent reported false positive "Created/Deleted" Integrity Monitoring events under some configurations. SF05434164/SEG-136425/DS-70656
- Deep Security Agent Scanner library didn't work properly with highly-interrupted SAP applications on Linux systems. This resulted in files were scanned, but results might be unable to report to the SAP applications. SF05390384/SEG-136659/DS-71251

- Following an upgrade, Deep Security Agent would send continuous "Security update in progress" reports to Deep Security Manager. SF05253107/SEG-131983/DS-69747
- Updated Deep Security Relay to prevent Deep Security Agent from retrieving incomplete signature files for packages. SF05332854/SEG-134394/DS-71228
- Deep Security Agent had connectivity issues caused when a Server Name Indicator (SNI) used an invalid format. SEG-127761/DS-70806
- An abnormal restart of Deep Security Agent sometimes lead to "Anti-Malware Engine Offline" errors. SEG-140234/DS-71333
- Secondary DNS setting from IP pool was not configured when Appliance was deployed. SF05215036/SEG-134844/DSSEG-7535

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. DS-52329

Highest Common Vulnerability Scoring System (CVSS) score: 7.5

Highest severity: High

## Deep Security Agent - 20.0.0-4416 (20 LTS Update 2022-04-28)

Release date: April 28, 2022

Build number: 20.0.0-4416

### Enhancements

- Updated Deep Security Agent to improve Intrusion Prevention performance when the "Bypass Network Scanner" rule was applied. DS-69515

### Resolved issues

- With Intrusion Prevention enabled, a packet transmission error caused some systems to crash. SEG-136843/DSSEG-7524

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-7132/DS-70518

Highest Common Vulnerability Scoring System (CVSS) score: 7.5

Highest severity: High

## Deep Security Agent - 20.0.0-4185 (20 LTS Update 2022-04-06)

Release date: April 6, 2022

Build number: 20.0.0-4185

### New features

**Advanced TLS traffic inspection**: Advanced TLS traffic inspection adds the capability for inspecting TLS traffic encrypted with modern ciphers, including Perfect Forward Secrecy (PFS). It also enhances virtual patching for HTTPS servers to help protect against vulnerabilities such as Log4j.

### Resolved issues

- Running an Anti-Malware manual scan using the command line sometimes made Deep Security Agent unable to receive incoming connections. SF05385865/SEG-135256/DS-70364
- Deep Security Agent created an "Application Control Engine Offline" error during agent upgrade, and an "Application Control Engine Online Again" message after

upgrade completion. Note that an upgrade should not have triggered these events. DS-69888

- Application Control sometimes blocked unrecognized software even when running in maintenance mode. SF05234969/SEG-133594/DS-69752
- Deep Security Agent had SSL connectivity issues when Web Reputation Service was enabled. DS-67675
- Deep Security Agent sometimes consumed a high amount of system resources during policy updates. SEG-134417/DS-69810

## Deep Security Agent - 20.0.0-3964 (20 LTS Update 2022-03-01)

Release date: March 1, 2022

Build number: 20.0.0-3964

### New features

**Threat Intelligence**: Threat Intelligence (formerly known as Connected Threat Defense) provides enhanced malware protection for new and emerging threats. For more information, see Detect emerging threats using Threat Intelligence.

#### Enhanced platform support

- **Deep Security Agent 20.0.0-3964 or later is now supported on these platforms**:
  - Red Hat 8 (AWS Arm-based Graviton 2) (requires Deep Security Manager 20.0.605+)
  - Debian 11 (requires Deep Security Manager 20.0.605+)

### Enhancements

- Updated Deep Security Agent to exclude suspicious characters, such as `$`, found in strings from the "Original IP (XFF)" field for Intrusion Prevention events. SEG-129905/DS-68989

### Resolved issues

- With real-time Integrity Monitoring enabled, Integrity Monitoring delete events were not being generated after editing a file and then deleting it. DS-69057
- Deep Security Agent caused high CPU usage for systems protecting containers. Container protection can now be enabled or disabled in Deep Security Manager (from **Computer** (or **Policy**) **> Settings > Container Protection**). SEG-115751/DSSEG-7334

## Deep Security Agent - 20.0.0-3770 (20 LTS Update 2022-01-24)

Release date: January 24, 2022

Build number: 20.0.0-3770

### New features

**Zero config IPS inspection**: Deep Security Agent adds the capability for Intrusion Prevention to inspect TLS encrypted traffic without manually importing certificates. This adds support for more cipher suites as well. This feature is being rolled out gradually for Linux platforms, beginning with Trend Micro Cloud One - Workload Security customers.

**CRI-O support**: A Deep Security Agent's "CRI-O engine version" is now displayed in Deep Security Manager, as well as Anti-Malware event information for containers. Note that CRI-O is currently only supported for Deep Security Manager (On-Premise). Support for Trend Micro - Cloud One Workload Security will be added later.

### Enhancements

- Updated Deep Security Agent to allow Intrusion Prevention to connect to Deep Security Manager if the manager is using TLS 1.2 strong ciphers. DS-69042
- Updated Deep Security Agent to correctly display the host's IP address in the "LastIpUsed" field. Previously, the field displayed the load balancer or proxy IP in environments using one of those. SF05283977/SEG-133073

### Resolved issues

- A Deep Security Agent conflict with network interface controllers (NICs) caused systems with multiple NICs to crash. 05048124/SEG-126094/DS-68730
- When an Integrity Monitoring scan timed out, it sometimes generated false "create" or "delete" events for "user" or "group" entities. SEG-117739/DS-66885
- Application Control, Anti-Malware, and Real-time Integrity Monitoring failed to function properly for Deep Security Agents with certain combinations of Integrity Monitoring rules configured. DS-68494
- A Deep Security Agent parsing issue was causing "Anti-Malware Engine Offline" errors. SF05171312/SEG-129367/DSSEG-7428

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. DS-68180

Highest Common Vulnerability Scoring System (CVSS) score: 9.1

Highest severity: High

## Deep Security Agent - 20.0.0-3445 (20 LTS Update 2021-11-24)

Release date: November 24, 2021

Build number: 20.0.0-3445

### New features

**Collection of the agent metrics in the on-premise environment**: You can now collect the agent metrics on-premises for SEG troubleshooting purposes. These metrics are stored as ZIP files on Windows in the `C:\ProgramData\Trend Micro\Deep Security Agent\metrics` directory and on Linux, AIX, and Solaris in the `/var/opt/ds_agent/metrics` directory. The ZIP files are rotated periodically on the local file system.

Each ZIP file is approximately 1 MB in size and contains up to 100 files. The metrics are collected along with the diagnostic package.

## Enhancements

- Deep Security Agent sometimes crashed when it could not connect to Deep Security Manager. DS-67654
- Deep Security Agent no longer uses CBC cipher suites by default in order to improve security. DS-67204
- Deep Security Agent was upgraded to use locally installed kernel modules when new ones can't be fetched from the Deep Security Relay. DS-66599
- Updated Deep Security Agent to support using the "process name" property in "ignore from source" rules for Application Control Trust Entities on Cloud One Workload Security. DS-67322
- Updated Deep Security Agent's database size management to optimize disk space usage. DS-67347

## Resolved issues

- Insufficient file access permission for the Deep Security Relay sometimes caused the agent installer to fail. DS-67278
- Deep Security Agent sometimes showed an incorrect "No such file or directory" error message during installation. DS-67317
- Deep Security Agent sometimes showed plugin installation failures during an upgrade even when the upgrade was successful. DS-67336
- Deep Security Agent sometimes could not start after an upgrade. SF04943063/SEG-123155/DS-67475
- Deep Security Agent sometimes changed the access time of files during the on-demand Anti-Malware scan. DS-67119
- The Deep Security Agent and MQTT connection would sometimes go offline, requiring an agent restart. DS-67487
- Deep Security Agent couldn't properly handle SAP NetWeaver MIME type scan requests containing leading and trailing spaces. DS-67448
- With Anti-Malware real-time scan enabled, Deep Security Agent would sometimes scan unchanged files. DS-67806

- Deep Security Agent sometimes caused the system to crash. SEG-123338/DS-67445

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-6489/DSSEG-7210/DS-65113/DS-67367

Highest Common Vulnerability Scoring System (CVSS) score: 9.8

Highest severity: High

## Deep Security Agent - 20.0.0-3288 (20 LTS Update 2021-10-28)

Release date: October 28, 2021

Build number: 20.0.0-3288

### New features

**Kernel support package updates**: You can now choose when to perform kernel support package updates, using the new "Automatically update kernel package when agent restarts" option in the computer or policy editor.

**Evolution of the agent installer**: The Deep Security Agent installer now installs most agent content. This results in the following changes:

- Agent size requirements have increased, including a slightly larger installer package on most platforms.
- All agent content is now installed on the computer being protected. Content remains unloaded on a computer until a plug-in is activated by a policy or by the manager console.
- The agent is now much less dependent on relays because all plug-in installations use the content already installed with the agent. This mitigates plug-in install

issues due to relay communications because plug-ins can be installed without a connection to a relay.

#### Enhanced platform support

- **Deep Security Agent 20.0.0-3288 or later now supports these platforms**:
  - AlmaLinux 8 (requires Deep Security Manager 20.0.503+)
  - Rocky Linux 8 (requires Deep Security Manager 20.0.543+)
  - Ubuntu 20.04 (AWS Arm-based Graviton 2) (requires Deep Security Manager 20.0.503+)
  - Ubuntu 18.04 (AWS Arm-based Graviton 2) (requires Deep Security Manager 20.0.482+)
- **Secure boot support**: Deep Security Agent now supports Oracle Linux 7 (in both UEK-R5 and UEK-R6) and Oracle Linux 8 with Secure Boot enabled.

### Enhancements

- Deep Security Agent 10.0 to 20.0 upgrades now keep their "NIC bypass" configuration (used for bypassing a network interface). DS-64985
- You can now exclude container file events from the kernel module. DS-65547

### Resolved issues

- Anti-Malware updates sometimes failed, resulting in "Security Update: Pattern Update on Agents/Appliances Failed" errors. 04763356/SEG-119138/DS-66569
- The Deep Security Agent Scanner library sometimes couldn't be loaded by SAP NetWeaver. DS-67530
- With Intrusion Protection enabled, Deep Security Agent caused the system to crash under some configurations. SF04931669/SEG-123338/DS-67441
- With SAP integrated and running, Deep Security Agent would block MP4 files. 04660120/SEG-117094/DSSEG-7254
- Deep Security Agent sometimes was unable to connect to the manager via proxies. DS-65929
- Deep Security Agent sometimes showed package signature errors during an upgrade because of a mismatched Certification Revocation List (CRL). DS-65056

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. DS-46018/DSSEG-7210/DSSEG-7217

Highest Common Vulnerability Scoring System (CVSS) score: 7.8

Highest severity: High

## Deep Security Agent - 20.0.0-3165 (20 LTS Update 2021-10-08)

Release date: October 08, 2021

Build number: 20.0.0-3165

**Note:** Deep Security Agent 20.0.0.3165 has been released to Trend Micro Cloud One - Workload Security customers. However, it is not available on the Deep Security Agent software download page or released to customers using Deep Security Manager.

### New features

- **AlmaLinux 8 support**: Deep Security Agent is now supported on AlmaLinux 8.
- **Ubuntu 18.04 (AWS Arm-based Graviton 2) support**: Deep Security Agent is now supported on Ubuntu 18.04 (AWS Arm-based Graviton 2).
- **Oracle Linux 7 support**: Deep Security Agent is now supported on Oracle Linux 7 with Secure Boot (in both uek-R5 and uek-R6).
- **Kernel support package updates**: You can now choose when to perform kernel support package updates, using the new **Automatically update kernel package when agent restarts** option in the computer or policy editor.
- **Evolution of the agent installer**: The Deep Security Agent installer now installs most agent content. This results in the following changes:
  - Agent size requirements have increased, including a slightly larger installer package on most platforms.

  - All agent content is now installed on the computer being protected. Content remains unloaded on a computer until a plug-in is activated by a policy or by the manager console.
  - The agent is now much less dependent on relays because all plug-in installations use the content already installed with the agent. This mitigates plug-in install issues due to relay communications because plug-ins can be installed without a connection to a relay.

### Enhancements

- Updated Deep Security Agent to prevent agents upgraded from version 10.0 to 20.0 from losing their "NIC bypass" configuration (used for bypassing a network interface). DS-64985
- You can now exclude container file events from the kernel module. DS-65547

### Resolved issues

- Deep Security Agent sometimes was unable to connect to Manager via proxies. DS-65929

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. DSSEG-7210/DSSEG-7217

Highest Common Vulnerability Scoring System (CVSS) score: 7.8

Highest severity: High

## Deep Security Agent - 20.0.0-2971 (20 LTS Update 2021-09-08)

Release date: September 08, 2021

Build number: 20.0.0-2971

## New features

**FIPS mode on Red Hat Enterprise Linux 8**: Deep Security Agent 20.0.0-2971 or later now supports FIPS mode for Red Hat Enterprise Linux 8.

**FIPS mode on Amazon Linux 2**: Deep Security Agent 20.0.0-2971 or later now supports FIPS mode for Amazon Linux 2.

## Enhancements

- Updated Deep Security Agent to improve performance and compatibility by using a unified driver for file, process, and network events. DS-61784
- Updated Deep Security Agent to improve TLS traffic inspection. This feature is being rolled out gradually, beginning with Trend Micro Cloud One - Workload Security customers. DS-15576
- Updated Deep Security Agent to improve connectivity with Deep Security Manager during agent deployment and activation. DS-62547

## Resolved issues

- Deep Security Agent sometimes caused performance issues on systems with folders in NFS format. SF04816680/SEG-118993/DS-66280
- With Integrity Monitoring enabled, Deep Security Agent sometimes caused high CPU usage. DS-65986
- Deep Security Agent 20.0.0-2740 fr Linux was causing performance and third-party compatibility issues on some systems. This agent was removed from the Trend Micro Download Center. For more information see Removal of Deep Security Agent (DSA) Build 20.0.0-2740 for Linux from Download Center.
- Deep Security Agent console commands sometimes failed to return proxy information for Deep Security Relay or Deep Security Manager. DS-65419
- Deep Security Agent sometimes failed to properly display items under **Events and Reports**. DSSEG-7057
- Deep Security Agent was sometimes unable to create or manage tasks on RPM-based platforms due to a SystemD (Linux service manager) process limitation. SF04543580/SEG-113833/DS-65550

- Deep Security Agent Anti-Malware Real-Time Scan exclusions sometimes failed within container environments. DS-65528
- Deep Security Agent Anti-Malware Real-Time Scan directory exclusions sometimes failed if filenames were not in UTF-8 format. SEG-115198/DS-65495
- With Anti-Malware enabled, Deep Security Agent encountered an "Insufficient Disk Space" alert which sometimes crashed the agent or stopped other programs from working properly. SF04584157/SEG-113377/DS-64405
- Deep Security Agent failed to execute some agent-initiated (dsa_control) console commands. 04564385/SEG-112050/DSSEG-6990
- Deep Security Agent sometimes crashed while trying to establish a connection with Deep Security Manager. 04634804/SEG-113539/DS-64862
- Deep Security Agent sometimes lost connectivity while trying to establish an SSL connection. SF04323898/SEG-107451/DS-64268
- Deep Security Agent was sometimes unable to connect to web applications on systems with older OS versions. SF04451029/SEG-109652/DS-64528
- Deep Security Agent upgrade (**Administration > Updates > Software**) sometimes failed if a previous (RPM package) upgrade was triggered using console commands. SF04586071/SEG-113583/DS-64978
- With Web Reputation enabled, Deep Security Agent caused connectivity issues for some third-party software. SF04072723/SEG-97952/DSSEG-6963
- With Integrity Monitoring enabled, Deep Security Manager caused high CPU usage on the authentication server for some systems. 04488319/SEG-110088/DS-63855
- With Integrity Monitoring real-time scan enabled, Deep Security Agent sometimes prevented files on network drives from being deleted. SEG-108636/C1WS-1787

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. SF04613197/SEG-113566/DS-64050

Highest Common Vulnerability Scoring System (CVSS) score: 9.8

Highest severity: High

## Deep Security Agent - 20.0.0-2593 (20 LTS Update 2021-07-01)

Release date: July 01, 2021

Build number: 20.0.0-2593

### New feature

**FIPS mode on Ubuntu 18.04**: Deep Security Agent 20.0.0-2593 or later now supports FIPS mode for Ubuntu 18.04.

### Resolved issues

- Integrity Monitoring alerts sometimes triggered but did not appear in the **Events and Reports** tab. 04266346/SEG-103731/DS-62992
- Deep Security Agent sometimes triggered multiple "Log Inspection Engine Initialized" alerts due to an agent-manager communication issue. SF03968169/SEG-95731/DS-60840
- Application Control was detecting multiple "Application Control Software Changes Detected" events due to '.tmp" files being generated by PowerShell. C1WS-1608

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-5850/DS-54705

Highest Common Vulnerability Scoring System (CVSS) score: 4.4

Highest severity: Medium

## Deep Security Agent - 20.0.0-2395 (20 LTS Update 2021-05-24)

Release date: May 24, 2021

Build number: 20.0.0-2395

### New features

#### Enhanced platform support

- Application Control and Integrity Monitoring for Amazon Linux 2 (AWS Arm-based Graviton 2): Deep Security Agent now supports Application Control and Integrity Monitoring for Amazon Linux 2 on AWS Graviton 2. DS-62775

### Enhancements

- Deep Security Agent 20.0.0-2395 or later now supports Entrust Root Certificate Authority (G2) certificates. Non-G2 security certificates expire on 2022/07/09. After that date, only Deep Security Agent 20.0.0-2395 or later will have the latest Anti-Malware Smart Scan protection. DS-63010
- Updated Deep Security Agent to add Predictive Machine Learning support for Malware Scan on Linux platforms. DS-62857
- Updated Deep Security Agent's Anti-Malware default configuration to monitor file access from the local host only, improving compatibility for some file systems. DS-62222

### Resolved issues

- Anti-Malware Real-Time Scan sometimes didn't detect files properly with the "During read" setting selected (**Computers > Details > Anti-Malware > General > Real-Time Scan > Malware Scan Configuration > Edit > Advanced > Real-Time Scan**). SEG-104496/DS-61836
- Deep Security Agent was unable to install in some environments because it misidentified the OS. DSSEG-2915/DS-28321
- Deep Security Agent sometimes showed package signature errors during an upgrade because of a mismatched Certification Revocation List (CRL). DS-62154

- Anti-Malware Real-Time Scan sometimes caused high CPU usage. 04331007/SEG-107814/DS-62593
- Insufficient host information caused by connectivity issues sometimes resulted in offline or duplicate listings in the **Computers** tab for Deep Security Agents on AWS workspaces. SF04198134/SEG-102818/DS-61666
- Anti-Malware Real-Time Scan caused unintentional file changes under some configurations. DS-62412
- Deep Security Agent sometimes could not successfully perform an upgrade because of a missing package. SF04302125/SEG-104084/DS-62692
- Anti-Malware kernel modules sometimes did not bypass file activity on remote shared storages when Network Directory Scan was disabled. DS-62985

## Deep Security Agent - 20.0.0-2204 (20 LTS Update 2021-04-12)

Release date: April 12, 2021

Build number: 20.0.0-2204

### New feature

#### Enhanced platform support

- Anti-Malware and Log Inspection support for Amazon Linux 2 (AWS Arm-based Graviton 2): Deep Security Agent 20.0.0-2204 or later now supports the Anti-Malware, Firewall, Intrusion Prevention, Log Inspection, and Web Reputation protection modules. Note that Advanced Threat Scan Engine (ATSE) update is not currently supported for Amazon Linux 2 on AWS Graviton 2, but will be added in a future release.

### Resolved issues

- With Anti-Malware enabled, Deep Security Agent sometimes caused "defunct processes" (that is, processes that remain in the system process table after they've completed execution). SEG-104452/DS-61593
- When Application Control was in block mode, it was unable to build a proper software inventory in some cases. DS-58813

- When Web Reputation was enabled, the system sometimes crashed. SF04258834/SEG-102756/DS-61067
- When Integrity Monitoring real-time scan was enabled, sometimes directories on NFS volumes couldn't be removed. SF03977538/SEG-98656/DS-61062
- When Intrusion Prevention was enabled, the system would crash under some configurations. SF04286712/SEG-103971/DS-61274
- A proxy server issue sometimes caused connectivity issues with Deep Security Agents after registering with Trend Micro Vision One (XDR). SF04318864/SEG-104847/DS-61516

## Deep Security Agent - 20.0.0-2009 (20 LTS Update 2021-03-08)

Release date: March 08, 2021

Build number: 20.0.0-2009

### Enhancements

- Updated Deep Security Agent to include CPU information (number of logical cores) to improve diagnostics and performance tracking. DS-60011

### Resolved issues

- The MQTT connection went offline because an old MQTT connection was not properly cleaned. SF04236908/SEG-102056/DS-60893
- When Firewall, Intrusion Prevention, and Web Reputation were enabled, the system sometimes crashed. SF03992370/SEG-100828/DS-60589
- After restarting Deep Security Virtual Appliance, protected VMs sometimes became inaccessible. SEG-94723/SF03949466/DS-58962

## Deep Security Agent - 20.0.0-1876 (20 LTS Update 2021-02-08)

Release date: February 08, 2021

Build number: 20.0.0-1876

### Resolved issues

- The Deep Security Agent was sometimes unable to establish an SSL connection to the web server. DS-59893

## Deep Security Agent - 20.0.0-1822 (20 LTS Update 2021-01-18)

Release date: January 20, 2021

Build number: 20.0.0-1822

### New features

#### Enhanced platform support

- Amazon Linux 2 (AWS Arm-based Graviton 2): Deep Security Agent now supports Amazon Linux 2 on AWS Graviton 2. The agent currently supports the Firewall, Intrusion Prevention, and Web Reputation protection modules. Other protection modules are coming soon.

**Behavior Monitoring for Linux**: This release adds support for Behavior Monitoring on the Linux platform.

## Deep Security Agent - 20.0.0-1681 (20 LTS Update 2021-01-04)

Release date: January 04, 2021

Build number: 20.0.0-1681

### Resolved issues

- A driver conflict was causing the Deep Security Agent to hang and require a reboot. SEG-94278/SF03941184/DS-59020
- If an error related to Secure Boot occurs, the user is no longer blocked from installing the plugins and receive a "Secure Boot" error message on Deep Security

Manager. Instead, an "Engine is offline" error message is displayed. Users can check "Secure Boot" entries in ds_agent.log for error details. DS-58374

- In the SecureBoot environment, the SUSE15 SP2 kernel module load failed with kernel version 5.3.18-24.37-default or later. SEG-93737/DS-58373
- Anti-Malware would sometimes restart before fully loading a new driver, causing the AM engine to be offline. DS-58475

## Deep Security Agent 20.0.0-1559 (20 LTS Update 2020-12-07)

Release date: December 07, 2020

Build number: 20.0.0-1559

### New features

**TLS Directionality**: The manager heartbeat port can now act as both a TLS client and TLS server. Future agents will connect as TLS clients, not TLS servers. This resolves issues with agent-initiated connections through a proxy or firewall that requires TLS sessions to be initiated in the same direction as the TCP layer of the connection.

### Enhancements

- Improved Deep Security Relay's performance by only checking packages that have been modified. DS-55527
- Enhanced memory usage to improve performance. DS-53012
- Anti-Malware on-demand scans did not function as expected. DS-58346

### Resolved issues

- Deep Security Agent didn't detect Secure Boot state correctly. SEG-89042/03730368 /DS-57014
- The error "scheduling while atomic" occurred because the dsa_filter caused kernel panic. DS-56514
- Anti-Malware events didn't include file hashes in certain scenarios. SEG-91779/SF03818756/DS-57453
- The Anti-Malware driver showed warning messages during the initialization. SEG-92204/03784490/DS-57605

- After upgrading to Deep Security Agent 20.0.0-1194, the "Intrusion Prevention Rules Failed to Compile" and "Security Update Failed" errors sometimes incorrectly occurred. SEG-90503/03789013/DS-56904
- When Anti-Malware real-time scans were enabled, Rancher Kubernetes pods sometimes couldn't be terminated gracefully. SEG-87824/SF03695639/DS-58220
- When Integrity Monitoring was enabled, a high amount of CPU was used. SEG-88619/03720485/DS-56613
- Application Control events occurred multiple times for the same incident. SEG-86213/SF03620055/DS-57298
- Security updates were not automatically performed on new machines. SEG-91484/SF03828068/DS-57688

## Deep Security Agent 20.0.0-1337 (20 LTS Update 2020-10-28)

Release date: October 28, 2020

Build number: 20.0.0-1337

### Resolved issues

- When Anti-Malware real-time scans were enabled in Linux, sometimes the system crashed because of a compatibility issue with third-party security software. SF03700563/SEG-88135/DS-54799
- Secure boot appeared active when it was not. SEG-85550/DS-55052

## Deep Security Agent 20.0.0-1304 (20 LTS Update 2020-10-21)

Release date: October 21, 2020

Build number: 20.0.0-1304

### Enhancements

- Updated the Integrity Monitoring scan completion time in Deep Security Manager events to display in seconds with a thousands separator. DS-54680

### Resolved issues

- For agentless protected VMs, the settings under **Policies > Intrusion Prevention > General > Recommendation** were greyed out. DS-56665
- When "Serve Application Control rulesets from relays" was enabled, unnecessary relay error events occurred. DS-50905
- Real-time Anti-Malware with filesystem hooking enabled did not work on older kernel versions. SEG-82411/DS-54271
- Deep Security Manager reported a security update timeout because Deep Security Agent received exceptions at security updates. SEG-82072/DS-54720
- Deep Security Manager sometimes showed the incorrect Log Inspection status. SEG-77081/DS-54719
- The dsa_query command didn't display Anti-Malware patterns correctly. DS-55389
- The Anti-Malware driver did not check compatibility before loading into the kernel. SEG-88135

## Deep Security Agent 20.0.0-1194 (20 LTS Update 2020-10-05)

Release date: October 5, 2020

Build number: 20.0.0-1194

### New features

**Improved performance for real-time Anti-Malware scanning on Linux**: Real-time Anti-Malware scans have been improved for Deep Security Agent on Linux, resulting in increased response time, faster processing, and reduced CPU usage. Previously, all files were scanned during read/write. Now, Anti-Malware scanning is more efficient and file scanning during write is deferred (the file is added to a queue and scanned in the background).

**Differentiated platforms**: Deep Security Manager can now distinguish between Red Hat and CentOS platforms and operations. DS-52682

**Continued network scans**: After migrating guest VMs to another ESXi host in the same cluster using vMotion, the Deep Security Virtual Appliance's network scans now continue where they left off, without delay. This feature only applies if you are using NSX-T Data

Center and guest machines are using a policy without network feature overrides. DS-50482

## Enhancements

- Real-time Integrity Monitoring explicitly matches the directory specified in the base directory. Previously, it matched all paths that started with the base directory. DS-52692
- Integrity Monitoring detects changes to the "setuid" and "setgid" attributes for Linux and Unix platforms. DS-52061
- Ceph is now excluded from file system kernel hooking to prevent kernel panic. SEG-75664/SF03131718/DS-50298
- Recommendation Scans and Integrity Monitoring are now enabled for NSX-T environments. DS-50478
- Extended the scope of the "If a computer with the same name already exists" setting on **Administration > System Settings > Agents** to apply to existing unactivated computers. Previously, it only applied to existing activated computers. DS-51800

## Resolved issues

- Secure boot appeared active when it was not. DS-55052
- Deep Security Agent could not install any plugins with UEFI Secure Boot enabled. DS-54041
- After upgrading the Deep Security Agent, the "Sending Application Control Ruleset Failed" error sometimes occurred. DS-49828
- The Anti-Malware engine on Deep Security Virtual Appliance went offline when the signer field in the Census server reply was empty. DS-49807
- Anti-Malware directory exclusion with wildcards didn't match subdirectories correctly. DS-50245
- Deep Security Agent on Linux would sometimes crash. SEG-76460/SF03218198/DS-50852
- Deep Security Agent reported incorrect network interface information. SEG-77161/DS-51397

- The Deep Security Virtual appliance did not detect the EICAR test file. SEG-71955/SF02955546/DS-49387
- Application Control did not include scripts with the extension ".bash" in the inventory. This resulted in these scripts being blocking in lock down mode. DS-50696
- The Anti-Malware driver caused a system hang on Linux platforms where autofs was used. DS-51926
- When Integrity Monitoring was enabled, the owner of a file was incorrectly changed to a user that did not exist. DS-52058
- There was an upgrade issue with Deep Security Agent which would sometimes prevent the agent from going online if Integrity Monitoring or Log Inspection were enabled. DS-50672
- Kernel Panic occurred when Web Reputation, Firewall, or Intrusion Prevention were enabled. SEG-80201/DSSEG-5846/DS-52975
- When Anti-Malware real-time scans were enabled in Linux, sometimes the system crashed because buffers from procfs were not validated. SEG-80183/DS-53204
- When a re-transmission packet with new packets was sent, it sometimes produced an "Unsupported SSL Version" Intrusion Prevention event. SEG-73893/DSSEG-5866/DS-53144
- When Deep Security real-time Anti-Malware was enabled on a Linux system, it caused a high amount of CPU usage. SEG-75739/DS-52976

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-3704/DS-41233

Highest Common Vulnerability Scoring System (CVSS) score: 4.4

Highest severity: Medium

## Deep Security Agent 20 (long-term support release)

Release date: July 30, 2020

Build number: 20.0.0.877

## New features

### Enhanced platform support

- Ubuntu 20.04 (64-bit)
- Cloud Linux 8 (64-bit)
- Debian Linux 10 (64-bit)
- Oracle Linux 8 (64-bit)
- SUSE Linux Enterprise Server 15 (64-bit)
- Red Hat Enterprise Linux 8 (64-bit)
- CentOS 8 (64-bit)

**SystemD support**: SystemD is a Linux service manager that allows services to declare dependencies, which can enforce load and unload sequences of kernel modules and other services. See "Linux systemd support" on page 412 for information about which platforms are supported. DS-37395

**Secure Boot support**: Deep Security Agent supports additional Linux operating systems with Secure Boot enabled. For details, see "Linux Secure Boot support" on page 417.

### Improved security

**Agent integrity check**: Deep Security verifies your signature on the Deep Security Agent to ensure that the software files have not changed since the time of signing.

**Protect VMs in NSX-T environments**: The latest VMware Service Insertion and Guest Introspection technologies have been integrated. This enables you to protect your guest VMs using Intrusion Prevention, Web Reputation, Firewall, Integrity Monitoring and recommendation scans on NSX-T hosts with agentless protection.

**Seamless network protection**: Deep Security Manager now sends guest VMs' network configuration to all Deep Security Virtual Appliances that are under the same cluster. The effect is that the appliances can now maintain the protection of guest machines that use the network features during and after a vMotion migration from one ESXi host to another under the same cluster. This feature only applies to NSX-T environments where the guest machine is using an assigned policy without network features overrides.

**SELinux Support**: Security-Enhanced Linux (SELinux) enforcing mode is supported on Red Hat Enterprise Linux 7 and Red Hat Enterprise Linux 8. Deep Security Agent is compatible with the default SELinux policies.

> **Note:** Anti-Malware software such as ds_agent is required to run in an unconfined domain in order to protect the system. Any additional SELinux policy customization or configuration might be block blocked or fail because of ds_agent.

**SSL improvements**: Deep Security supports handshake hello_request (rfc5246) and Extension encrypt_then_mac (rfc7366) in SSL inspection.

**Continuous Anti-Malware protection**: Deep Security Manager now sends guest VMs' Anti-Malware real-time configuration to all Deep Security Virtual Appliances that are under the same cluster. The effect is that the appliances can now maintain the protection of guest machines that use the Anti-Malware real-time feature during and after a vMotion migration from one ESXi host to another under the same cluster. This feature only applies to NSX-T environments.

#### Improved management and quality

**Automate the upgrade of agents in your environment**: Deep Security gives you the flexibility to decide if new agents, when activated, should be upgraded to a newer version if one is available. This can be particularly useful in cases where application teams are using older golden images containing a version of the agent that is out of date. Simply enable upgrade on activation, define the lineup of agents you want to use in your environment using Agent Version Control, and as older agents come online and activate they are automatically upgraded for you.

**NSX-T Network Throughput improvement**: By introducing the Data Plane Development Kit (DPDK), the network throughput has been made three times faster when compared with prior technology.

**Upgrade to supported paths**: The Upgrade on activation feature only upgrades the agent on the computer from the last two major releases. If the agent does not meet the criteria, you must upgrade the agent manually to a release within the last two major releases. Then the Upgrade on activation feature detects the newer version and complete the upgrade to the designated release.

**Protection for AWS accounts with incorrect credentials**: In the past, if your credentials were entered incorrectly for AWS accounts in Deep Security, the agent failed to activate.

This might have occurred because the credentials were entered incorrectly or because, over time, the credentials changed without a corresponding update on Deep Security. To help ensure protection remains in place in this situation, which in many cases is a simple configuration error, the computer is now created outside of the account and the agent is allowed to activate.

**Instance Metadata Service Version 2 (IMDSv2) support**: IMDSv2 is supported in this release. For details, see "How does Deep Security Agent use the Amazon Instance Metadata Service?" on page 1691

**Actionable recommendations for scan failures**: The Deep Security Agent provides actionable information about why a scheduled malware scan has been cancelled, and the recommended actions that should be taken to remedy the failure. For more information, see "Anti-Malware scan failures and cancellations" on page 1054.

**Improved process exceptions**: The process exception experience has been improved in the following ways:

- Information about why process exclusion items are not functioning correctly is provided, enabling you to troubleshoot the issue and know which actions to take to resolve it.
- The process exception configuration workflow has been improved to make it more robust.

## Enhancements

- Integrity Monitoring detects changes to the "setuid" and "setgid" attributes for Linux and Unix platforms.
- Improved the heartbeat handling for Amazon WorkSpaces deployments when the workspace sync feature is not turned on for the matching AWS connector.
- Extended the scope of the **If a computer with the same name already exists** setting on **Administration > System Settings > Agents** to apply to existing unactivated computers. Previously, it only applied to existing activated computers.
- Improved the Deep Security Agent activation experience in the following ways:
    - Enhanced the agent-initiated activation experience by displaying the activation status (for example, a success message or a message that explains a newer Deep Security Manager version is required) on Deep Security Manager.

- After migrating guest VMs to another ESXi host in the same cluster using vMotion, the Deep Security Virtual Appliance's Anti-Malware real-time scans now continue where they left off, without delay. This feature only applies to NSX-T environments.
- Increased the scan engine's URI path length limitation.
- Added the ability for Deep Security Agent Anti-Malware to scan compressed files no matter their data types when IntelliScan is disabled.
- Enhanced Linux real-time Anti-Malware performance when executing a Docker pull command.
- Improved the time it takes to auto-activate guest VMs protected by the Deep Security Virtual Appliance in an NSX-T environment.

  > **Note:** This feature requires Deep Security Manager FR 2019-12-12 or newer releases.

- Streamlined event management for improved agent performance.
- Added the ability to enable or disable Common Scan Cache for each agent through a CLI command.
- Enhanced the Malware Scan Failure event description to indicate the possible reason.
- Enhanced the Anti-Malware kernel level exclusion on Linux. File events coming from remote file systems won't be handled by Deep Security Agent anymore when Network Directory Scan is disabled.
- Added the ability to retrieve process and container information for Intrusion Prevention events, including process name, container ID, container name, image name, image digest and pod ID.

## Resolved issues

- When Anti-Malware real-time scans were enabled in Linux, sometimes the system crashed because buffers from procfs were not validated. SEG-80183/DS-53204
- When Deep Security real-time Anti-Malware was enabled in Linux, it caused a high amount of CPU system usage. SEG-75739/SF03036857/DS-52976
- Ceph caused kernel panic. SEG-75664/SF03131718/DS-50298
- Deep Security Agent sometimes crashed. SEG-76460/SF03218198/DS-50852

- Deep Security Agent reported incorrect network interface information. SEG-77161/DS-51397
- Application Control did not include scripts with the extension ".bash" in the inventory. This resulted in these scripts being blocked in lock down mode. SEG-73174/DS-50696
- Deep Security Virtual Appliance sometimes went offline. SEG-53294/DS-46728
- The interface isolation feature was still on when Firewall was turned off. SEG-32926/DS-27099
- In a Red Hat Enterprise Linux 5 or 6 or a CentOS 5 or 6 environment, Integrity Monitoring events related to the following rule were displayed even if users or groups were not created or deleted: 1008720 - Users and Groups - Create and Delete Activity. SEG-22509/DS-25250
- Integrity Monitoring events showed an incorrect file path with Unicode encoding. SEG-45239/DS-33911
- Anti-Malware events displayed a blank file path with invalid Unicode encoding. SEG-46912/DS-34011
- Certain data structures in the Deep Security Agent packet engine were cleaned up prematurely, leading to a kernel panic and system crash. SF01423970/SEG-43481/DS-34436
- Kernel panic occurred when dsa_filter.ko was obtaining network device's information. SEG-50480/DS-35192
- An SAP system with Java running in a Linux environment failed to start when Deep Security Scanner returned an error code without an error message. SF01339187/SEG-38497/SEG-33163/DS-31330
- Kernel panic occurred because of redirfs. SF01137463/SEG-34751/DS-32182
- Deep Security Anti-Malware caused the fusermount process to fail when mounting the filesystem. SF01531697/SEG-43146/DS-32753
- Deep Security Agent's Intrusion Prevention module silently dropped zero payload UDP packets. SEG-39711/DS-32799
- For Web Reputation, Deep Security Agent sent the incorrect credentials to the proxy, which returned HTTP 407. SF01704358/SEG-45004/DS-32077
- Deep Security Agent GSCH driver had an issue with another third-party file system. SF01248702/SEG-44565/DS-33155)

- The Environment Variable Overrides for Deep Security Anti-Malware did not work in Linux. SEG-43362/DS-31328
- Deep Security Agent process potentially crashed when the detailed logging of SSL message was enabled and outputted. SF01745654/SEG-45832/DS-33007
- When multiple Smart Protection Servers were configured, the Deep Security Agent process would sometimes crash due to an invalid sps_index. SF01415702/SEG-42919/DS-33008
- The Send Policy action failed because of a GetDockerVersion error in Deep Security Agent. SF1939658/SEG-49191/DS-34222
- Deep Security Agent sent invalid JSON objects in response to Deep Security Manager, which caused errors in Deep Security Manager's log file. SF01919585/SEG-48728/DS-34022
- The ds_agent process would sometimes crash under certain conditions when Integrity Monitoring was enabled. SEG-50728/DS-35446
- Deep Security Agent failed to install on Ubuntu 18.04. SF01593513/SEG-43300/DS-37359
- The Deep Security Agent network engine crashed because the working packet object was deleted accidentally. SF01526046/SF02159742/SEG-55453/DS-38812
- Unicode user names could not be displayed in real-time Integrity Monitoring file scan events. SF02187371/SEG-56645/DS-39398
- The agent operating system would sometimes crash when Firewall interface ignores were set. SF01775560/SEG-49866/DS-39339
- Deep Security Agent did not add Python extension module (PYD) files to the inventory of Application Control. SF01804378/SEG-47425/DS-33690
- Too many file open events were being processed in user mode, resulting in high cpu usage. SF02179544/SEG-55745/DS-39638
- The "mq_getattr: Bad file descriptor" error occurred while accessing the message queue when Deep Security real-time Anti-Malware was enabled. SF02042265/SEG-52088/DS-39890
- Linux kernel logs were flooded by Deep Security Anti-Malware driver. SF02299406/SEG-57561/DS-41589

- Non-executable files that were opened with execute permissions resulted in security events and drift that should not have been generated. SF01780211/SEG-46616/DSSEG-3607
- High CPU use occurred when Application Control was enabled and the host application was creating a high volume of non-executable files. SF02179544/SEG-55745/DS-41142
- Deep Security Agent real-time Anti-Malware scans didn't work with Debian 10 64-bit.
- When a guest VM was migrated between ESXi hosts frequently (using vMotion), sometimes the VM couldn't save the state file. This caused the guest to lose the protection of the Deep Security Virtual Appliance for several minutes after migration, until the VM was reactivated by Deep Security Manager automatically under the new ESXi server. DSSEG-4341/DS-38221
- When uninstalling Deep Security Agent in Linux, the uninstall log included a typo. DSSEG-4139/DS-34504
- Deep Security Anti-Malware detected sample malware files but did not automatically delete them. SF02230778/SEG-55891/DS-40687
- When the Deep Security Agent connected through a proxy to the Deep Security Manager on Deep Security as a Service, Identified Files could not be deleted. SF01979829/SEG-51013/DS-37252
- After applying rule 1006540, "Enable X-Forwarded-For HTTP Header Logging", Deep Security would extract the X-Forwarded-For header for Intrusion Prevention events correctly. However, a URL intrusion like "Invalid Traversal" would be detected in the HTTP request string before the header was parsed. The Intrusion Prevention engine has been enhanced to search X-Forwarded-For header after the header is parsed. SEG-60728/DSSEG-5094
- Deep Security Agent sent invalid JSON objects in response to Deep Security Manager, which caused errors in Deep Security Manager's log file. SF01919585/SEG-48728/DSSEG-4995

## Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-3704/VRTS-3176

Highest Common Vulnerability Scoring System (CVSS) score: 7.8

Highest Severity: High

- Updated NGINX to 1.16.1 (DSSEG-4600)
- Updated to curl 7.67.0.
- Updated to openssl-1.0.2t.
- Updated JRE to the latest Java Update (8.0.241/8.43.0.6).

### Kernel support

To see which Linux kernels are currently supported, see "Linux kernel compatibility" on page 408.

To view the Linux kernel support release history, see the Readme for Trend Micro (TM) Deep Security Agent 20.0 for Linux.

### Known issues

- Autofs is currently not supported for use when real-time Anti-Malware is enabled. If autofs is used with real-time Anti-Malware enabled, some mountpoints are unmounted successfully. SEG-58841

Windows

## Deep Security Agent - 20.0.3-860 (20 LTS Update 2026-01-21)

Release date: January 21, 2026

Build number: 20.0.3-860

### New features

**Endpoint Event Viewer**: Access Endpoint Event Viewer to view all security and system events across managed computers with filtering by period, severity, event origin, and action. This is only supported for Trend Vision One - Server & Workload Protection.

### Resolved issues

- Deep Security Agent crashed when syslog hostnames were longer than 64 characters. PCT-87531/DSA-14252
- When Web Reputation Service was enabled, system memory usage continuously increased. PCT-80352/DSA-13866
- Deep Security Agent sometimes crashed when processing HTTP/2 packets that were formatted differently from what the agent expected. PCT-85552/DSA-13755
- After Deep Security Agent restarted, Intrusion Prevention Detection sometimes stopped working. PCT-82352/DSA-13755
- Deep Security Agent was unable to send its status to Deep Security Notifier when managed by Trend Vision One - Server & Workload Protection. For details, see Trend Micro™ Deep Security™ Notifier displays an "Unknown/Unreachable" status for Deep Security Agent. PCT-87617/PCT-87643/PCT-87679/PCT-87740/PCT-87829/DSA-14115

## Deep Security Agent - 20.0.2-29810 (20 LTS Update 2025-12-24)

Release date: December 24, 2025

Build number: 20.0.2-29810

### Resolved issues

- Application Control failed to retain the inventory when a ruleset update was applied. For details, see Trend Vision One™ Server & Workload Protection, Cloud One Workload Security, and Deep Security Application Control may fail to save the inventory when updating rules. DSA-13750

## Deep Security Agent - 20.0.2-29760 (20 LTS Update 2025-12-09)

Release date: December 09, 2025

Build number: 20.0.2-29760

## Enhancements

- Firewall and Intrusion Prevention System events now display process and user info if that data is available. This is being rolled out gradually to all customers. DSA-13741
- Strong cipher (`app.relay.strongciphers=true`) and minimum Transport Layer Security (TLS) version (`app.relay.restrictRelayMinimumTLSProtocol=TLSv1.2`) can now be set in the Deep Security Agent configuration file for agents using Deep Security Relay. DSA-2163
- Advanced Threat Scan Engine has been updated to version 25.560. DSA-11917

## Resolved issues

- Uploading logs using the File Collection or Custom Script functions failed on some systems. This issue only affected Trend Vision One. V1E-115291
- Software builds took much longer on certain systems running Deep Security Agent with Device Control enabled. PCT-76169/V1E-114202
- Trend Vision One - Deep Security Agent did not populate the **Last updated** column in the **Software information** tab of Trend Vision One Endpoint Security. V1E-64601
- Anti-Malware protection sometimes stopped working when the operating system was running in low power mode (with the laptop screen off or closed, for example). DSA-13698/DSA-11913
- After upgrading to Deep Security Agent 20.0.2.22850 or 20.0.2.26670, the enhanced recommendation scan would disable and not automatically re-enable. When this issue occurred, the system reverted to using classic recommendation scan after 36 hours to ensure continued functionality. This issue only affected Endpoint & Workload Security. WS-13982

## Security updates

This release contains updates to third-party libraries. DSA-7695/DSA-13181/DSA-13204

### Known issues

- Application Control fails to retain the AC inventory when a ruleset update is applied.

  **Recommended actions:**
  - If you have agents running Application Control that have not been upgraded to version 20.0.2-29760, do not upgrade these agents.
  - If you have agents running Application Control that have already been upgraded to version 20.0.2-29760, perform the following actions in order:
    a. Disable Application Control's block mode for all 20.0.2-29760 agents that have Application Control enabled.
    b. Downgrade all agents that have Application Control enabled to a previous agent version.
    c. Re-enable Application Control block mode for these agents, if desired.

  For more information see Trend Vision One™ Server & Workload Protection, Cloud One Workload Security, and Deep Security Application Control may fail to save the inventory when updating rules. DSA-13750

## Deep Security Agent - 20.0.2-26670 (20 LTS Update 2025-11-12)

Release date: November 12, 2025

Build number: 20.0.2-26670

### New features

**User-based Firewall**: Firewall rules can now be configured based on user account. This feature is being rolled out gradually to all customers.

**Enhanced HTTP/2 support**: The Intrusion Prevention System engine now supports inbound HTTP/2 connections. This feature will be rolled out gradually through backend updates to ensure stability and performance enhancements. (This release also includes fixes aimed at improving HTTP/2 handling and security. PCT-77306/DSA-13105)

**Windows 11 25H2 support**: Deep Security Agent 20.0.2-26670 or later supports Windows 11, version 25H2.

### Resolved issues

- Events failed to generate for some Smart Protection Server connection issues. PCT-55362/DSA-11534
- Web Reputation Service was not working in Google Chrome version 140 or later when the browser was running in incognito mode. DSA-13161
- Deep Security Agent sometimes crashed due to an issue in the MQTT code. PCT-79555/DSA-3839

## Deep Security Agent - 20.0.2-22850 (20 LTS Update 2025-10-08)

Release date: October 08, 2025

Build number: 20.0.2-22850

### Enhancements

- Advanced TLS Traffic Inspection now supports TLS 1.3 on Windows 11, Windows Server 2022, and Windows Server 2025. DSA-12834

## Deep Security Agent - 20.0.2-20480 (20 LTS Update 2025-09-17)

Release date: September 17, 2025

Build number: 20.0.2-20480

### Enhancements

- Log Inspection now supports glob character in directory names. PCT-8309

### Resolved issues

- Deep Security Agent running with Application Control enabled led to a memory leak on some systems. DSA-12148
- Restoring quarantined files would fail if no real-time scan configuration existed. PCT-73666/DSA-12139

### Known issues

- Web Reputation Service is not working in Google Chrome version 140 or later if the browser is running in incognito mode. DSA-13001

## Deep Security Agent - 20.0.2-17700 (20 LTS Update 2025-08-13)

Release date: August 13, 2025

Build number: 20.0.2-17700

### Enhancements

- Deep Security Agent now ensures the use of proper path strings when Anti-Malware Solution Platform creates temporary folders. PCT-60262/DSA-11532

### Resolved issues

- Deep Security Agent sometimes crashed when establishing a heartbeat connection. PCT-66595/DSA-11386

## Deep Security Agent - 20.0.2-14490 (20 LTS Update 2025-07-09)

Release date: July 09, 2025

Build number: 20.0.2-14490

### New features

**Agent Interface**: Agent Interface allows Trend Vision One to manage agent and component updates, and to trigger scans for any endpoint with the Trend Micro Endpoint Basecamp (XBC) agent installed. This is currently only supported for Trend Vision One - Server & Workload Protection.

### Enhancements

- When Advanced TLS Traffic Inspection is enabled, Deep Security Agent now injects packets to speed up the connection as long that connection is not blocked. PCT-63207/DSA-10919

### Resolved issues

- On demand scans could not be started manually until an automatic scan had been triggered, after either an activation or a restart of Deep Security Agent. WS-12581
- Deep Security Agent changed its language setting to the system's default language after a remote upgrade. PCT-52649/DSA-11221
- After changing to a higher detection level, files previously deemed safe by Predictive Machine Learning were being excluded from scans when they should have been included. DSA-11204

## Deep Security Agent - 20.0.2-12290 (20 LTS Update 2025-06-11)

Release date: June 11, 2025

Build number: 20.0.2-12290

### Enhancements

- Enabled by default, Web Reputation Service now uses Server Name Indication (SNI) queries when determining the risk level of a website.
- Activity Monitoring now supports JavaServer Page (JSP) files. V1E-54751
- Process Memory Scan results now provide additional information about the cause of a scan when multiple scans are triggered by the same process identifier (PID).

You can find more details by searching for "trigger_info" in the Vision One Endpoint Security Search app (**XDR Threat Investigation > Search**). Only suspicious detections support trigger_info at this time. DSA-9085

### Resolved issues

- Deep Security Agent sometimes crashed during SSL handshake. PCT-55526/DSA-9902
- Enhanced Recommendation Scan failed due to unexpected registry values. WS-12303
- When Web Reputation Service was enabled, Deep Security Agent sometimes crashed on systems with x86 architecture. DSA-11060
- Deep Security Agent upgrade was sometimes unsuccessful when using Trend Vision One version control policies. PCT-52924/PCT-61392/PCT-62122/DSA-10972
- Deep Security Agent incremental pattern updates sometimes failed, even when the full pattern update was available as an alternative download option. PCT-64289/PCT-65578/DSA-10953
- The system would sometimes hang when Anti-Malware Solution Platform (AMSP) was trying to write a log. PCT-41894/PCT-48493/PCT-51094/PCT-54129/PCT-54163/PCT-61016/PCT-64506/DSA-10327

### Security updates

This release contains updates to third-party libraries. DSA-10530

## Deep Security Agent - 20.0.2-9810 (20 LTS Update 2025-05-14)

Release date: May 14, 2025

Build number: 20.0.2-9810

### Enhancements

- The Trend Micro Deep Security Web Reputation App (`dsa-wrs-app.exe`) is now called the Trend Micro Web Reputation App. DSA-9779

- Web Reputation Service now points to a 403 Forbidden rather than a 200 OK page when blocking an http proxy connection to a suspicious or malicious site. PTC-60576/DSA-10325

### Resolved issues

- Deep Security Agent configurations using advanced TLS caused some systems to freeze. PCT-63207/DSA-10380
- The URL column for **Web Reputation Events** was sometimes missing information. PCT-60576/DSA-10090
- Some systems experienced a Blue Screen (BSoD) error. PCT-60927/DSA-10191
- Offline Scheduled Scan sometimes used the Server & Workload Protection time zone when it should have used the Deep Security Agent time zone, causing Weekly and Daily scans to trigger at the wrong time, and causing high CPU usage for Monthly scans when triggered on the last day of a month. PCT-55169/DSA-9303
- Restarting Deep Security Agent sometimes caused a Blue Screen (BSoD) error. PCT-63627/DSA-10364
- Disabling and then enabling Deep Security Agent could cause events to be missing from **Events & Reports > Anti-Malware Events**. PCT-53209/DSA-9707

### Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. VRTS-13942/DSA-9225

Highest Common Vulnerability Scoring System (CVSS) score: 7.8

Highest severity: High

## Deep Security Agent - 20.0.2-7600 (20 LTS Update 2025-04-16)

Release date: April 16, 2025

Build number: 20.0.2-7600

## New features

**Dynamic Intelligence Mode**: Dynamic Intelligence Mode enables Deep Security Agent to automatically adjust monitoring levels to optimize security responses based on detected threats, user behavior, and system configuration.

## Enhancements

- Web Reputation Service now supports the "Trend Micro Toolbar for Enterprise" browser extension for Microsoft Edge and Google Chrome on Windows Server 2025. DSA-9538

## Resolved issues

- The Trend Micro Solution Platform service (`coreServiceShell.exe`) crashed unexpectedly. PCT-52712/DSA-9932
- Environments with a Pure Storage solution installed sometimes had performance issues. PCT-47586/DSA-9553
- A driver issue sometimes caused a Blue Screen (BSoD) error. PCT-55477/DSA-8421
- PowerPoint sometimes crashed when the system was waking up from hibernate. PCT-48516/DSA-8421

## Security updates

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. VRTS-13942/DSA-10038

Highest Common Vulnerability Scoring System (CVSS) score: 7.8

Highest severity: High

## Deep Security Agent - 20.0.2-4960 (20 LTS Update 2025-03-12)

Release date: March 12, 2025

Build number: 20.0.2-4960

### Enhancements

- The `dsa_scan` command now includes a `scanLargeFile` option for managing larger files. DSA-8785
- SAP scans are now faster due to the introduction of a caching mechanism and reduction of unnecessary operations. DSA-7219
- Deep Security Agent can now log Device Control events directly to security information and event management (SIEM) for the system. V1E-40316

### Resolved issues

- SAP Scanner sometimes incorrectly classified CSV files if they were larger than 4096 bytes. PCT-51974/DSA-9139
- If the Windows Base Filtering Engine service was not running, the Trend Micro Windows Filtering Platform (TBIMWFP) driver sometimes crashed while it was stopping. PCT-38921/PCT-53750/DSA-9154
- Certificate-related error events were being generated with outdated links to solution articles in their event description fields. These links led to a "404 page not found." PCT-54305/DSA-9113

## Deep Security Agent - 20.0.2-1390 (20 LTS Update 2025-01-15)

Release date: January 15, 2025

Build number: 20.0.2-1390

### New features

**Windows Server 2025 support**: Deep Security Agent 20.0.2-1390 or later now supports Windows Server 2025, including FIPS mode support. This requires Deep Security Manager 20.0.1017 or later.

**User-based Firewall events**: Firewall events now include username whenever possible. This feature is in preview and is only available to certain customers at this time.

### Enhancements

- Deep Security Agent now queues packets to handle them in sequence, improving performance. DSA-6916
- Updated Deep Security Agent to improve spyware prevention. PCT-18199/DSA-5889

### Resolved issues

- Deep Security Agent sometimes had connectivity issues when Advanced TLS Traffic Inspection was enabled. DSA-8577

### Security updates

This release contains updates to third-party libraries. DSA-7695/DSA-8042

## Deep Security Agent - 20.0.1-25770 (20 LTS Update 2024-12-10)

Release date: December 10, 2024

Build number: 20.0.1-25770

### New features

**Version Control Policy**: Deep Security Agent now supports Version Control Policy, which allows Trend Vision One version control policies to manage agent and component updates for any endpoint with the Trend Micro Endpoint Basecamp (XBC) agent installed. For more information, see Version Control Policies. This is currently in pre-release, and is only supported for Trend Vision One - Server & Workload Protection.

## Enhancements

- Updated Deep Security Agent to reduce the duration of on-demand scans when the CPU Usage is set to Medium (**Computer** or **Policy > Settings > General > CPU Usage Control**). DSA-8171
- Deep Security SAP Scanner can now report results to SAP applications when it identifies password-protected compressed files attached to an email in Microsoft Outlook Item (MSG) format. SF07873657/PCT-23367/DSA-7562
- Deep Security Agent now detects if its relay proxy is Trend Vision One Service Gateway Forward Proxy Service, and uses the Service Gateway domain allow list to decide whether the connection should use the relay proxy or not. SF07267852/PCT-29311/DSA-6274
- Trend Cloud One - Endpoint & Workload Security can now install Trend Vision One Endpoint Security agent via Deep Security Agent. DSA-7532
- Deep Security Agent can now add existing detections (by malware name, or rule ID for Anti-Malware or Behavior Monitoring) to the Rule Exceptions list from **Computer** or **Policy > Anti-Malware > Advanced**. DSA-6318
- Deep Security Agent now supports additional options to fine-tune detection sensitivity for Anti-Malware, Behavior Monitoring, Predictive Machine Learning, Process Memory Scan, and the Windows Antimalware Scan Interface for real-time scan. This enhancement is only available in Trend Cloud One - Endpoint & Workload Security. DSA-6062
- Deep Security Agent now supports wildcard `*` use in Anti-Malware process path exclusions, which is being rolled out gradually for Windows platforms. PCT-36703/DSA-7768

## Resolved issues

- Events including packet data were being logged with an incorrect packet size. PCT-45556/DSA-8074
- Deep Security Agent had higher than usual CPU usage if Integrity Monitoring was disabled following an Integrity Monitoring scan. SF07991055/PCT-31459/DSA-6195
- Anti-Malware manual scans of files or folders with special characters sometimes failed. PCT-43895/DSA-8126

- The Trend Micro Windows Filtering Platform (TBIMWFP) driver caused a memory leak on some systems, which led to higher than normal memory usage. DSA-7968
- Deep Security SAP Scanner would incorrectly report scan failures when two or more files with the same content were included in a compressed file. PCT-38781/DSA-7557
- The Anti-Malware Solution Platform (AMSP) service was crashing on some systems. PCT-41566/DSA-7952

### Security updates

This release contains updates to third-party libraries. DSA-7124

Security updates are included in this release. For more information about Trend Micro protection against vulnerabilities, see Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details are only available for select security updates once patches are available for all impacted releases. VRTS-13016/DSA-7645

Highest Common Vulnerability Scoring System (CVSS) score: 7.8

Highest severity: High

## Deep Security Agent - 20.0.1-23340 (20 LTS Update 2024-11-13)

Release date: November 13, 2024

Build number: 20.0.1-23340

### New features

**Windows 11, version 24H2 support**: Deep Security Agent 20.0.1-23340 or later supports Windows 11, version 24H2.

### Enhancements

- Web Reputation Service can now use Server Name Indication (SNI) queries when determining the risk level of a website. DSA-7314

- Advanced Transport Layer Security (TLS) inspection can now support Windows Local Security Authority (LSA) protection. DSA-5642

### Resolved issues

- When Application Control was operating in block mode, files in some directories were being allowed to run when they should have been blocked. PCT-38516/DSA-7613
- Deep Security Agent sometimes caused a file handle leak when performing an Anti-Malware manual scan. DSA-7676

### Security updates

Security updates are included in this release. For more information about how we protect against vulnerabilities, visit Vulnerability Response. Please note, in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-13428//VRTS-13017/DSA-7666/DSA-7646

Highest Common Vulnerability Scoring System (CVSS) score: 6.7

Highest severity: Medium

## Deep Security Agent - 20.0.1-21510 (20 LTS Update 2024-10-16)

Release date: October 16, 2024

Build number: 20.0.1-21510

### Enhancements

- Add a failsafe to help prevent the Firewall driver causing systems to be stuck in a Blue Screen (BSoD) loop. DSA-7448
- Add new Windows events to logs when the Firewall driver is initialized. Events include Windows Base Filtering Engine State changes and the results registered by the tbimwfp driver. DSA-7547

### Resolved issues

- High CPU usage would occur when both Application Control and FIPS were enabled. DSA-6842
- Deep Security Agent would crash the system if the Windows Base Filtering Engine Service was not running. PCT-38921/DSA-7334
- When the SAP Scanner library re-established connections to Deep Security Agent, the scan requests sent from the SAP Scanner library would sometimes be rejected. SF08196066/PCT-34824/DSA-7608
- Deep Security SAP Scanner would sometimes crash when scanning for files in certain formats, like CSV. PCT-41353/DSA-7609

### Security updates

Security updates are included in this release. For more information about how we protect against vulnerabilities, visit Vulnerability Response. Please note, in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-12953/DSA-7559

Highest Common Vulnerability Scoring System (CVSS) score: 8.0

Highest severity: High

## Deep Security Agent - 20.0.1-19250 (20 LTS Update 2024-09-18)

Release date: September 18, 2024

Build number: 20.0.1-19250

### Enhancements

- Updated Deep Security Agent to improve compatibility with older versions of the SAP Scanner. SF08196066/PCT-34824/DSA-6819
- Deep Security Agent now supports the Alibaba Cloud connector type. DSA-6018

- Web Reputation Service can now provide protection when using HTTPS in Mozilla Firefox on Windows 10 (64-bit), Windows 11, Windows Server 2016, Windows Server 2019, and Windows Server 2022. DSA-6770

### Resolved issues

- Deep Security Agent caused high CPU usage on systems with both Application Control and FIPS enabled. DSA-6842

### Security updates

This release contains updates to third-party libraries. DSA-6156/DSA-6942

## Deep Security Agent - 20.0.1-17380 (20 LTS Update 2024-08-21)

Release date: August 21, 2024

Build number: 20.0.1-17380

### Enhancements

- Web Reputation Service "Smart Protection Server Disconnected" events now include FQDN or IP address information in the description field. DSA-5408
- SAP Scanner now classifies Society for Worldwide Interbank Financial Telecommunication (SWIFT) messages as text files. SF07895338/PCT-24359/DSA-5790
- SAP Scanner now associates JavaScript with compatible file extensions. For details, see Supported MIME types. SF08102626/PCT-31518/DSA-6192
- uAgentWscHandler.exe is a new process that supports Windows Anti-Malware Protected Process Light technology and integrates with Windows Security Center on Windows 10 or Windows 11. DSA-5138
- Advanced Threat Scan Engine has been updated to version 24.550. DSA-5968

## Resolved issues

- SAP Scanner would incorrectly classify valid CSV files if the data was formatted on a single line. SF07967718/PCT-26844/DSA-6102
- SAP Scanner sometimes incorrectly identified image files as ASP scripts. SF07764878/PCT-20406/DSA-6122
- Deep Security Agent could not load the policy if some policy configuration fields contained curly brackets. DSA-6189
- Deep Security Agent would fail to activate if the hostname contained non-ASCII characters. PCT-32214/DSA-6268
- Deep Security Agent would sometimes cause an Operating System crash if Advanced TLS inspection was enabled. PCT-34149/DSA-6346
- When Anti-Malware was enabled, some Citrix Virtual Desktop Infrastructure (VDI) environments encountered a blue screen (BSoD) error. PCT-26799/DSA-6036
- When Intrusion Prevention was enabled for Deep Security Agent, some third-party applications had connectivity issues if they were reusing a source port. SF07685331/PCT-20541/DSA-5596

## Security updates

Security updates are included in this release. For more information about how we protect against vulnerabilities, visit Vulnerability Response. Please note, in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-12301/DSA-5967/DSA-6150

Highest Common Vulnerability Scoring System (CVSS) score: 7.8

Highest severity: High

## Known issues

- Deep Security Agent Application Control causes high CPU usage. PCT-36414

## Deep Security Agent - 20.0.1-14610 (20 LTS Update 2024-07-17)

Release date: July 17, 2024

Build number: 20.0.1-14610

### Enhancements

- SAP Scanner now associates the following MIME types with compatible file extensions. For details, see Integrate with SAP NetWeaver.
  - TrueType Font (TTF). SF08102626/PCT-31518/DSA-6049
  - Java Archive (JAR). SF08102626/PCT-31518/DSA-6044
  - Apple QuickTime File Format (QTFF). SF07967718/SF07840151/PCT-22825/PCT-26844/DSA-5887/DSA-5567
  - Microsoft Advanced Systems Format (ASF). SF07967718/PCT-26844/DSA-5886

### Resolved issues

- Deep Security Agent would still try to test connections for Service Gateways. DSA-5814
- A Deep Security Agent restart sometimes caused Application Control to report drift events. SF07813110/PCT-25731/DSA-5798
- Deep Security Agent was only able to use the primary IP address for Service Gateway. DSA-4513
- Integrity Monitoring real-time scans sometimes failed to generate events. SF07269768/PCT-21721/DSA-5877
- The Anti-Malware configuration file size was impacting SAP Scanner performance on some systems. SF08057009/PCT-30380/DSA-5987

## Deep Security Agent - 20.0.1-12510 (20 LTS Update 2024-06-19)

Release date: June 19, 2024

Build number: 20.0.1-12510

### Enhancements

- Advanced TLS Traffic Inspection now supports separate configurations for "Inspect Inbound TLS/SSL Traffic" and "Inspect Outbound TLS/SSL Traffic". For detailed configuration steps, see https://help.deepsecurity.trendmicro.com/20_0/on-premise/intrusion-prevention-ssl-traffic.html#EnableTLS.

### Resolved issues

- Web Reputation Service might cause high CPU usage in VDI environments. PCT-24431/PCT-28543/PCT-29364/PCT-29712/PCT-30043/PCT-30401/PCT-30669/DSA-5766
- Edge Relay couldn't use the operating system proxy configuration without IoT features enabled. PCT-16603/DSA-5422

### Known issues

- There is a performance impact when **Inspect Inbound TLS/SSL Traffic** and **Inspect Outbound TLS/SSL Traffic** are enabled at the same time in Advanced TLS Inspection settings. For details, see Performance impact of bi-directional TLS inspection in Deep Security. DSA-5959

## Deep Security Agent - 20.0.1-9400 (20 LTS Update 2024-05-16)

Release date: May 16, 2024

Build number: 20.0.1-9400

### Enhancements

- SAP Scanner now supports the `SCANLOGPATH` parameter. For details, see Integrate with SAP NetWeaver. PCT-21958/DSA-4924
- Updated Deep Security Agent to improve the priority for configurations using a proxy. DSA-4817/PCT-21750

- Deep Security Agent can now retrieve Service Gateway settings from the Trend Micro Endpoint Basecamp (XBC) agent. DSA-4841/V1E-13468
- Web Reputation Service now supports HTTPS protection for Google Chrome browser's Incognito mode and Microsoft Edge browser's InPrivate mode on Windows 10 (64-bit), Windows 11, Windows Server 2016, Windows Server 2019, and Windows Server 2022. DSA-4296

### Resolved issues

- Deep Security Agent security updates sometimes failed after reconfiguring proxy settings. PCT-18382/DSA-5390
- Using Deep Security Agent with Web Reputation Service enabled prevented some Application Performance Monitoring (APM) applications from functioning correctly. SF04072723/SEG-97952/PCT-15716/DSA-4750
- Using multiple Smart Protection Servers sometimes generated "Smart Protection Server Disconnected for Smart Scan" warnings, even if Smart Scan was still connected. PCT-13313/DSA-4488
- Deep Security Agent security updates sometimes failed after an agent update was applied. PCT-23614/DSA-5371

### Security updates

This release contains updates to third-party libraries. DSA-4187

## Deep Security Agent - 20.0.1-7380 (20 LTS Update 2024-04-24)

Release date: April 24, 2024

Build number: 20.0.1-7380

### Enhancements

- Deep Security Agent now supports Trend Vision One Service Gateway exclusions. This is only supported for Trend Cloud One - Endpoint & Workload Security users at this time. V1E-17754

- Deep Security Agent can have its proxy configuration set by the Trend Vision One Proxy Manager. V1E-14557
- Deep Security Agent now supports custom actions "ActiveAction" or "Pass" for the Process Memory Scan. This is only supported for Trend Cloud One - Endpoint & Workload Security users on Windows platforms at this time. DSA-3621

### Resolved issues

- Deep Security Agents running in cloud environments sometimes could not be activated for Trend Cloud One - Endpoint & Workload Security. DSA-4861
- When SAP Scanner was enabled, system events for "SAP: Anti-Malware module is not ready" or "SAP: Virus Scan service is not working correctly" sometimes displayed during Deep Security Agent upgrade. These system event messages were triggered by the restart of Deep Security Agent modules. There was no functional impact. DSA-4603

## Deep Security Agent - 20.0.1-4540 (20 LTS Update 2024-03-20)

Release date: March 20, 2024

Build number: 20.0.1-4540

### Enhancements

- The SAP Scanner status for Deep Security Agent is now displayed in the console. DSA-3329
- The Deep Security Agent version is now displayed in the SAP Scanner library. SF07483850/PCT-10077/DSA-3304
- Stopping a Deep Security Agent managed by Trend Cloud One - Endpoint & Workload Security now takes less time. DSA-4208
- Anti-Malware events (Events & Reports > Anti-Malware Events) now display the date and time that files or folders were created and modified. SF07199253/PCT-1378/DSA-3578

### Resolved issues

- Deep Security Agent incorrectly classified the MIME type of `.dwg` files generated by AutoCAD, from AutoCAD 2004 to AutoCAD 2024. SF07027236/SEG-186079/PCT-5797/DSA-2901

## Deep Security Agent - 20.0.1-3180 (20 LTS Update 2024-02-29)

Release date: February 29, 2024

Build number: 20.0.1-3180

### New features

- Anti-Malware now supports Advanced Process Memory Scan by default in Trend Cloud One. Process Memory Scan is now available for Manual Scan and Scheduled Scan configurations (this is in addition to the Real Time Scan configuration). The **Action to Take** option in Process Memory Scan is available in Real Time Scan, Manual Scan, and Scheduled Scan configurations. DSA-4242

### Enhancements

- Deep Security Scanner (SAP) now reports files containing Microsoft Office Macros as Active Content, while previously they were identified as Malware. PCT-5979/DSA-3911

### Resolved issues

- Migration of agents from on-premise Deep Security Manager to Trend Cloud One - Endpoint & Workload Security using Trend Vision One Service Gateway failed. This issue could also occur when migrating using other proxy services. PCT-16649/DSA-4144
- Remote Desktop Services on Windows Server 2008 R2 was blocked by the TLS inspection process (tm_netagent). PCT-12049/PCT-12172/PCT-13878/DSA-3944
- Behavior Monitoring exclusions sometimes failed to apply because they were case sensitive. PCT-16168/PCT-16005/PCT-16476/CTSKA-27/DSA-4116

- The expected MIME type for `.msg` files by the Deep Security Agent SAP Scanner was incorrect. PCT-5797/DSA-4050
- Enabling Intrusion Prevention or Web Reputation Service in Deep Security Agent sometimes resulted in a TLS inspection process (tm_netagent) error log rotation issue. DSA-3965
- When a password is required for a local override, the password was checked after the Deep Security Agent self-protection was locally disabled. PCT-10861/DSA-3293
- Uninstalling Deep Security Agent did not remove all folders associated with Deep Security Agent. DSA-2460

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-11708/DSA-3702

Highest Common Vulnerability Scoring System (CVSS) score: 7.8

Highest severity: High

### Known issues

- The Application Control Trust Entities "block by target" trust rule sometimes does not work properly when running a copy of an executable file. PCT-11105/DSA-3324

## Deep Security Agent - 20.0.1-700 (20 LTS Update 2024-04-17)

Release date: April 17, 2024

Build number: 20.0.1-700

### Enhancements

- Updated Deep Security Agent to improve the priority for configurations using a proxy. This is only supported for Trend Cloud One - Endpoint & Workload Security customers on Windows x64 platforms at this time. DSA-4817/PCT-21750

### Known issues

- Updating to Deep Security Agent 20.0.1.700 fails on some 20.0.0 versions when using Deep Security Relay. For more details, see Failed remote upgrade of self-deployed Workload Security relay from 20.0.0-3445 or later to version revision 20.0.1. DSA-3317
- Enabling Intrusion Prevention or Web Reputation Service in Deep Security Agent might result in a TLS inspection process (tm_netagent) error log rotation issue. For more details, see TLS inspection process error log rotation problem in Deep Security. DSA-3773

## Deep Security Agent - 20.0.1-690 (20 LTS Update 2024-01-17)

Release date: January 17, 2024

Build number: 20.0.1-690

### New features

**Command line scan**: Deep Security Agent now supports on-demand scans triggered using `dsa_scan` from a command line interface.

This is currently only available to Trend Cloud One - Endpoint & Workload Security customers. For more information, see Command-line basics. V1E-6993

### Enhancements

- From 2024 onward, Deep Security Agent versioning is being revised from 20.0.0 to 20.0.1. This requires Deep Security Manager 20.0.883 or later. DSA-3584

  For details, see Platform support updates for Deep Security Agent (DSA) version revision in January 2024 Update Release.

### Resolved issues

- Deep Security Agent was sometimes unable to connect to the local Smart Protection Server. DSA-3564
- Deep Security Agent could have memory leaks on some systems while trying to route to Domain Controllers. DSA-3266
- Deep Security Agent sometimes froze at launch if Windows APIs were verifying digital signatures for portable executable (PE) files. DSA-3626
- When FIPS mode was disabled, Deep Security Agent used the OpenSSL configuration specified by the system environment variables rather than the config specified by the agent. PCT-4914/DSA-2651/DSA-2737/DSA-2738

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. V1E-10952

Highest Common Vulnerability Scoring System (CVSS) score: 9.8

Highest severity: Critical

### Known issues

- Updating to Deep Security Agent 20.0.1-690 from some 20.0.0 versions sometimes fails when using Deep Security Relay on Trend Cloud One - Endpoint & Workload Security. For details, see Failed remote upgrade of self-deployed Workload Security relay from 20.0.0-3445 or later to version revision 20.0.1 DSA-3317
- Enabling Intrusion Prevention or Web Reputation Service in Deep Security Agent might result in a TLS inspection process (`tm_netagent`) error log rotation issue. For details, see TLS inspection process error log rotation problem in Deep Security. DSA-3773

## Deep Security Agent - 20.0.0-8438 (20 LTS Update 2023-12-12)

Release date: December 12, 2023

Build number: 20.0.0-8438

### New features

**Windows 11, version 23H2 support**: Deep Security Agent 20.0.0-8438 or later support Windows 11, version 23H2. DSA-2255

### Enhancements

- Remove some file types from the scanning list to avoid high CPU and disk consumption. SF07099651/SEG-188688/DSA-2010
- Agent self-protection now protects the Advanced TLS Traffic Inspection process (tm_netagent) preventing local users with administrator privileges from stopping it. DSA-1042/DSA-1043

### Resolved issues

- When using a local Smart Protection Server and a configured proxy, Web Reputation Service would sometimes improperly send traffic through the proxy. Web Reputation Service now sends queries to the local Smart Protection Server directly. DSA-2981
- Anti-Malware scan mode would sometimes not match the policy configuration. SF07117203/SEG-191043/PCT-7856/DSA-2561
- A memory leak would occur when loading large Suspicious Object lists. SF06904914/SEG-182231/DSA-1370

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-11015/DSA-2156

Highest Common Vulnerability Scoring System (CVSS) score: 7.8

Highest severity: High

### Known issues

- Enabling Intrusion Prevention or Web Reputation Service in Deep Security Agent might result in a TLS inspection process (`tm_netagent`) error log rotation issue. For details, see TLS inspection process error log rotation problem in Deep Security. DSA-3773
- Deep Security Agent is sometimes unable to connect to the local Smart Protection Server. This issue is fixed in 20.0.1-690. For details, see Deep Security Agent (DSA) connection issues with Smart Protection Server (SPS) when using proxy DSA-3564

## Deep Security Agent - 20.0.0-8268 (20 LTS Update 2023-11-21)

Release date: November 21, 2023

Build number: 20.0.0-8268

### Resolved issues

- Deep Security Anti-Malware sometimes did not function as expected after the system had resumed from sleep mode (S0 low-power idle mode of the working state, also known as modern standby). SF07326571/PCT-5476/DSA-2485
- Deep Security Agent incorrectly classified MIME type of `.xml` files generated by Microsoft Word, Excel, PowerPoint, as well as `.dwg` files generated by AutoCAD and R2000. SF07027236/SEG-186079/DSA-2202

### Known issues

- Enabling Intrusion Prevention or Web Reputation Service in Deep Security Agent might result in a TLS inspection process (`tm_netagent`) error log rotation issue. For details, see TLS inspection process error log rotation problem in Deep Security. DSA-3773

## Deep Security Agent - 20.0.0-8137 (20 LTS Update 2023-10-26)

Release date: October 26, 2023

Build number: 20.0.0-8137

### New features

- **Process Memory Scan**: Anti-Malware manual and scheduled scans now support the process memory scan which scans the memory of running processes. This requires Deep Security Manager 20.0.844 or later.
 This feature will be disabled in the November release of Deep Security Manager and in Trend Cloud One - Workload Security. For more information, see High Memory Usage for random process when using Deep Security Agent 20.0.0-8137

### Resolved issues

- When Intrusion Prevention System was enabled on a machine with Windows Network Load Balancing (NLB) installed and Unicast Mode configured, Network Load Balancing performance was sometimes affected. SF06426122/SEG-169878/DSSEG-7852
- When agent self-protection was enabled for Deep Security Agent 20.0.0-7719, access violation errors would sometimes appear in the Windows System Log. DSA-1962

### Known issues

- Enabling Intrusion Prevention or Web Reputation Service in Deep Security Agent might result in a TLS inspection process (`tm_netagent`) error log rotation issue. For details, see TLS inspection process error log rotation problem in Deep Security. DSA-3773

## Deep Security Agent - 20.0.0-7943 (20 LTS Update 2023-09-26)

Release date: September 26, 2023

Build number: 20.0.0-7943

### Enhancements

- In order to display agent pattern updates properly, Deep Security Agent 20.0.0-7943 or later requires Deep Security Manager 20.0.759+. For more information, see Incompatible Agent / Appliance Version error in Deep Security Agent 20.0.0-7943. SEG-190866/SEG-191017/DSA-1531
- New commands exist to get proxy information from the command line: `dsa_query -c GetProxyInfo` `dsa_query -c GetProxyInfo details=true`. DSA-864
- Web Reputation Service now supports the "Trend Micro Toolbar for Enterprise" browser extension for Microsoft Edge on Windows 10 (64-bit), Windows 11, Windows Server 2016, Windows Server 2019 and Windows Server 2022. DSA-1565

### Resolved issues

- When Log Inspection was enabled, Deep Security Agent sometimes crashed on Windows Server 2019 systems. DS-77766

## Deep Security Agent - 20.0.0-7719 (20 LTS Update 2023-08-29)

Release date: August 29, 2023

Build number: 20.0.0-7719

### New features

**New language support**: Deep Security Agent now supports Polish and Czech.

### Enhancements

- Deep Security Agent no longer updates the Smart Scan agent pattern when Smart Scan is disabled, saving network bandwidth. SEG-186625/DSA-1063

- Deep Security Agent now downloads fewer incremental pattern updates, saving network bandwidth. Note that agents configured as a Deep Security Relay still download all pattern updates. DSA-1000
- The blocking page Web Reputation Service redirects users to when they try to access a blocked URL can now be viewed in Czech or Polish. DSA-444
- Deep Security Agent now triggers a security update automatically when the Anti-Malware Solution Platform (AMSP) service is ready. Previously, security updates could fail if triggered before the AMSP was ready, causing "Anti-Malware Engine Offline" and "Pattern Update on Agents/Appliances Failed" errors. DSA-1020

## Resolved issues

- Stopping the Deep Security Agent service (ds_agent) took longer than usual on some systems. SEG-187365/DSA-1212
- Deep Security Agent sometimes performed security updates even if none were scheduled. SEG-187449/DSA-1064
- When Anti-Malware was enabled, Deep Security Agent impacted the performance of some third-party applications. SEG-182065/DSA-790
- Deep Security Agent caused high CPU usage on some systems. SEG-185563/DSA-756
- Device Control blocked Windows Server Storage Area Network (SAN) drives that should have been allowed. SEG-178278/V1E-3895
- Network drivers failed to bind to the network interface automatically on some Azure VMs. DSA-1040

## Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-7976/DSA-1386

Highest Common Vulnerability Scoring System (CVSS) score: 7.8

Highest severity: High

## Deep Security Agent - 20.0.0-7476 (20 LTS Update 2023-07-25)

Release date: July 25, 2023

Build number: 20.0.0-7476

### New features

**Deep Security Agent Right-Click Scan**: Deep Security Agent now allows users to trigger a manual scan from Windows File Explorer by right-clicking a file or folder and selecting **Scan**. Note that this feature is only available to Trend Vision One Endpoint users and Trend Cloud One - Endpoint & Workload users at this time.

### Enhancements

- If anti-malware is offline because AMSP service was not installed correctly, Deep Security Agent now tries to reinstall AMSP when the agent service launches. DSSEG-7903/SEG-181443
- Updated the dsa-connect service to improve CPU performance. C1WS-12970
- Updated Deep Security Agent to support the Notifier Anti-Malware Protected Process Light (AM-PPL) service for Windows 10 desktop platforms. This requires Deep Security Manager 20.0.789 - 20.0.833. DS-77160
- Improved Advanced TLS Traffic Inspection coverage for Windows Server 2012 R2, 2016, and 2019. SEG-182585/DSA-583

### Resolved issues

- Smart Protection Servers would sometimes lose connectivity with Web Reputation Service. SF06423462/SEG-166651/DSSEG-7858
- The system sometimes crashed when Intrusion Prevention was enabled. SF06983729/SEG-184423/DSSEG-7907
- Deep Security Agent upgrades triggered from the Deep Security Manager console would fail on some system configurations, returning MSI error code 1601: Windows installer is not accessible. SEG-177789/DS-78084

- Deep Security Agent sometimes reported that the network module was disabled (Event ID 1013, Trend Micro LightWeight Driver failed to bind on all network interfaces) even if the module was enabled. SEG-184701/SEG-182649/DSA-686
- Updated Deep Security Agent to support systems using Dell MAC Address Passthrough. SEG-177651/DSA-455

## Deep Security Agent - 20.0.0-7303 (20 LTS Update 2023-06-28)

Release date: June 28, 2023

Build number: 20.0.0-7303

### Enhancements

- Deep Security Agent now supports IPv6 addresses using either CIDR or double colon notation, such as fe80:0:0:0:0:0:0:1/24 or fe80::01. SF04849178/SEG-122076/DS-67280
- Web Reputation Service now automatically monitor the ports used by the OS proxy configuration. DS-77233
- When a specific process is sending backup packets through an unencrypted connection, Intrusion Prevention optimizes the scan flow to reduce CPU impact. SF06456142/SEG-166877/DS-76500

### Resolved issues

- The Windows Malicious Software Removal Tool (MSRT) installation could fail while Application Control is in maintenance mode. SF06446534/SEG-172729/DS-77094
- Intrusion Prevention (IPS) might not read the correct payload value, which can result in rule malfunctions. DS-74647
- The Deep Security Agent would report "dsa-connect has not provided status" on every heartbeat, even when Endpoint Sensor was not in use. C1WS-14696
- The Deep Security Agent upgrade would fail when specific features were enabled. SF06794868/SEG-177789/DS-78008

- Deep Security Agent sometimes crashed when it was unable to connect to Deep Security Manager using a proxy. DS-77786
- When Application Control was enabled, MSI file installations failed on some versions of Windows. SF06509811/SEG-170485/DS-76906
- Deep Security Relay 20.0.0-7119 failed to provide security and software updates when using the improved Relay. SF06935222/SEG-183184/DS-78201
- Some MQTT messages would be sent repeatedly and cause dsa-connect to get stuck in a shutdown loop. DS-76709

## Deep Security Agent - 20.0.0-7119 (20 LTS Update 2023-05-29)

Release date: May 29, 2023

Build number: 20.0.0-7119

### Enhancements

- When Application Control is enabled, MSI file installations fail on some systems. SF06509811/SEG-170485/DS-76906
- Agent self-protection now secures the Advanced TLS inspection process (`ds_nuagent`), preventing local users with administrator privileges from stopping it. DS-74080
- Deep Security Agent 20.0.0-7119 or later now supports FIPS mode for the `dsa-connect` service for Workload Security customers on Windows platforms that support FIPS mode as detailed here: Supported features by platform. C1WS-7467

### Resolved issues

- Deep Security Agent only reported a single Anti-Malware event for an infected compressed file, even if it contained multiple infected files. DS-76339
- After replacing a connection, Deep Security Agent reported metrics as though it was still connected to the old connection for up to 4 minutes. DS-77453
- If Advanced TLS traffic inspection was enabled, rebooting the operating system sometimes caused Deep Security Agent to get stuck on the "stopping services" screen. SF06494167/SEG-170082/DS-76880

- The Deep Security Notifier service (`ds_notifier`) caused a memory leak during agent updates on some systems. SF06454240/SEG-167684/DSSEG-7863

### Known issues

- Upgrading to Deep Security Agent version 20.0.0-6860, 20.0.0-6690, or 20.0.0-7119 using the Deep Security Manager console sometimes results in upgrade failure. After the upgrade failure, the Deep Security Agent service stops and may show "Agent Offline" from the manager console. SEG-177789, SEG-177748, SEG-178496, SEG-178742, SEG-177423, SEG-178470, SEG-178940, SEG-178956

## Deep Security Agent - 20.0.0-6860 (20 LTS Update 2023-04-25)

Release date: April 25, 2023

Build number: 20.0.0-6860

### Enhancements

- Updated Deep Security Agent to make the connection timeout for proxy probing configurable by adding a line to `ds_agent.ini`. SF06664116/SEG-173848/DS-77182

  Example proxy probing line in `ds_agent.ini` config file: `dsa.proxymanager.ProbeTimeoutInSec=120`
- Made improvements to Deep Security Agent to prevent it incorrectly sending "MQTT Connection Offline" warnings when the connection is online. SEG-171358/C1WS-12979
- Updated Deep Security Agent to improve MQTT connection quality and reduce the occurrence of connection timeouts. DS-76840
- Deep Security Agent installer now prevents the agent from updating if it detects SHA-1 was used to sign the certificate on the agent installer. This prevents the agent from updating and becoming unresponsive, since Deep Security Agent 20.0.0-6313 and higher requires RSA-2048 and SHA-256. For more information on

certificate upgrade, see Upgrade the Deep Security cryptographic algorithm. DS-76499

- Error messages from the Trend Micro Deep Security Notifier now provide more details when the on-demand scans fail. VO-2132

### Resolved issues

- Deep Security Agent was unable to load the third-party libraries required to use Remote Shell, File Collection, or Network Isolation on the Windows 2008 platform. DS-75176
- Deep Security Agent would sometimes freeze on system startup, which caused the Windows Service Control Manager service to generate "service hung on starting" events (Event ID 7022). DS-77212
- When Anti-Malware Predictive Machine Learning was enabled, file operations initiated by Powershell sometimes encountered sharing violations. SF05904706/SEG-150738/DSSEG-7695
- When Web Reputation Service was enabled, Deep Security Agent caused some systems to shutdown unexpectedly. SF06680505/SEG-174730/DSSEG-7866
- Deep Security Agent sometimes reported the network driver status incorrectly after the driver had restarted. C1WS-12896

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-8320/DSSEG-7865

Highest Common Vulnerability Scoring System (CVSS) score: 2.9

Highest severity: Low

## Deep Security Agent - 20.0.0-6690 (20 LTS Update 2023-03-29)

Release date: March 29, 2023

Build number: 20.0.0-6690

## New features

**Service Gateway**: Deep Security Agent 20.0.0-6690 or later with Deep Security Manager 20.0.741 or later now supports the Service Gateway feature, providing forward proxy functionality.

## Enhancements

- Deep Security Agent installation now performs a pre-check to verify if its operating system meets Azure Code Signing (ACS) requirements. For more information, see Trend Micro Server and Endpoint Protection Agent Minimum Windows Version Requirements. DS-75552
- Application Control now checks the execution of Microsoft Windows Control Panel Applet (.CPL) files. DS-74587
- Application Control now checks the execution of Microsoft Compiled HTML help (.CHM) files. DS-74828
- When an Application Control Trust Entities path rule uses a wildcard without specifying a filename, the wildcard now applies to all files in any directory matching the rule's path. Note that previously, the globstar (`**`) wildcard would apply to a path rule's directory and subdirectories, as opposed to the single star (`*`) wildcard which would only match within the path rule's directory. DS-75133
- Web Reputation Service now includes OS platform metadata. DS-75453
- Deep Security Agent 20.0.0-6690 or later now supports the Proxy Manager for Trend Micro Vision One (XDR) Threat Intelligence - User Defined Suspicious Object (UDSO). DS-75365
- Updated Deep Security Agent's logging system to provide additional information and tracing to debug customer issues more efficiently. The agent now generates five (5) log files (`dsa-connect-X.log`) that are 2MB each instead of the agent's previous three 1MB log files. C1WS-9598

  The logger supports an on-demand JSON config file (either `dsa-connect.ini` or `dsa-connect.conf`) with the following configurable options:
  - Debug: Enable the debug log messages. The default value is false.
  - Count: Number of log files to generate. The default value is 5.

  - Size: Maximum size of each log file in bytes. The default value is 2097152.

  Example config file:

  ```
  {
  "Debug": true,
  "Count": 5,
  "Size": 2097152
  }
  ```

- The Web Reputation Service's Browser Extension now allows Trend Micro Toolbar for Chrome browser to inspect URLs for content scripts in all frames. DS-75387
- Anti-Malware events generated by the SAP Scanner now include file hashes. DS-75648/SEG-165491

## Resolved issues

- Deep Security Agent events and module status changes sometimes failed to appear in the console. DS-46344/SEG-67100/SEG-101719/SEG-112311
- When Anti-Malware's "Enable network directory scan" option was enabled (**Computer** or **Policy > Anti-Malware > General > Real-Time Scan > Malware Scan Configuration > Advanced > Network Directory Scan)**), malware was detected but a corresponding event was not recorded in some cases. SF06198579/SEG-160763/DSSEG-7786
- When the Advanced TLS Traffic Inspection "Inspect TLS/SSL traffic" option was set to "No" from the console (**Computer** or **Policy > Intrusion Prevention > General > Advanced TLS Traffic Inspection**), driver-side SSL packets were sometimes still being processed. DS-76160
- Deep Security Agent's Intrusion Prevention System sometimes failed to block "TCP Congestion Flags" properly. DS-76182
- When Anti-Malware Smart Scan was enabled, an IPC connectivity issue caused some systems to crash. SEG-169132/C1WS-10821
- Updated Deep Security Agent to increase the MQTT timeout from 30 minutes to 2 hours to help resolve connection issues on some systems. C1WS-11835

- Deep Security Agent was incorrectly generating system events showing that the Advanced Threat Search Engine (ATSE) component had been removed on some systems. SEG-147779/DS-75463
- Deep Security Agent upgrade sometimes failed because of a missing signature in the agent package. SF06045259/SEG-154576/DS-73668
- Application Control now checks web browser execution of .HTML, .HTM, and .JS files. DS-75102
- When a SOCKS proxy was used, Deep Security Agent failed to provide a Web Reputation Services rating for HTTP URLs. DS-73482/DS-73364
- Deep Security Agent security updates were failing due to a file handle issue that prevented files from being removed during an update. DS-75907
- Deep Security Agent Scanner (SAP) couldn't generate reports for files with one or more trailing dots `.` in their file name. SF06181341/SEG-166326/DS-76404

### Known issues

- Deep Security Agent 20.0.0-6313 or later is currently unable to load the third-party libraries required to use Remote Shell, File Collection, or Network Isolation on the Windows 2008 platform. If you need these three features on a Windows 2008 system, refrain from upgrading your agent. DS-75176
- Updating Deep Security Agent causes Deep Security Manager to show an unknown error event (ID: 740) on some systems. A future Deep Security Manager release will address this issue. For more details, see Unrecognized Agent / Appliance Error Event in Deep Security Manager (Event ID 1010 - 1013). DS-76813

## Deep Security Agent - 20.0.0-6313 (20 LTS Update 2023-01-31)

Release date: January 31, 2023

Build number: 20.0.0-6313

## New features

**Windows 10 22H2 support**: Deep Security Agent 20.0.0-6313 or later with Deep Security Manager 20.0.716 or later now supports Windows 10 22H2.

## Enhancements

- Deep Security no longer supports certificates signed with the SHA-1 algorithm. The agent now requires SSL certificates issued using SHA-256 to communicate with the Deep Security Manager. C1WS-5676

- With Anti-Malware and Behavior Monitoring enabled, Deep Security Agent now monitors for suspicious behavior to improve protection against MITRE attack scenarios. This functionality requires Deep Security Manager 20.0.711+. DS-73644
- Updated Deep Security Agent to support the "Trend Micro Toolbar for Enterprise" Chrome browser extension, improving HTTPS protection for Web Reputation Service. DS-74870

## Resolved issues

- When Application Control was enabled, Deep Security Agent's status sometimes became stuck at "Application Control Ruleset Update In Progress". DS-74627
- An issue with the TLS protocol record layer in Deep Security Agent caused some systems to crash. SF06297487/SEG-162236/DSSEG-7774
- Deep Security Agent sometimes caused file handle leaks when communicating with Deep Security Manager or agent command-line tools. DS-75111
- For component updates, Deep Security Agent would attempt with and without use of a proxy and generate an event for each attempt. To make event reporting more straightforward, this behavior has been changed so that after a successful update the agent only shows the final successful event. SF06207160/SEG-160085/DSSEG-7765
- With Web Reputation Enabled, some characters entered in console commands were not being parsed properly. For example, an underscore (`_`) entered in a command was replaced with a dash (`-`), and an uppercase Z was replaced with a lowercase z. DS-74335

## Deep Security Agent - 20.0.0-5995 (20 LTS Update 2022-11-28)

Release date: November 28, 2022

Build number: 20.0.0-5995

### New features

**Windows 11 22H2 support**: Deep Security Agent 20.0.0-5995 or later with Deep Security Manager 20.0.711 or later now supports Windows 11 22H2.

### Enhancements

- Updated Deep Security Agent to support the "Trend Micro Toolbar for Enterprise," a Chrome browser extension that extends HTTPS protection for Web Reputation Service. This is only supported for Trend Micro Cloud One - Workload Security customers at this time. DS-74568
- Updated the Web Reputation Service to support multi-thread processing on the web browser extension, improving the query rate. DS-74098
- Updated Deep Security Agent to include the details of command line Behavior Monitoring violations in the console under **Events and Reports > Events > Anti-Malware Events**. DS-72866

### Resolved issues

- A file handle leak in the Deep Security notifier (`notifier.exe`) caused high system memory usage. DS-74325
- In Workload Security, enabling OS proxy (by setting **Allow agents to apply OS proxy or direct connect when the configured proxy is inaccessible** to Yes from **Administration > System Settings > Proxies**) would cause Deep Security Agent to crash if the proxy data the agent needed was missing on the operating system side. SEG-158968/DS-75034
- While running Application Control in maintenance mode, executable files that should have been accessible were sometimes blocked due to a sharing violation. SF04922652/SEG-131710/DS-74592

- Application Control was unable to block scripts executed using GitBash shell (`sh.exe`). DS-73827
- Deep Security Agent caused an outdated "Early Launch Anti-Malware Pattern" component to appear on the Security Updates page, causing the Security Update Status to be "Out-of-Date". This pattern was unused, which is why it always appeared as an outdated component. SEG-158345/DSSEG-7745
- Deep Security Agent sometimes allowed a higher access level than the one set by a user's group. For example, the "Users" group was able to modify files even if it had read-only access. SEG-157530/DSSEG-7737
- With Anti-Malware enabled, a Deep Security Agent driver caused some systems running Windows Server 2008 to crash. SF05926337/SEG-157388/DSSEG-7739

## Deep Security Agent - 20.0.0-5810 (20 LTS Update 2022-10-27)

Release date: October 27, 2022

Build number: 20.0.0-5810

### New features

**Installed software reporting**: Deep Security Agent now reports installed software with additional details from the Microsoft Windows Installer. This is currently only available to Trend Micro Cloud One Workload Security customers.

### Enhancements

- Updated Deep Security Agent to include additional metadata, such as `UserAgent` and `Referrer`, for Web Reputation Services. DS-72196
- Updated Deep Security Agent to include the Integrity Monitoring database in the agent diagnostic package. DS-73293
- Updated Deep Security Agent to support NULL cipher when inspecting TLS traffic with Intrusion Prevention. DS-71085

### Resolved issues

- With Anti-Malware Behavior Monitoring enabled, uninstalling or upgrading from Deep Security Agent 20.0.0-5761 caused some systems to crash. For more details see BSOD Encountered During Uninstall of Deep Security Agent 20.0.0-5761. DS-74322
- With Log Inspection enabled, Deep Security Agent sometimes generated "Abnormal Restart Detected" events. SF05951130/SEG-151372/DS-73737
- If the Deep Security Agent service stopped while running Application Control in Maintenance Mode, executable files created after the service stopped were not being auto-approved as intended. SF05961688/SEG-152045/DS-73570
- Software, if renamed or copied while Application Control had Maintenance Mode enabled, would remain authorized in the software inventory under its original filename or location. DS-74015
- Virtual Machines using vMotion sometimes deactivated unexpectedly and displayed an "Offline (Activation required)" status. SEG-153050/DS-73807
- The TLS inspection support package failed to download on Deep Security Agents using Edge Relay. DS-73789
- While an Application Control inventory build is in progress, the agent would sometimes appear offline. DS-72189

### Known issues

- After upgrading the Deep Security Agent 20.0.0-5761 to 20.0.0-5810 on Windows, a reboot is required to solve an issue that causes computers to crash. For details including steps to work around the issue, see BSOD Encountered During Uninstall of Deep Security Agent 20.0.0-5761. DS-74383

## Deep Security Agent - 20.0.0-5512 (20 LTS Update 2022-09-22)

Release date: September 22, 2022

Build number: 20.0.0-5512

### Enhancements

- Deep Security Agent now supports the automatic update of Advanced TLS Traffic Inspection as operating system libraries change (**Computer** or **Policy > Settings > TLS Inspection Package Update**). This requires Deep Security Manager 20.0.677 or later. DS-72828

### Resolved issues

- Integrity Monitoring events (**Events and Reports > Integrity Monitoring**) were created with N/A displayed in the KEY and TYPE columns. SF05533287/SEG-139293/DS-71899
- Updating Deep Security Agent and removing the expired TLS session key caused some systems to crash. SF06007238/SEG-153175/DS-73404
- With Anti-Malware enabled, some computers froze in a "Security Update In Progress" state. SF05106626/SEG-129777/DSSEG-7500
- With Deep Security Agent self-protection enabled, enabling or disabling Advanced TLS inspection service caused "Event ID 7006" in the Windows Service Control Manager. DS-73305
- Deep Security Agent reported host metadata in an unexpected format. DS-73411

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-8100/VRTS-8101/DS-73087/DS-72528

Highest Common Vulnerability Scoring System (CVSS) score: 7.0

Highest severity: High

## Deep Security Agent - 20.0.0-5394 (20 LTS Update 2022-08-29)

Release date: August 29, 2022

Build number: 20.0.0-5394

## Enhancements

- Application Control now detects software changes for executables with non executable extensions. DS-70805
- Added SYSTEM user network drives and mount points for Windows to the information collected when generating a diagnostics package. DS-71816
- Updated Deep Security Agent to add support for inspecting packets using dynamic ports in a TLS connection. DS-71078
- Updated Deep Security Agent so Application Control automatically authorizes test PowerShell scripts created by AppLocker. DS-71762
- Behavior Monitoring exclusions now support wildcard characters. DS-71976
- Updated Deep Security Agent to add more metrics for Advanced TLS Inspection. DS-72833

## Resolved issues

- When TLS inspection was done on a UDP connection with dynamic ports, the operating system would sometimes crash. SEG-151169/DS-73043
- Log Inspection Engine would go offline when using '$' character in match or regex fields together with variables. SEG-146965/SEG-146966/DS-72325
- When assigning a policy with real-time Anti-Malware turned off to a new guest VM, it would sometimes turn off real-time Anti-Malware for all other guest VMs registered to the same Deep Security Virtual Appliance. SEG-146057/DS-72856
- When Behavior Monitoring is enabled, Deep Security Agent would sometimes prevent Docker on Windows from starting. SF05709278/SEG-146323/DSSEG-7660
- Application Control would still block access to network files while in maintenance mode. SF04922652/SEG-131710/DS-72037
- When Application Control is enabled, Adobe plugins were generating unexpected security events. SF05823607/SEG-148570/DS-72679
- Deep Security Agent would sometimes retrieve incorrect PID information on Windows for connection metrics and log events. DS-72526

- Deep Security Agent would return "revision mismatch (-10039)" errors when loading certain configuration files during an agent update. DS-72499
- Deep Security Agent would report detected software changes before Application Control inventory scan was completed. DS-72071
- When Anti-Malware accessed files on a Cluster Shared Volume, the Hyper-V host would crash. SF05713918/SF05850687/SEG-146660/SEG-148664/DSSEG-7664

### Known issues

- When executing multiple custom script tasks, new tasks are currently overwritten by previous unfinished tasks. You can execute custom script tasks one by one to bypass this issue. Note that this issue will be fixed in a future release. DS-72699

## Deep Security Agent - 20.0.0-5137 (20 LTS Update 2022-07-26)

Release date: July 26, 2022

Build number: 20.0.0-5137

### New features

**Advanced TLS Traffic Inspection**: Deep Security Agent 20.0.0-5137 or later adds Advanced TLS Traffic Inspection support to platforms that run system updates or package updates. Note that this feature is currently only supported for Trend Micro - Cloud One Workload Security. Support for Deep Security Manager (On-Premise) will be added later.

### Enhancements

- Deep Security Agent 20.0.5137 or later for Windows uses an additional certificate: "Microsoft Identity Verification Root Certificate Authority 2020". For details see Updating the VeriSign, DigiCert, USERTrust RSA certificate on Deep Security and Trend Cloud One - Endpoint & Workload Security. DS-72711
- Deep Security Agent Scanner (SAP) now generates infection reports with additional details. DS-71660

- Updated Deep Security Agent to improve the "zero-config" SSL process for outbound connections. DS-70715
- Updated Deep Security Agent to improve Trust Entities functionality. Trust rule wildcard support now includes globstar `\*\*` which matches many sub directories. Single star `\*` now only matches within your current directory. Existing rules that used a single star `\*` to match many folders no longer work and need to be changed to use a globstar `\*\*`. DS-71817

## Resolved issues

- With Anti-Malware enabled, Deep Security Agent had a driver conflict causing some third-party applications to freeze. SF05570686/SEG-140749/DSSEG-7650
- Deep Security Agent's Scanner (SAP) library install sometimes failed because required certificates on hosts were outdated. DS-71917
- Deep Security Agent SAP scanner could not detect the MIME (.TTF) files. DS-55897
- Intrusion Prevention rules with certain setting combinations failed to compile. DS-71889

## Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-7102/VRTS-7070/VRTS-7041/VRTS-7039/DSSEG-7636

Highest Common Vulnerability Scoring System (CVSS) score: 4.4

Highest severity: Medium

## Known issues

- When executing multiple custom script tasks, new tasks are currently overwritten by previous unfinished tasks. You can execute custom script tasks one by one to bypass this issue. Note that this issue will be fixed in a future release. DS-72699

## Deep Security Agent - 20.0.0-4959 (20 LTS Update 2022-07-04)

Release date: July 4, 2022

Build number: 20.0.0-4959

### Resolved issues

- Deep Security Agent caused increased CPU usage for systems running the WMI provider service (WmiPrvSE.exe). 05528968/SEG-142736/DS-71626
- Deep Security Agent Scanner (SAP) reports displayed .SAR files in the wrong order. DS-71651
- Deep Security Agent had a conflict preventing TMUMH drivers from loading (on Windows 11 and Windows 2022), and in some cases causing a system crash (affecting all Windows platforms). SEG-143164/DSSEG-7596
- Using the command line (`dsa_control -b`), Deep Security Relay failed to extract the bundle file required to update in a closed network environment. SF05715642/SEG-144571/DSSEG-7600
- With Log Inspection enabled, updates to Deep Security Agent 20.0.0-4726 encountered "Get Events Failed" and "Command Not Found" alerts. SF05738607/SEG-145679/DS-72117
- When Anti-Malware is enabled alongside Integrity Monitoring, Deep Security Agent caused high CPU usage. SF05169148/SEG-129522/DS-69594
- With Anti-Malware enabled, Deep Security Agent generated "Anti-Malware Engine Offline" errors caused by service restarts following a software upgrade. SF05521775/SEG-144639/DSSEG-7615
- With Anti-Malware enabled, Deep Security Agent sometimes caused a system crash or high system memory usage, or failed to deliver event reports. SF05475742/SEG-142632/DSSEG-7626
- Updated Deep Security Agent to immediately report its status to Deep Security Manager when Application Control's maintenance mode is enabled on the agent. DS-71617
- Deep Security Agent sometimes created unclear error log entries referencing "invalid" or "badly-formed" proxy URLs. SEG-144613/DS-71866

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-7633/DS-71687

Highest Common Vulnerability Scoring System (CVSS) score: 6.2

Highest severity: Medium

## Deep Security Agent - 20.0.0-4726 (20 LTS Update 2022-05-31)

Release date: May 31, 2022

Build number: 20.0.0-4726

### Enhancements

- Updated Deep Security Relay to record its status and other metrics for potential troubleshooting. DS-65763

### Resolved issues

- Trust Entities "Allow by target" rules sometimes blocked processes they weren't intended to block. SF04922652/SEG-131710/DS-71060
- Deep Security Agent reported false positive "Created/Deleted" Integrity Monitoring events under some configurations. SF05434164/SEG-136425/DS-70656
- Updated Deep Security Relay to prevent Deep Security Agent from retrieving incomplete signature files for packages. SF05332854/SEG-134394/DS-71228
- Deep Security Agent had connectivity issues caused when a Server Name Indicator (SNI) used an invalid format. SEG-127761/DS-70806
- An abnormal restart of Deep Security Agent sometimes lead to "Anti-Malware Engine Offline" errors. SEG-140234/DS-71333

- With Intrusion Prevention enabled, a packet transmission error caused some systems to crash. SEG-136843/DSSEG-7524

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-7090/DSSEG-7541/DS-52329

Highest Common Vulnerability Scoring System (CVSS) score: 7.5

Highest severity: High

## Deep Security Agent - 20.0.0-4416 (20 LTS Update 2022-04-28)

Release date: April 28, 2022

Build number: 20.0.0-4416

### Enhancements

- Updated Deep Security Agent to improve Intrusion Prevention performance when the "Bypass Network Scanner" rule was applied. DS-69515
- Updated Deep Security Agent to support enabling the Anti-Malware module while Windows Defender is running in passive mode under some system configurations DS-69161. Currently this is only supported on systems running the following versions:
  - Defender (AM) product / engine versions:
    - AMProductVersion: 4.18.2202.4
    - AMEngineVersion: 1.1.18900.3
  - Windows server and desktop versions:
    - Windows Server 2016 and newer

    - Windows 10 x64 RS5 and newer
- Deep Security Agent 20.0.0-4416+

### Resolved issues

- Deep Security Agent generated multiple "Anti-malware Engine Offline" events during agent upgrades under some system configurations. SF04500910/SEG-129316/DSSEG-7458

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-7132/DS-70518

Highest Common Vulnerability Scoring System (CVSS) score: 7.5

Highest severity: High

## Deep Security Agent - 20.0.0-4185 (20 LTS Update 2022-04-06)

Release date: April 6, 2022

Build number: 20.0.0-4185

### New features

**Advanced TLS traffic inspection**: Advanced TLS traffic inspection adds the capability for inspecting TLS traffic encrypted with modern ciphers, including Perfect Forward Secrecy (PFS). It also enhances virtual patching for HTTPS servers to help protect against vulnerabilities such as Log4j.

### Enhancements

- Updated Deep Security Agent to properly execute Application Control settings for software changes made during a Windows upgrade. Previously, trust rules auto-authorizing software changes associated with a Windows upgrade would fail if Application Control was in lock down mode. DS-69579

- When certificates are missing for an Anti-Malware installation, Deep Security Agent now forwards the certificate details to Deep Security Manager. The specific certificates missing will appear in the manager under **Events and Reports > System Events**. DS-69074

### Resolved issues

- Running an Anti-Malware manual scan using the command line sometimes made Deep Security Agent unable to receive incoming connections. SF05385865/SEG-135256/DS-70364
- Deep Security Agent created an "Application Control Engine Offline" error during agent upgrade, and an "Application Control Engine Online Again" message after upgrade completion. Note that an upgrade should not have triggered these events. DS-69888
- Application Control sometimes blocked unrecognized software even when running in maintenance mode. SF05234969/SEG-133594/DS-69752
- Deep Security Agent sometimes consumed a high amount of system resources during policy updates. SEG-134417/DS-69810

## Deep Security Agent - 20.0.0-3964 (20 LTS Update 2022-03-01)

Release date: March 1, 2022

Build number: 20.0.0-3964

### New features

**Threat Intelligence**: Threat Intelligence (formerly known as Connected Threat Defense) provides enhanced malware protection for new and emerging threats. For more information, visit Detect emerging threats using Threat Intelligence.

### Enhancements

- Updated Deep Security Agent to exclude suspicious characters, such as `$`, found in strings from the "Original IP (XFF)" field for Intrusion Prevention events. SEG-129905/DS-68989

### Resolved issues

- Deep Security Agent accepted policy change parameters even if the self-protection password verification did not pass. SF05177188/SEG-129643/DS-69293
- Deep Security Agent sometimes went offline unexpectedly after activation. SEG-130280
- With Intrusion Prevention enabled, issues establishing an SSL connection caused "Unsupported SSL Version" events. SF04955719/SEG-127437/DS-68689
- Deep Security Agent was generating unexpected "Log File Delete Error" system events. DS-69641
- Deep Security Agent sometimes created unnecessary User (Created/Deleted) or Group (Added/Removed/Updated) events. DS-62413

## Deep Security Agent - 20.0.0-3771 (20 LTS Update 2022-01-24)

Release date: January 26, 2022

Build number: 20.0.0-3771

### New features

**Zero config IPS inspection**: Deep Security Agent adds the capability for Intrusion Prevention to inspect TLS encrypted traffic without manually importing certificates. This adds support for more cipher suites as well. This feature is being rolled out gradually for Windows platforms, beginning with Trend Micro Cloud One - Workload Security customers.

**Windows 21H2 support**: Deep Security Agent 20.0.0-3771 or later now supports Windows 21H2.

## Enhancements

- Updated Deep Security Agent to allow Intrusion Prevention to connect to Deep Security Manager if the manager is using TLS 1.2 strong ciphers. DS-69042

## Resolved issues

- Pairing Deep Security Agent with a proxy failed on Windows 11 when the "http://" prefix was unexpectedly added to the proxy address. The prefix was added if the address was accessed from the LAN settings window (**Control Panel > Network and Internet > Internet Options > Connections > LAN settings**), and then the window was closed by selecting OK. DS-68568
- Deep Security Agent security update would fail and generate "AMSP" events if Anti-Malware was offline during the update. SF04696674/SEG-120215/DSSEG-7287
- Application Control, Anti-Malware, and Real-time Integrity Monitoring failed to function properly for Deep Security Agents with certain combinations of Integrity Monitoring rules configured. DS-68494
- Updated Deep Security Agent to enable "Write Defer Scan" by default for real-time Anti-Malware scanning, resulting in increased response time, faster processing, and reduced CPU usage. Previously, all files were scanned during read/write by default. Now, Anti-Malware file scanning during write is deferred (the file is added to a queue and scanned in the background). DS-66344
- With Smart Scan enabled, Deep Security Agent was downloading the full size pattern update file, instead of the incremental one it was expected to, during security updates SEG-124937/DSSEG-7317

## Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-6187/DS-65070/DS-68180

Highest Common Vulnerability Scoring System (CVSS) score: 9.1

Highest severity: High

# Deep Security Agent - 20.0.0-3530 (20 LTS Update 2021-12-15)

Release date: December 15, 2021

Build number: 20.0.0-3530

## New features

- **OS proxy support**: Deep Security Agent 20.0.0-3530 or later for Windows can now apply proxy settings from the computer's OS to automatically connect to Trend Micro Cloud One - Workload Security, Deep Security Relay, and other Trend Micro backend services if the default agent-configured proxy loses its connection. **This feature is only available to certain Workload Security customers at this time.**

## Important Notes

- Pairing Deep Security Agent with a proxy currently fails on Windows 11 when the "http://" prefix is unexpectedly added to the proxy address after accessing it (under **Control Panel > Network and Internet > Internet Options > Connections > LAN settings**) and then selecting **OK** to close the window. This issue will be fixed in a future release. DS-68568

## Resolved issues

- With Smart Scan enabled, Deep Security Agent downloaded the full size pattern update file instead of the incremental one it was expected to during security updates. DSSEG-7317

# Deep Security Agent - 20.0.0-3445 (20 LTS Update 2021-11-24)

Release date: November 24, 2021

Build number: 20.0.0-3445

## New features

- **Anti-Malware offline scheduled scan**: Deep Security Agent 20.0.0-3445 or later adds the offline scheduled scan feature, enabling Anti-Malware scheduled scans to run while an agent is not connected to Cloud One Workload Security. **This feature is only available to certain Cloud One Workload Security customers at this time.**
- **Windows 11 support**: Deep Security Agent 20.0.0-3445 or later now supports Windows 11.
- **Windows Server 2022 support**: Deep Security Agent 20.0.0-3445 or later now supports Windows Server 2022.

## Enhancements

- Updated Deep Security Agent allow the Deep Security Notifier to be locked on (when installed through the command prompt using `msiexec /I "Notifier's installer name" LockAppSettingsDefault=1`), preventing users from hiding notifications. DS-64527
- Deep Security Agent sometimes crashed when it could not connect to Deep Security Manager. DS-67654
- Deep Security Agent no longer uses CBC cipher suites by default in order to improve security. DS-67204
- Updated Deep Security Agent to support using the "process name" property in "Ignore from source" rules for Application Control Trust Entities on Cloud One Workload Security. DS-67322
- Updated Deep Security Agent's database size management to optimize disk space usage. DS-67347

## Resolved issues

- With Anti-Malware enabled, Deep Security Agent caused connectivity issues for third-party software on some systems. SF04087024/SEG-125579/DSSEG-7321
- Deep Security Agent sometimes showed plugin installation failures during an upgrade even when the upgrade was successful. DS-67336

- When an expired certificate was removed from the host, the Anti-Malware plug-in update would fail, creating "Anti-Malware Component Update" events. SEG-117871/DS-66139
- If an Anti-Malware scan began before the module had completed its installation on Deep Security Agent, it could cause a system crash and "Anti-Malware Engine Offline" errors after a reboot. SEG-108355/DS-63721
- Deep Security Agent couldn't properly handle SAP NetWeaver MIME type scan requests containing leading and trailing spaces. DS-67448
- When Integrity Monitoring rules using "UserSet" or "GroupSet" were enabled for a Deep Security Agent on Windows Active Directory Domain Controllers, excessive CPU and memory consumption would sometimes occur. Deep Security Agent 20.0.0-3445 blocks these types of Integrity Monitoring rules on Windows Active Directory domain controllers and generates an "Inapplicable Integrity Monitoring Rule" event. DS-65965

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-6489/DSSEG-7210/DS-65113/VRTS-6207/DSSEG-7026

Highest Common Vulnerability Scoring System (CVSS) score: 7.8

Highest severity: High

## Deep Security Agent - 20.0.0-3288 (20 LTS Update 2021-10-28)

Release date: October 28, 2021

Build number: 20.0.0-3288

## New features

- **Evolution of the agent installer**: The Deep Security Agent installer now installs most agent content. This results in the following changes:
  - Agent size requirements have increased, including a slightly larger installer package on most platforms.
  - All agent content is now installed on the computer being protected. Content remains unloaded on a computer until a plug-in is activated by a policy or by the manager console.
  - The agent is now much less dependent on relays because all plug-in installations use the content already installed with the agent. This mitigates plug-in install issues due to relay communications because plug-ins can be installed without a connection to a relay.

## Resolved issues

- On Deep Security Agent 20.0.0-3165, "Anti-Malware Component Update Failed"events were sometimes generated when computers performed security updates. This defect is now fixed in Deep Security Agent 20.0.0-3288. SF04937346/SEG-122765/DSSEG-7268
- With Intrusion Protection enabled, Deep Security Agent sometimes caused high CPU usage and sometimes caused the system to crash. DS-65902
- With Intrusion Protection enabled, Deep Security Agent caused the system to crash under some configurations. SF04931669/SEG-123338/DS-67441
- With SAP integrated and running, Deep Security Agent would block MP4 files. 04660120/SEG-117094/DSSEG-7254
- Deep Security Agent sometimes was unable to connect to the manager via proxies. DS-65929
- CPU usage would spike when Deep Security Agent queried the runtime status of the Anti-Malware component. DSSEG-7222
- Deep Security Agent did not always check that metadata was ready before initializing connection with the manager. DS-51103
- Deep Security Agent sometimes showed package signature errors during an upgrade because of a mismatched Certification Revocation List (CRL). DS-65056

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. DS-46018/DSSEG-7210/DSSEG-7217

Highest Common Vulnerability Scoring System (CVSS) score: 7.8

Highest severity: High

## Deep Security Agent - 20.0.0-3165 (20 LTS Update 2021-10-08)

Release date: October 08, 2021

Build number: 20.0.0-3165

> **Note:** Deep Security Agent 20.0.0.3165 has been released to Trend Micro Cloud One - Workload Security customers. However, it is not available on the Deep Security Agent software download page or released to customers using Deep Security Manager.

### New features

- **Evolution of the agent installer**: The Deep Security Agent installer now installs most agent content. This results in the following changes:
  - Agent size requirements have increased, including a slightly larger installer package on most platforms.
  - All agent content is now installed on the computer being protected. Content remains unloaded on a computer until a plug-in is activated by a policy or by the manager console.
  - The agent is now much less dependent on relays because all plug-in installations use the content already installed with the agent. This mitigates plug-in install issues due to relay communications because plug-ins can be installed without a connection to a relay.

### Resolved issues

- Deep Security Agent sometimes was unable to connect to Manager via proxies. DS-65929
- CPU usage would spike when Deep Security Agent queried the runtime status of the Anti-Malware component DSSEG-7222
- Deep Security Agent did always check that metadata was ready before initializing connection with the manager. DS-51103

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. DSSEG-7210/DSSEG-7217

Highest Common Vulnerability Scoring System (CVSS) score: 7.8

Highest severity: High

## Deep Security Agent - 20.0.0-2921 (20 LTS Update 2021-08-30)

Release date: August 30, 2021

Build number: 20.0.0-2921

### New features

**Census feedback**: Deep Security Agent 20.0.0-2921 or later can now send census file feedback to the Smart Protection Network (SPN) if Trend Micro Smart Feedback is enabled (**System Settings > Smart Feedback**).

### Enhancements

- Updated Deep Security Agent to detect the "HiveNightmare" exploit. DS-65217

### Resolved issues

- With Application Control enabled, Deep Security Agent sometimes crashed when a .MSI file was launched. SF04647983/SEG-114894/DSSEG-7032
- Deep Security Agent console commands sometimes failed to return proxy information for Deep Security Relay or Deep Security Manager. DS-65419
- Deep Security Agent sometimes failed to properly display items under **Events and Reports**. DSSEG-7057

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. DSSEG-7046/DS-65668

Highest Common Vulnerability Scoring System (CVSS) score: 7.8

Highest severity: High

## Deep Security Agent - 20.0.0-2740 (20 LTS Update 2021-07-29)

Release date: July 29, 2021

Build number: 20.0.0-2740

### Enhancements

- Updated Deep Security Agent to improve TLS traffic inspection. This feature is being rolled out gradually, beginning with Trend Micro Cloud One - Workload Security customers. DS-15576
- Updated Deep Security Agent to improve connectivity with Deep Security Manager during agent deployment and activation. DS-62547

### Resolved issues

- With Application Control enabled, files with '.tmp" extensions were creating a large number of "Application Control Software Changes Detected" events in the Deep Security Manager console. 04671615/SEG-115017/DS-65043
- Deep Security Agent failed to execute some agent-initiated (dsa_control) console commands. 04564385/SEG-112050/DSSEG-6990
- Deep Security Agent sometimes crashed while trying to establish a connection with Deep Security Manager. 04634804/SEG-113539/DS-64862
- Deep Security Agent sometimes lost connectivity while trying to establish an SSL connection. SF04323898/SEG-107451/DS-64268
- Deep Security Agent was sometimes unable to connect to web applications on systems with older OS versions. SF04451029/SEG-109652/DS-64528
- With Web Reputation enabled, Deep Security Agent caused connectivity issues for some third-party software. SF04072723/SEG-97952/DSSEG-6963

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. SF04613197/SEG-113566/DS-64050

Highest Common Vulnerability Scoring System (CVSS) score: 9.8

Highest severity: High

## Deep Security Agent - 20.0.0-2593 (20 LTS Update 2021-07-01)

Release date: July 01, 2021

Build number: 20.0.0-2593

### Resolved issues

- Deep Security Agent sometimes triggered multiple "Log Inspection Engine Initialized" alerts due to an agent-manager communication issue. SF03968169/SEG-95731/DS-60840
- Anti-Malware sometimes went offline after enabling Application Control on Deep Security Agent. SF04532752/SEG-110572/DS-63406
- Application Control was detecting multiple "Application Control Software Changes Detected" events due to '.tmp" files being generated by PowerShell. C1WS-1608
- Citrix Virtual App or Desktop users sometimes encountered a grey screen (with error code 1003/1005) when Anti-Malware was enabled for Deep Security Agent. DS-64318
- Anti-Malware sometimes caused high system CPU usage when the Windows WMI service accessed files repeatedly. SEG-109271/DSSEG-6983

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-5850/DS-54705

Highest Common Vulnerability Scoring System (CVSS) score: 4.4

Highest severity: Medium

## Deep Security Agent - 20.0.0-2419 (20 LTS Update 2021-06-02)

Release date: June 02, 2021

Build number: 20.0.0-2419

### Resolved issues

- Deep Security Agent 20.0.0-2395 for Windows always displayed an "Out-of-Date" Security Update Status. This agent was removed from the Trend Micro Download

Center. For more information see Removal of Deep Security Agent 20.0.0-2395 for Windows. SF04537047/SEG-110737/DS-63424

- Integrity Monitoring alerts sometimes triggered but then did not appear in the **Events and Reports** tab. 04266346/SEG-103731/DS-62992
- Items queued for Anti-Malware scan sometimes caused higher than normal Deep Security Agent CPU usage. DS-63106
- Deep Security Agent sometimes showed package signature errors during an upgrade because of a mismatched Certification Revocation List (CRL). DS-62154
- Insufficient host information caused by connectivity issues sometimes resulted in offline or duplicate listings in the **Computers** tab for Deep Security Agents on AWS workspaces. SF04198134/SEG-102818/DS-61666
- Deep Security Agent sometimes could not successfully perform an upgrade because of a missing package. SF04302125/SEG-104084/DS-62692

## Deep Security Agent - 20.0.0-2204 (20 LTS Update 2021-04-12)

Release date: April 12, 2021

Build number: 20.0.0-2204

### Resolved issues

- When Application Control was in block mode, it was unable to build a proper software inventory in some cases. DS-58813
- When Web Reputation was enabled, the system sometimes crashed. SF04258834/SEG-102756/DS-61067
- When Anti-Malware self-protection was enabled, sometimes third-party software could not be installed. SEG-101840/DSSEG-6694
- Behavior Monitoring exceptions sometimes did not work properly. SF03775351/SEG-89899/DSSEG-6718
- With Anti-Malware enabled, network transfer speeds slowed down significantly on some systems. SF04299217/SEG-103986/DSSEG-6780
- Anti-Malware Behavior Monitoring exceptions sometimes did not work properly. SF04259521/SEG-102792/DSSEG-6714

## Deep Security Agent - 20.0.0-2009 (20 LTS Update 2021-03-08)

Release date: March 08, 2021

Build number: 20.0.0-2009

### Enhancements

- Updated Deep Security Agent to include CPU information (number of logical cores) to improve diagnostics and performance tracking. DS-60011

### Resolved issues

- The MQTT connection went offline because an old MQTT connection was not properly cleaned. SF04236908/SEG-102056/DS-60893
- Behavior Monitoring sometimes blocked a program without generating an event. SF03604820/SEG-86752/DS-60526
- When Anti-Malware was enabled, a high amount of CPU was used. SF04106889/SEG-99034/DS-60526
- Deep Security Agent sometimes crashed during an Anti-Malware manual scan. SEG-100231/DSSEG-6664

## Deep Security Agent - 20.0.0-1876 (20 LTS Update 2021-02-08)

Release date: February 08, 2021

Build number: 20.0.0-1876

### Resolved issues

- The Deep Security Agent sometimes crashed when running Intrusion Prevention in passive mode. DS-57497

## Deep Security Agent - 20.0.0-1822 (20 LTS Update 2021-01-18)

Release date: January 20, 2021

Build number: 20.0.0-1822

### Resolved issues

- After a Windows update occurred, "Maintenance mode" for Application Control turned off automatically. SF03905860/SEG-93631/DS-58413

## Deep Security Agent - 20.0.0-1681 (20 LTS Update 2021-01-04)

Release date: January 04, 2021

Build number: 20.0.0-1681

This release contains general improvements.

## Deep Security Agent 20.0.0-1559 (20 LTS Update 2020-12-07)

Release date: December 07, 2020

Build number: 20.0.0-1559

### New features

#### Enhanced platform support

- Windows 10 20H2

#### Improved security

**TLS Directionality**: The manager heartbeat port can now act as both a TLS client and TLS server. Future agents will connect as TLS clients, not TLS servers. This resolves issues with agent-initiated connections through a proxy or firewall that requires TLS sessions to be initiated in the same direction as the TCP layer of the connection.

### Enhancements

- Improved Deep Security Relay's performance by only checking packages that have been modified. DS-55527
- Enhanced memory usage to improve performance. DS-53012
- Deep Security Agent now supports custom actions for Behavior Monitoring and Predictive Machine Learning. DS-48081

### Resolved issues

- When Integrity Monitoring was enabled, a high amount of CPU was used. SEG-88619/03720485/DS-56613
- Application Control events occurred multiple times for the same incident. SEG-86213/SF03620055/DS-57298
- Security updates were not automatically performed on new machines. SEG-91484/SF03828068/DS-57688

## Deep Security Agent 20.0.0-1337 (20 LTS Update 2020-10-28)

Release date: October 28, 2020

Build number: 20.0.0.1337

### New features

**Upgrade to supported paths**: The Upgrade on activation feature only upgrades the agent on the computer from the last two major releases. If the agent does not meet the criteria, you must upgrade the agent manually to a release within the last two major releases. Then the Upgrade on activation feature detects the newer version and complete the upgrade to the designated release.

### Enhancements

- Added various executable files as trusted installers so they are automatically recognized by Application Control. SF03568205/SEG-85141/DS-54884
- Extended the scope of the "If a computer with the same name already exists" setting on **Administration > System Settings > Agents** to apply to existing

unactivated computers. Previously, it only applied to existing activated computers. DS-51800/DS-51879

- Real-time Integrity Monitoring explicitly matches the directory specified in the base directory. Previously, it matched all paths that started with the base directory. DS-52692
- Updated the Integrity Monitoring scan completion time in Deep Security Manager events to display in seconds with a thousands separator. DS-54680

### Resolved issues

- In combined mode with agent-only and agent-preferred settings enabled, Deep Security Notifier sometimes turned the Antivirus status in the Windows action center on and off, which caused high CPU. DS-54799
- After upgrading the Deep Security Agent, the "Sending Application Control Ruleset Failed" error sometimes occurred. DS-49828
- The Behavior Monitoring feature of Anti-Malware sometimes raised false alarms. DS-44974
- When Integrity Monitoring was enabled, the owner of a file was incorrectly changed to a user that did not exist. DS-52058
- When "Serve Application Control rulesets from relays" was enabled, unnecessary relay error events occurred. DS-50905
- Deep Security Agent crashed unexpectedly because it was unable to detect the Docker engine version on Windows Servers. DS-29590
- Deep Security Manager reported a security update timeout because Deep Security Agent received exceptions at security updates. SEG-82072/DS-54720
- There were detection issues with real-time Anti-Malware scans. DS-50286
- Deep Security Manager sometimes showed the incorrect Log Inspection status. SEG-77081/DS-54719
- When a re-transmission packet with new packets was sent, it sometimes produced an "Unsupported SSL Version" Intrusion Prevention event. DS-53144

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-3704/DS-41233

Highest Common Vulnerability Scoring System (CVSS) score: 4.4

Highest severity: Medium

### Known issues

While the Deep Security Relay is upgrading co-located or independent relays, the alerts "Anti-Malware protection is absent or out of date" and "Security Update: Security Update Check and Download Failed (Agent/Appliance error)" might occur for up to 20 minutes or longer before they're automatically resolved and the respective alerts cleared. For any subsequent Deep Security Agent upgrades to succeed, wait for the Deep Security Relay alerts to clear automatically. DS-54056

## Deep Security Agent 20 (long-term support release)

Release date: July 30, 2020

Build number: 20.0.0.877

### New features

#### Improved security

**Agent integrity check**: Deep Security verifies your signature on the Deep Security Agent to ensure that the software files have not changed since the time of signing.

**Protect AWS accounts with incorrect credentials**: In the past, if your credentials were entered incorrectly for AWS accounts in Deep Security, the agent failed to activate. This might have occurred because the credentials were entered incorrectly or because, over time, the credentials changed without a corresponding update on Deep Security. To help ensure protection remains in place in this situation, which in many cases is a simple configuration error, the computer is now created outside of the account and the agent is allowed to activate.

**SSL improvements**: Deep Security supports handshake hello_request (rfc5246) and Extension encrypt_then_mac (rfc7366) in SSL inspection.

### Improved quality and management

**Reboot requirement removed for agent upgrade**: Previously, there were several situations where a Windows server would require a reboot for a new agent to complete the upgrade. The need to reboot when upgrading from Deep Security Agent 11.0, 12.0, or 20.0 on any Windows Operating System has been completely removed, enabling the application to not be impacted as result of upgrading Deep Security Agent.

**Automate the upgrade of agents in your environment**: Deep Security gives you the flexibility to decide if new agents, when activated, should be upgraded to a newer version if one is available. This can be particularly useful in cases where application teams are using older golden images containing a version of the agent that is out of date. Simply enable upgrade on activation, define the lineup of agents you want to use in your environment using Agent Version Control, and as older agents come online and activate they are automatically upgraded for you.

**Instance Metadata Service Version 2 (IMDSv2) support**: IMDSv2 is supported with Deep Security Manager FR 2020-04-30. For details, see "How does Deep Security Agent use the Amazon Instance Metadata Service?" on page 1691

**Actionable recommendations for scan failures**: The Deep Security Agent provides actionable information about why a scheduled malware scan has been canceled, and the recommended actions that should be taken to remedy the failure. For more information, see "Anti-Malware scan failures and cancellations" on page 1054.

**Anti-Malware real-time file scan report**: Deep Security has the ability to determine the top 10 files that are scanned by Anti-Malware real-time scan. This provides a starting point for performance evaluating and tuning, as you can use this information to set file exclusions and avoid unnecessary scans. The 'AmTopNScan.txt' file with the collected data can be generated using the following methods:

- By the command `dsa_control --AmTopNScan`
- By the diagnostic service

**Improved process exceptions**: The process exception experience has been improved in the following ways:

- Information about why process exclusion items are not functioning correctly is now provided, so you can troubleshoot the issue and know which actions to take to

resolve it.
- The process exception configuration workflow has been improved to make it more robust.

**Windows Event Channel for Log Inspection**: Windows Event Channel logging provides a new option for tracking OS and Application logging for Windows platforms newer than Windows Vista. Event channels can be used to collect Log Inspection events which you can view later.

## Enhancements

- Improved the heartbeat handling for Amazon WorkSpaces deployments when the workspace sync feature is not turned on for the matching AWS connector.
- Removed Integrity Monitoring and Application Control's dependency on Anti-Malware, so they no longer require Anti-Malware to be installed to function.
- Added the ability for Deep Security Agent Anti-Malware to scan compressed files no matter their data types when IntelliScan is disabled.
- Added support for agentless mode on vCloud connector for version 9.5 or later.
- Enhanced the agent-initiated activation experience by displaying the activation status (for example, a success message or a message that explains a newer Deep Security Manager version is required) on Deep Security Manager.
- Enhanced the Malware Scan Failure event description to indicate the possible reason.
- Streamlined event management for improved agent performance.
- Added the ability to enable or disable Common Scan Cache for each agent through a CLI command.
- Added support for Deep Security Agent delayed upgrade to reduce the Anti-Malware offline issue after triggering an upgrade.

## Resolved issues

- After upgrading the Deep Security Agent, the "Sending Application Control Ruleset Failed" error sometimes occurred. DS-49828
- Application Control occasionally appeared offline when Application Control and Anti-Malware were enabled at the same time.

- Deep Security Agent restarted unexpectedly because of the way Log Inspection was accessing the SQLite database. DS-48395
- The interface isolation feature stayed active when Firewall was turned off. SEG-32926/DS-27099
- Web Reputation, Firewall, Intrusion Prevention, and Log Inspection couldn't be enabled correctly when the system locale was set to Turkish. DS-48916
- Integrity Monitoring events showed an incorrect file path with Unicode encoding. SEG-45239/DS-33911
- The Windows Update procedure was blocked when Application Control was enabled in Block-Mode. SF02092464/SEG-53938/DS-38578
- Deep Security Agent's Intrusion Prevention module silently dropped zero payload UDP packets. SEG-39711/DS-32799
- For Web Reputation, Deep Security Agent sent the incorrect credentials to the proxy, which returned HTTP 407. SF01704358/SEG-45004/DS-32077
- Deep Security's Notifier.exe process caused high CPU usage. SF01716752/SEG-45507/DS-33645
- The "Smart Protection Server Disconnected for Smart Scan" alert did not automatically clear after the connection had been restored. SF1609675/SEG-43574/DS-32947
- In some cases, the Windows driver did not correctly release spinlock, causing the system to hang. SF01990859/SEG-50709/DS-36066
- Deep Security Agent process sometimes crashed when the detailed logging of SSL message was enabled and outputted. SF01745654/SEG-45832/DS-33007
- When multiple Smart Protection Servers were configured, the Deep Security Agent process would sometimes crash due to an invalid sps_index. SF01415702/SEG-42919/DS-33008
- The Send Policy action failed because of a GetDockerVersion error in Deep Security Agent. SF1939658/SEG-49191/DS-34222
- Deep Security Agent sent invalid JSON objects in response to Deep Security Manager, which caused errors in Deep Security Manager's log file. SF01919585/SEG-48728/DS-34022
- The ds_agent process would sometimes crash under certain conditions when Integrity Monitoring was enabled. SEG-50728/DS-35446

- The Deep Security Agent network engine crashed because the working packet object was deleted accidentally. SF01526046/SF02159742/SEG-55453/DS-38812
- Deep Security Agent restarted abnormally along with an "Unable to send data to Notifier app." error message in ds_agent.log. SEG-21208/DS-33134/DS-21352
- When the system region format is "Chinese (Traditional, Hong Kong SAR)", Deep Security Notifier displayed simplified Chinese instead of traditional Chinese. SEG-48075/DS-34778
- Unicode user names could not be displayed in real-time Integrity Monitoring file scan events. SF02187371/SEG-56645/DS-39398
- Deep Security Agent did not add Python extension module (PYD) files to the inventory of Application Control. SF01804378/SEG-47425/DS-33690
- Too many file open events were being processed in user mode resulting in high CPU usage. SF02179544/SEG-55745/DS-39638
- The Type attribute was not displayed in Integrity Monitoring events when the default STANDARD attribute was set to monitor registry value changes. SF02412251/SEG-59848/DS-41118
- Non-executable files that were opened with execute permissions resulted in security events and drift that should not have been generated. SF01780211/SEG-46616/DSSEG-3607
- High CPU use occurred when Application Control was enabled and the host application was creating a high volume of non-executable files. SF02179544/SEG-55745/DS-41142
- The Windows Update procedure was blocked when Application Control was enabled in Block-Mode. SF02092464/SEG-53938/DS-39981
- Deep Security failed to download security updates because of an outdated user agent string. SF02043400/SEG-52069/DS-41316
- When machines wrote document files to a file server, Anti-Malware needed to scan the files frequently, which caused other machines to fail to write the file because the file was being scanned. SF01949194/SEG-49854/DS-40100
- When Deep Security Agent scanned large files for viruses, it consumed a large amount of memory. SF01572110/SEG-48704/DS-43114

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-3704/VRTS-3176

Highest Common Vulnerability Scoring System (CVSS) score: 7.8

Highest severity: High

- Updated NGINX to 1.16.1. DSSEG-4600
- Updated to curl 7.67.0.
- Updated to openssl-1.0.2t.
- Updated JRE to the latest Java Update (8.0.241/8.43.0.6).

### Known issues

- After upgrading the Deep Security Agent, the "Sending Application Control Ruleset Failed" error may occur. To work around this issue, right-click the affected computer and select **Actions > Clear Warnings/Errors**, then **Send Policy**.
- After upgrading the Deep Security Agent on Windows 2008, Anti-Malware may go offline. If this occurs, fully uninstall Deep Security Agent, reboot your server, then reinstall the agent.

### Upgrade notice

- If you have Application Control enabled, there may be a temporary performance impact while your software inventory is automatically rebuilding. DS-41775

Unix

## Deep Security Agent - 20.0.3-860 (20 LTS Update 2026-01-21)

Release date: January 21, 2026

Build number: 20.0.3-860

### New features

**Endpoint Event Viewer**: Access Endpoint Event Viewer to view all security and system events across managed computers with filtering by period, severity, event origin, and action. This is only supported for Trend Vision One - Server & Workload Protection.

### Resolved issues

- Deep Security Agent crashed when syslog hostnames were longer than 64 characters. PCT-87531/DSA-14252
- When Web Reputation Service was enabled, system memory usage continuously increased. PCT-80352/DSA-13866
- Deep Security Agent sometimes crashed when processing HTTP/2 packets that were formatted differently from what the agent expected. PCT-85552/DSA-13755
- After Deep Security Agent restarted, Intrusion Prevention Detection sometimes stopped working. PCT-82352/DSA-13755

## Deep Security Agent - 20.0.2-29760 (20 LTS Update 2025-12-09)

Release date: December 09, 2025

Build number: 20.0.2-29760

### Enhancements

- Firewall and Intrusion Prevention System events now display process and user info if that data is available. This is being rolled out gradually to all customers. DSA-13741

### Security updates

This release contains updates to third-party libraries. DSA-13204

## Deep Security Agent - 20.0.2-26670 (20 LTS Update 2025-11-12)

Release date: November 12, 2025

Build number: 20.0.2-26670

### New features

**User-based Firewall**: Firewall rules can now be configured based on user account. This feature is being rolled out gradually to all customers.

**Enhanced HTTP/2 support**: The Intrusion Prevention System engine now supports inbound HTTP/2 connections. This feature will be rolled out gradually through backend updates to ensure stability and performance enhancements. (This release also includes fixes aimed at improving HTTP/2 handling and security. PCT-77306/DSA-13105)

### Resolved issues

- Firewall and Intrusion Prevention System events could not be collected due to a missing library in Deep Security Agent for AIX platforms. DSA-13176

## Deep Security Agent - 20.0.2-22850 (20 LTS Update 2025-10-08)

Release date: October 08, 2025

Build number: 20.0.2-22850

### Known issues

- This release excludes the Deep Security Agent package for AIX due to an issue preventing event collection when Intrusion Prevention System or Firewall is enabled. For more information, see The Firewall and IPS events cannot be collected due to a missing library on AIX platform in Trend Micro™ Deep Security™. DSA-13176

## Deep Security Agent - 20.0.2-20480 (20 LTS Update 2025-09-17)

Release date: September 17, 2025

Build number: 20.0.2-20480

This release contains general improvements.

## Deep Security Agent - 20.0.2-17500 (20 LTS Update 2025-08-13)

Release date: August 13, 2025

Build number: 20.0.2-17500

This release contains general improvements.

## Deep Security Agent - 20.0.2-14430 (20 LTS Update 2025-07-09)

Release date: July 09, 2025

Build number: 20.0.2-14430

### Enhancements

- When Advanced TLS Traffic Inspection is enabled, Deep Security Agent now injects packets to speed up the connection as long that connection is not blocked. PCT-63207/DSA-10919

### Resolved issues

- On demand scans could not be started manually until an automatic scan had been triggered, after either an activation or a restart of Deep Security Agent. WS-12581

## Deep Security Agent - 20.0.2-12010 (20 LTS Update 2025-06-11)

Release date: June 11, 2025

Build number: 20.0.2-12010

### Enhancements

- Enabled by default, Web Reputation Service now uses Server Name Indication (SNI) queries when determining the risk level of a website.

### Resolved issues

- Deep Security Agent sometimes crashed during SSL handshake. PCT-55526/DSA-9902

### Security updates

This release contains updates to third-party libraries. DSA-10530

## Deep Security Agent - 20.0.2-9810 (20 LTS Update 2025-05-14)

Release date: May 14, 2025

Build number: 20.0.2-9810

### Enhancements

Web Reputation Service now points to a 403 Forbidden rather than a 200 OK page when blocking an http proxy connection to a suspicious or malicious site. PTC-60576/DSA-10325

### Resolved issues

- Deep Security Agent configurations using advanced TLS caused some systems to freeze. PCT-63207/DSA-10380
- The URL column for **Web Reputation Events** was sometimes missing information. PCT-60576/DSA-10090

## Deep Security Agent - 20.0.2-7600 (20 LTS Update 2025-04-16)

Release date: April 16, 2025

Build number: 20.0.2-7600

This release contains general improvements.

## Deep Security Agent - 20.0.2-4961 (20 LTS Update 2025-03-12)

Release date: March 12, 2025

Build number: 20.0.2-4961

### Enhancements

- The `dsa_scan` command now includes a `scanLargeFile` option for managing larger files. DSA-8825

## Deep Security Agent - 20.0.2-1390 (20 LTS Update 2025-01-15)

Release date: January 15, 2025

Build number: 20.0.2-1390

### Enhancements

- Deep Security Agent now queues packets to handle them in sequence, improving performance. DSA-6916

### Resolved issues

- Deep Security Agent sometimes had connectivity issues when Advanced TLS Traffic Inspection was enabled. DSA-8577

## Deep Security Agent - 20.0.1-25771 (20 LTS Update 2024-12-10)

Release date: December 10, 2024

Build number: 20.0.1-25771

### Resolved issues

- Events including packet data were being logged with an incorrect packet size. PCT-45556/DSA-8074

## Deep Security Agent - 20.0.1-23340 (20 LTS Update 2024-11-13)

Release date: November 13, 2024

Build number: 20.0.1-23340

### Enhancements

- Web Reputation Service can now use Server Name Indication (SNI) queries when determining the risk level of a website. DSA-7314

### Resolved issues

- When Application Control was operating in block mode, files in some directories were being allowed to run when they should have been blocked. PCT-38516/DSA-7613

## Deep Security Agent - 20.0.1-21510 (20 LTS Update 2024-10-16)

Release date: October 16, 2024

Build number: 20.0.1-21510

This release contains general improvements.

## Deep Security Agent - 20.0.1-19250 (20 LTS Update 2024-09-18)

Release date: September 18, 2024

Build number: 20.0.1-19250

This release contains general improvements.

## Deep Security Agent - 20.0.1-17380 (20 LTS Update 2024-08-21)

Release date: August 21, 2024

Build number: 20.0.1-17380

### Resolved issues

- Deep Security Agent could not load the policy if some policy configuration fields contained curly brackets. DSA-6189
- Deep Security Agent would fail to activate if the hostname contained non-ASCII characters. PCT-32214/DSA-6268
- When Intrusion Prevention was enabled for Deep Security Agent, some third-party applications had connectivity issues if they were reusing a source port. SF07685331/PCT-20541/DSA-5596

## Deep Security Agent - 20.0.1-14610 (20 LTS Update 2024-07-17)

Release date: July 17, 2024

Build number: 20.0.1-14610

### Resolved issues

- Integrity Monitoring real-time scans sometimes failed to generate events. SF07269768/PCT-21721/DSA-5877
- Deep Security Agent for AIX platforms was sometimes unable to start without configuring a supported locale. DSA-5876

## Deep Security Agent - 20.0.1-12510 (20 LTS Update 2024-06-19)

Release date: June 19, 2024

Build number: 20.0.1-12510

### Resolved issues

- When Anti-Malware was enabled, Deep Security Agent sometimes failed to shut down completely. PCT-26090/DSA-5492

## Deep Security Agent - 20.0.1-9400 (20 LTS Update 2024-05-16)

Release date: May 16, 2024

Build number: 20.0.1-9400

### Resolved issues

- Using Deep Security Agent with Web Reputation Service enabled prevented some Application Performance Monitoring (APM) applications from functioning correctly. SF04072723/SEG-97952/PCT-15716/DSA-4750
- The Anti-Malware Scheduled Scan on AIX platforms was including Network File System (NFS) contents, which should have been excluded. PCT-13912/DSA-4098

## Deep Security Agent - 20.0.1-7380 (20 LTS Update 2024-04-24)

Release date: April 24, 2024

Build number: 20.0.1-7380

### Enhancements

- Deep Security Agent now supports Trend Vision One Service Gateway exclusions. This is only supported for Trend Cloud One - Endpoint & Workload Security users at this time. V1E-17754
- Updated Deep Security Agent for AIX platforms to increase the pre-remove script timeout to 120 seconds. PCT-19843/DSA-4839

### Resolved issues

- Deep Security Agents running in cloud environments sometimes could not be activated for Trend Cloud One - Endpoint & Workload Security. DSA-4861

## Deep Security Agent - 20.0.1-4540 (20 LTS Update 2024-03-20)

Release date: March 20, 2024

Build number: 20.0.1-4540

This release contains general improvements.

## Deep Security Agent - 20.0.1-3180 (20 LTS Update 2024-02-29)

Release date: February 29, 2024

Build number: 20.0.1-3180

### Resolved issues

- Migration of agents from on-premise Deep Security Manager to Trend Cloud One - Endpoint & Workload Security using Trend Vision One Service Gateway failed. This issue could also occur when migrating using other proxy services. PCT-16649/DSA-4144
- Enabling Intrusion Prevention or Web Reputation Service in Deep Security Agent sometimes resulted in a TLS inspection process (tm_netagent) error log rotation issue. DSA-3965

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-11708/DSA-3702

Highest Common Vulnerability Scoring System (CVSS) score: 7.8

Highest severity: High

### Known issues

- The Application Control Trust Entities "block by target" trust rule sometimes does not work properly when running a copy of an executable file. PCT-11105/DSA-3324

## Deep Security Agent - 20.0.1-690 (20 LTS Update 2024-01-17)

Release date: January 17, 2024

Build number: 20.0.1-690

### Enhancements

- From 2024 onward, Deep Security Agent versioning is being revised from 20.0.0 to 20.0.1. This requires Deep Security Manager 20.0.883 or later. DSA-3584.

  For details, see Platform support updates for Deep Security Agent (DSA) version revision in January 2024 Update Release.

### Resolved issues

- Deep Security Agent was sometimes unable to connect to the local Smart Protection Server. DSA-3564

### Known issues

- Updating to Deep Security Agent 20.0.1-690 from some 20.0.0 versions sometimes fails when using Deep Security Relay on Trend Cloud One - Endpoint & Workload Security. For details, see Failed remote upgrade of self-deployed Workload Security relay from 20.0.0-3445 or later to version revision 20.0.1 DSA-3317

## Deep Security Agent - 20.0.0-8438 (20 LTS Update 2023-12-12)

Release date: December 12, 2023

Build number: 20.0.0-8438

### Resolved issues

- When using a local Smart Protection Server and a configured proxy, Web Reputation Service would sometimes improperly send traffic through the proxy. Web Reputation Service now sends queries to the local Smart Protection Server directly. DSA-2981

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. DSA-2722

Highest Common Vulnerability Scoring System (CVSS) score: 9.8

Highest severity: Critical

### Known issues

- Deep Security Agent is sometimes unable to connect to the local Smart Protection Server. This issue is fixed in 20.0.1-690. For details, see Deep Security Agent connection issues with Smart Protection Server when using proxy DSA-3564

## Deep Security Agent - 20.0.0-8268 (20 LTS Update 2023-11-21)

Release date: November 21, 2023

Build number: 20.0.0-8268

### Resolved issues

- Deep Security Anti-Malware sometimes did not function as expected after the system had resumed from sleep mode (S0 low-power idle mode of the working state, also known as modern standby). SF07326571/PCT-5476/DSA-2485
- Deep Security Agent incorrectly classified MIME type of `.xml` files generated by Microsoft Word, Excel, PowerPoint, as well as `.dwg` files generated by AutoCAD and R2000. SF07027236/SEG-186079/DSA-2202
- A memory leak would occur when loading large Suspicious Object lists. SF06904914/SEG-182231/DSA-1370

## Deep Security Agent - 20.0.0-8137 (20 LTS Update 2023-10-26)

Release date: October 26, 2023

Build number: 20.0.0-8137

This release contains general improvements.

## Deep Security Agent - 20.0.0-7943 (20 LTS Update 2023-09-26)

Release date: September 26, 2023

Build number: 20.0.0-7943

### Enhancements

- New commands exist to get proxy information from the command line:
  ```
  dsa_query -c GetProxyInfo
  dsa_query -c GetProxyInfo details=true
  ```
  DSA-864
- In order to display agent pattern updates properly, Deep Security Agent 20.0.0-7943 or later requires Deep Security Manager 20.0.759 or later. For more information, see Incompatible Agent / Appliance Version error in Deep Security Agent 20.0.0-7943. SEG-190866/SEG-191017/DSA-1531

## Deep Security Agent - 20.0.0-7719 (20 LTS Update 2023-08-29)

Release date: August 29, 2023

Build number: 20.0.0-7719

### Enhancements

- Deep Security Agent no longer updates the Smart Scan agent pattern when Smart Scan is disabled, saving network bandwidth. SEG-186625/DSA-1063
- Deep Security Agent now downloads fewer incremental pattern updates, saving network bandwidth. Note that agents configured as a Deep Security Relay still download all pattern updates. DSA-1000
- The "blocking page" Web Reputation Service redirects users to when they try to access a blocked URL can now be viewed in Czech or Polish. DSA-444
- Intrusion Prevention can now limit how many bytes are scanned for connections with a dynamic port number between 10001-65535. DS-78036
- Advanced Threat Scan Engine has been updated to version 22.6. DSA-453

### Resolved issues

- Stopping the Deep Security Agent service (ds_agent) took longer than usual on some systems. SEG-187365/DSA-1212
- Deep Security Agent sometimes performed security updates even if none were scheduled. SEG-187449/DSA-1064
- Deep Security Agent caused high CPU usage on some systems. SEG-185563/DSA-756

## Deep Security Agent - 20.0.0-7476 (20 LTS Update 2023-07-25)

Release date: July 25, 2023

Build number: 20.0.0-7476

### Enhancements

- Updated the dsa-connect service to improve CPU performance. C1WS-12970

### Resolved issues

- Deep Security Agent upgrades from 20.0.0.6313 to a newer version would sometimes fail, generating an "Abnormal Restart Detected" warning. SF06897730/SEG-180989/DS-78063

## Deep Security Agent - 20.0.0-7303 (20 LTS Update 2023-06-28)

Release date: June 28, 2023

Build number: 20.0.0-7303

### Enhancements

- Deep Security Agent now supports IPv6 addresses using either CIDR or double colon notation, such as fe80:0:0:0:0:0:0:1/24 or fe80::01. SF04849178/SEG-122076/DS-67280
- Web Reputation Service now automatically monitors the ports used by the OS proxy configuration. DS-77233

### Resolved issues

- Deep Security Agents on AIX would sometimes crash when trying to upgrade to a new version. SF06643647/SEG-173140/DS-77359
- Intrusion Prevention (IPS) might not read the correct payload value, which can result in rule malfunctions. DS-74647
- The Deep Security Agent would report "dsa-connect has not provided status" on every heartbeat, even when Endpoint Sensor was not in use. C1WS-14696
- Some MQTT messages would be sent repeatedly and cause dsa-connect to get stuck in a shutdown loop. DS-76709

## Deep Security Agent - 20.0.0-7119 (20 LTS Update 2023-05-29)

Release date: May 29, 2023

Build number: 20.0.0-7119

### Enhancements

- Updated Deep Security Agent for Solaris to add an option to enable collecting interface latency metrics on Azure Data Explorer dashboards. DS-77025

### Resolved issues

- MQTT connection credentials were entered in the Deep Security Agent log file (`ds_agent.log`) in certain scenarios. SEG-174560/C1WS-13282
- Deep Security Agent only reported a single Anti-Malware event for an infected compressed file, even if it contained multiple infected files. DS-76339
- After replacing a connection, Deep Security Agent reported metrics as though it was still connected to the old connection for up to 4 minutes. DS-77453

## Deep Security Agent - 20.0.0-6912 (20 LTS Update 2023-05-02)

Release date: May 02, 2023

Build number: 20.0.0-6912

### Enhancements

- Updated Deep Security Agent to make the connection timeout for proxy probing configurable by adding a line to `ds_agent.ini`. SF06664116/SEG-173848/DS-77182

  Example proxy probing line in `ds_agent.ini` config file: `dsa.proxymanager.ProbeTimeoutInSec=120`

- Updated Deep Security Agent to improve MQTT connection quality and reduce the occurrence of connection timeouts. DS-76840

### Resolved issues

- Deep Security Agent sometimes reported the network driver status incorrectly after the driver had restarted. C1WS-12896
- When Web Reputation Service was enabled, Deep Security Agent caused some systems to shutdown unexpectedly. SF06680505/SEG-174730/DSSEG-7866
- Deep Security Agent sometimes crashed when shutting down after downloading new plugins from the relay. DS-76961

## Deep Security Agent - 20.0.0-6658 (20 LTS Update 2023-03-22)

Release date: March 22, 2023

Build number: 20.0.0-6658

### New features

**Service Gateway**: Deep Security Agent 20.0.0-6658 or later with Deep Security Manager 20.0.741 or later now supports the Service Gateway feature, providing forward proxy functionality.

### Enhancements

- Web Reputation Service now includes OS platform metadata. DS-75453
- Updated Deep Security Agent's logging system to provide additional information and tracing to debug customer issues more efficiently. The agent now generates five (5) log files (`dsa-connect-X.log`) that are 2MB each instead of the agent's previous three 1MB log files. C1WS-9598

  The logger supports an on-demand JSON config file (either `dsa-connect.ini` or `dsa-connect.conf`) with the following configurable options:
  - Debug: Enable the debug log messages. The default value is false.
  - Count: Number of log files to generate. The default value is 5.

- Size: Maximum size of each log file in bytes. The default value is 2097152.

Example config file:

```
{
"Debug": true,
"Count": 5,
"Size": 2097152
}
```

## Resolved issues

- When the Advanced TLS Traffic Inspection "Inspect TLS/SSL traffic" option was set to "No" from the console (**Computer** or **Policy > Intrusion Prevention > General > Advanced TLS Traffic Inspection**), driver-side SSL packets were sometimes still being processed. DS-76160
- Deep Security Agent's Intrusion Prevention System sometimes failed to block "TCP Congestion Flags" properly. DS-76182
- When Anti-Malware Smart Scan was enabled, an IPC connectivity issue caused some systems to crash. SEG-169132/C1WS-10821
- Deep Security Agent security updates were failing due to a file handle issue that prevented files from being removed during an update. DS-75907
- A process thread timeout caused the Anti-Malware Engine to restart unexpectedly on some systems. SF06524736/SEG-169218/DS-76656
- When a SOCKS proxy was used, Deep Security Agent failed to provide a Web Reputation Services rating for HTTP URLs. DS-73482/DS-73364
- Deep Security Agent upgrade sometimes failed because of a missing signature in the agent package. SF06045259/SEG-154576/DS-73668
- Deep Security Agent was incorrectly generating system events showing that the Advanced Threat Search Engine (ATSE) component had been removed on some systems. SEG-147779/DS-75463
- Updated Deep Security Agent to increase the MQTT timeout from 30 minutes to 2 hours to help resolve connection issues on some systems. C1WS-11835

## Deep Security Agent - 20.0.0-6313 (20 LTS Update 2023-01-31)

Release date: January 31, 2023

Build number: 20.0.0-6313

### Enhancements

- Deep Security no longer supports certificates signed with the SHA-1 algorithm. The agent now requires SSL certificates issued using SHA-256 to communicate with the Deep Security Manager. C1WS-5676

### Resolved issues

- Updated Deep Security Agent for AIX platforms to support Advanced Threat Scan Engine (ATSE) version 21.600. DS-75323
- For component updates, Deep Security Agent would attempt with and without use of a proxy and generate an event for each attempt. To make event reporting more straightforward, this behavior has been changed so that after a successful update the agent only shows the final successful event. SF06207160/SEG-160085/DSSEG-7765
- The Deep Security Agent log file (`ds-agent.log`) sometimes failed to rotate, causing it to use more disk space than intended. SF05306459/SEG-137003/DS-72899
- With Web Reputation Enabled, some characters entered in console commands were not being parsed properly. For example, an underscore (`_`) entered in a command was replaced with a dash (`-`), and an uppercase Z was replaced with a lowercase z. DS-74335

## Deep Security Agent - 20.0.0-5953 (20 LTS Update 2022-11-22)

Release date: November 22, 2022

Build number: 20.0.0-5953

This release contains general improvements. **Note that this release only includes an agent for Solaris platforms.**

## Deep Security Agent - 20.0.0-5761 (20 LTS Update 2022-10-21)

Release date: October 21, 2022

Build number: 20.0.0-5761

### Enhancements

- Updated Deep Security Agent to include additional metadata, such as `UserAgent` and `Referrer`, for Web Reputation Services. DS-72196
- Updated Deep Security Agent to include the Integrity Monitoring database in the agent diagnostic package. DS-73293
- Updated Deep Security Agent to support NULL cipher when inspecting TLS traffic with Intrusion Prevention. DS-71085

### Resolved issues

- With Log Inspection enabled, Deep Security Agent sometimes generated "Abnormal Restart Detected" events. SF05951130/SEG-151372/DS-73737
- Virtual Machines using vMotion sometimes deactivated unexpectedly and displayed an Offline (Activation required) status. SEG-153050/DS-73807

## Deep Security Agent - 20.0.0-5512 (20 LTS Update 2022-09-22)

Release date: September 22, 2022

Build number: 20.0.0-5512

### Enhancements

- Updated Deep Security Agent to add multi-thread support for On-Demand scan and Scheduled Scan. DS-72797/DS-72798

### Resolved issues

- Deep Security Agent reported host metadata in an unexpected format. DS-73411

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-8100/VRTS-8101/DS-73087/DS-72528

Highest Common Vulnerability Scoring System (CVSS) score: 7.0

Highest severity: High

## Deep Security Agent - 20.0.0-5394 (20 LTS Update 2022-08-29)

Release date: August 29, 2022

Build number: 20.0.0-5394

### New features

**AIX 7.3 support**: Deep Security Agent 20.0.0-5394 or later with Deep Security Manager 20.0.677 or later now supports AIX 7.3.

### Enhancements

- Application Control now detects software changes for executables with non executable extensions. DS-70805
- Updated Deep Security Agent to add support for inspecting packets using dynamic ports in a TLS connection. DS-71078
- Updated Deep Security Agent to add more metrics for Advanced TLS Inspection. DS-72833

### Resolved issues

- When TLS inspection was done on a UDP connection with dynamic ports, the operating system would sometimes crash. SEG-151169/DS-73043
- Log Inspection Engine would go offline when using '$' character in match or regex fields together with variables. SEG-146965/SEG-146966/DS-72325
- When assigning a policy with real-time Anti-Malware turned off to a new guest VM, it would sometimes turn off real-time Anti-Malware for all other guest VMs registered to the same Deep Security Virtual Appliance. SEG-146057/DS-72856
- Application Control would still block access to network files while in maintenance mode. SF04922652/SEG-131710/DS-72037
- When Application Control is enabled, Adobe plugins were generating unexpected security events. SF05823607/SEG-148570/DS-72679
- Deep Security Agent would return "revision mismatch (-10039)" errors when loading certain configuration files during an agent update. DS-72499
- Deep Security Agent would report detected software changes before Application Control inventory scan was completed. DS-72071

### Known issues

- When executing multiple custom script tasks, new tasks are currently overwritten by previous unfinished tasks. You can execute custom script tasks one by one to bypass this issue. Note that this issue will be fixed in a future release. DS-72699

## Deep Security Agent - 20.0.0-5137 (20 LTS Update 2022-07-26)

Release date: July 26, 2022

Build number: 20.0.0-5137

### Enhancements

- Updated Deep Security Agent to improve Trust Entities functionality. Trust rule wildcard support now includes globstar `\*\*` which matches many sub directories. Single star `\*` now only matches within your current directory. Existing rules that used a single star `\*` to match many folders no longer work and need to be changed to use a globstar `\*\*`. DS-71817

### Resolved issues

- Intrusion Prevention rules with certain setting combinations failed to compile. DS-71889

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-7102/VRTS-7070/VRTS-7041/VRTS-7039/DSSEG-7636

Highest Common Vulnerability Scoring System (CVSS) score: 4.4

Highest severity: Medium

### Known issues

- When executing multiple custom script tasks, new tasks are currently overwritten by previous unfinished tasks. You can execute custom script tasks one by one to bypass this issue. Note that this issue will be fixed in a future release. DS-72699

## Deep Security Agent - 20.0.0-4959 (20 LTS Update 2022-07-04)

Release date: July 4, 2022

Build number: 20.0.0-4959

### Resolved issues

- With Log Inspection enabled, upgrades to Deep Security Agent 20.0.0-4726 encountered "Get Events Failed" and "Command Not Found" alerts. SF05738607/SEG-145679/DS-72117

- When Anti-Malware is enabled alongside Integrity Monitoring, Deep Security Agent caused high CPU usage. SF05169148/SEG-129522/DS-69594
- With Anti-Malware enabled, Deep Security Agent sometimes crashed operating systems that were undergoing an ISO backup. SF05532786/SEG-139280/DS-71299
- Deep Security Agent sometimes created unclear error log entries referencing "invalid" or "badly-formed" proxy URLs. SEG-144613/DS-71866

## Deep Security Agent - 20.0.0-4726 (20 LTS Update 2022-05-31)

Release date: May 31, 2022

Build number: 20.0.0-4726

### Resolved issues

- On AIX servers, when the `LIBPATH` or `LD_LIBRARY_PATH` environment variables for the system are defined, Deep Security Agent sometimes would not start. DS-70882
- Deep Security Agent reported false positive "Created/Deleted" Integrity Monitoring events under some configurations. SF05434164/SEG-136425/DS-70656
- Deep Security Agent had connectivity issues caused when a Server Name Indicator (SNI) used an invalid format. SEG-127761/DS-70806
- An abnormal restart of Deep Security Agent sometimes lead to "Anti-Malware Engine Offline" errors. SEG-140234/DS-71333

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. DS-52329

Highest Common Vulnerability Scoring System (CVSS) score: 7.5

Highest severity: High

## Deep Security Agent - 20.0.0-4416 (20 LTS Update 2022-04-28)

Release date: April 28, 2022

Build number: 20.0.0-4416

### Enhancements

- Updated Deep Security Agent to improve Intrusion Prevention performance when the "Bypass Network Scanner" rule was applied. DS-69515

### Resolved issues

- With Intrusion Prevention enabled, a packet transmission error caused some systems to crash. SEG-136843/DSSEG-7524

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-7132/DS-70518

Highest Common Vulnerability Scoring System (CVSS) score: 7.5

Highest severity: High

## Deep Security Agent - 20.0.0-4185 (20 LTS Update 2022-04-06)

Release date: April 6, 2022

Build number: 20.0.0-4185

### Resolved issues

- Running an Anti-Malware manual scan using the command line sometimes made Deep Security Agent unable to receive incoming connections. SF05385865/SEG-135256/DS-70364
- Application Control sometimes blocked unrecognized software even when running in maintenance mode. SF05234969/SEG-133594/DS-69752
- Log Inspection was unable to parse system logs containing a single digit date format. SF04562942/SEG-115435/DS-69757

## Deep Security Agent - 20.0.0-3964 (20 LTS Update 2022-03-01)

Release date: March 1, 2022

Build number: 20.0.0-3964

### New features

**Threat Intelligence**: Threat Intelligence (formerly known as Connected Threat Defense) provides enhanced malware protection for new and emerging threats. For more information, visit Detect emerging threats using Threat Intelligence.

### Enhancements

- Updated Deep Security Agent to exclude suspicious characters, such as `$`, found in strings from the "Original IP (XFF)" field for Intrusion Prevention events. SEG-129905/DS-68989

## Deep Security Agent - 20.0.0-3770 (20 LTS Update 2022-01-24)

Release date: January 24, 2022

Build number: 20.0.0-3770

### Enhancements

- Updated Deep Security Agent to allow Intrusion Prevention to connect to Deep Security Manager if the manager is using TLS 1.2 strong ciphers. DS-69042

### Resolved issues

- Application Control, Anti-Malware, and Real-time Integrity Monitoring failed to function properly for Deep Security Agents with certain combinations of Integrity Monitoring rules configured. DS-68494

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. DS-68180

Highest Common Vulnerability Scoring System (CVSS) score: 9.1

Highest severity: High

## Deep Security Agent - 20.0.0-3445 (20 LTS Update 2021-11-24)

Release date: November 24, 2021

Build number: 20.0.0-3445

### Enhancements

- Updated Deep Security Agent to use TLS 1.2 strong cipher suite by default to improve security. The agent previously used the CBC cipher suite by default. DS-67204
- Updated Deep Security Agent to support using the "process name" property in "Ignore from source" rules for Application Control Trust Entities on Cloud One Workload Security. DS-67322

- Updated Deep Security Agent's database size management to optimize disk space usage. DS-67347

### Resolved issues

- Deep Security Agent sometimes crashed when it could not connect to Deep Security Manager. DS-67654
- Deep Security Agent sometimes caused connectivity issues, high CPU usage, or the system to crash. SEG-120758/SEG-123885/DS-67291

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-6489/DSSEG-7210/DS-65113

Highest Common Vulnerability Scoring System (CVSS) score: 7.8

Highest severity: High

## Deep Security Agent - 20.0.0-3288 (20 LTS Update 2021-10-28)

Release date: October 28, 2021

Build number: 20.0.0-3288

### New features

- **Evolution of the agent installer**: The Deep Security Agent installer now installs most agent content. This results in the following changes:
  - Agent size requirements have increased, including a slightly larger installer package on most platforms.
  - All agent content is now installed on the computer being protected. Content remains unloaded on a computer until a plug-in is activated by a policy or by the manager console.

- The agent is now much less dependent on relays because all plug-in installations use the content already installed with the agent. This mitigates plug-in install issues due to relay communications because plug-ins can be installed without a connection to a relay.

### Resolved issues

- Deep Security Agent sometimes was unable to connect to the manager via proxies. DS-65929
- Some customers encountered an issue when the run-time CPU number was larger than expected, which led to crashes. DS-65757
- Deep Security Agent sometimes showed package signature errors during an upgrade because of a mismatched Certification Revocation List (CRL). DS-65056

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. DS-46018/DSSEG-7210/DSSEG-7217

Highest Common Vulnerability Scoring System (CVSS) score: 7.8

Highest severity: High

## Deep Security Agent - 20.0.0-3165 (20 LTS Update 2021-10-08)

Release date: October 08, 2021

Build number: 20.0.0-3165

**Note:** Deep Security Agent 20.0.0.3165 has been released to Trend Micro Cloud One - Workload Security customers. However, it is not available on the Deep Security Agent software download page or released to customers using Deep Security Manager.

### New features

- **Evolution of the agent installer**: The Deep Security Agent installer now installs most agent content. This results in the following changes:
  - Agent size requirements have increased, including a slightly larger installer package on most platforms.
  - All agent content is now installed on the computer being protected. Content remains unloaded on a computer until a plug-in is activated by a policy or by the manager console.
  - The agent is now much less dependent on relays because all plug-in installations use the content already installed with the agent. This mitigates plug-in install issues due to relay communications because plug-ins can be installed without a connection to a relay.

### Resolved issues

- Deep Security Agent sometimes was unable to connect to Manager via proxies. DS-65929
- Some customers encountered an issue when the run-time CPU number was larger than expected, led to crashes. DS-65757

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. DSSEG-7210/DSSEG-7217

Highest Common Vulnerability Scoring System (CVSS) score: 7.8

Highest severity: High

## Deep Security Agent - 20.0.0-2921 (20 LTS Update 2021-08-30)

Release date: August 30, 2021

Build number: 20.0.0-2921

### Resolved issues

- Deep Security Agent console commands sometimes failed to return proxy information for Deep Security Relay or Deep Security Manager. DS-65419
- Deep Security Agent sometimes failed to properly display items under **Events and Reports**. DSSEG-7057

## Deep Security Agent - 20.0.0-2740 (20 LTS Update 2021-07-29)

Release date: July 29, 2021

Build number: 20.0.0-2740

### Enhancements

- Updated Deep Security Agent to improve connectivity with Deep Security Manager during agent deployment and activation. DS-62547

### Resolved issues

- Deep Security Agent failed to execute some agent-initiated (dsa_control) console commands. 04564385/SEG-112050/DSSEG-6990
- Deep Security Agent sometimes crashed while trying to establish a connection with Deep Security Manager. 04634804/SEG-113539/DS-64862
- Deep Security Agent sometimes lost connectivity while trying to establish an SSL connection. SF04323898/SEG-107451/DS-64268
- Deep Security Agent was sometimes unable to connect to web applications on systems with older OS versions. SF04451029/SEG-109652/DS-64528
- With Web Reputation enabled, Deep Security Agent caused connectivity issues for some third-party software. SF04072723/SEG-97952/DSSEG-6963
- With Integrity Monitoring enabled, Deep Security Manager caused high CPU usage on the authentication server for some systems. 04488319/SEG-110088/DS-63855

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. SF04613197/SEG-113566/DS-64050

Highest Common Vulnerability Scoring System (CVSS) score: 9.8

Highest severity: High

## Deep Security Agent - 20.0.0-2593 (20 LTS Update 2021-07-01)

Release date: July 01, 2021

Build number: 20.0.0-2593

### Resolved issues

- Deep Security Agent sometimes triggered multiple "Log Inspection Engine Initialized" alerts due to an agent-manager communication issue. SF03968169/SEG-95731/DS-60840
- Integrity Monitoring alerts sometimes triggered but did not appear in the **Events and Reports** tab. 04266346/SEG-103731/DS-62992
- Deep Security Agent failed to detect the correct platform under some configurations. 03804296/SEG-90864/DS-57809
- Application Control was detecting multiple "Application Control Software Changes Detected" events due to '.tmp" files being generated by PowerShell. C1WS-1608

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-5850/DS-54705

Highest Common Vulnerability Scoring System (CVSS) score: 4.4

Highest severity: Medium

## Deep Security Agent - 20.0.0-2395 (20 LTS Update 2021-05-24)

Release date: May 24, 2021

Build number: 20.0.0-2395

### Enhancement

- Deep Security Agent 20.0.0-2395 or later now supports Entrust Root Certificate Authority (G2) certificates. Non-G2 security certificates expire on 2022/07/09. After that date, only Deep Security Agent 20.0.0-2395 or later will have the latest Anti-Malware Smart Scan protection. DS-63010

### Resolved issues

- Deep Security Agent sometimes showed package signature errors during an upgrade because of a mismatched Certification Revocation List (CRL). DS-62154

## Deep Security Agent - 20.0.0-2204 (20 LTS Update 2021-04-12)

Release date: April 12, 2021

Build number: 20.0.0-2204

### New feature

#### Enhanced platform support

- Anti-Malware support for AIX: Deep Security Agent 20.0.0-2204 or later now supports Anti-Malware for AIX 6.1, AIX 7.1, and AIX 7.2.

### Resolved issues

- With Anti-Malware enabled, Deep Security Agent sometimes caused "defunct processes" (that is, processes that remain in the system process table after they've completed execution). SEG-104452/DS-61593
- When Application Control was in block mode, it was unable to build a proper software inventory in some cases. DS-58813
- When Web Reputation was enabled, the system sometimes crashed. SF04258834/SEG-102756/DS-61067

## Deep Security Agent - 20.0.0-2009 (20 LTS Update 2021-03-08)

Release date: March 08, 2021

Build number: 20.0.0-2009

### Resolved issues

- The MQTT connection went offline because an old MQTT connection was not properly cleaned. SF04236908/SEG-102056/DS-60893

## Deep Security Agent - 20.0.0-1876 (20 LTS Update 2021-02-08)

Release date: February 08, 2021

Build number: 20.0.0-1876

## Deep Security Agent - 20.0.0-1822 (20 LTS Update 2021-01-18)

Release date: January 20, 2021

Build number: 20.0.0-1822

### New feature

**Anti-Malware support for AIX**: Deep Security Agent 20.0.0-1822 or later now supports Anti-Malware for AIX 7.1 and 7.2.

## Deep Security Agent - 20.0.0-1681 (20 LTS Update 2021-01-04)

Release date: January 04, 2021

Build number: 20.0.0-1681

This release contains general improvements.

## Deep Security Agent 20.0.0-1559 (20 LTS Update 2020-12-07)

Release date: December 07, 2020

Build number: 20.0.0-1559

### New features

**TLS Directionality**: The manager heartbeat port can now act as both a TLS client and TLS server. Future agents will connect as TLS clients, not TLS servers. This resolves issues with agent-initiated connections through a proxy or firewall that requires TLS sessions to be initiated in the same direction as the TCP layer of the connection.

### Enhancements

- Improved Deep Security Relay's performance by only checking packages that have been modified. DS-55527
- Enhanced memory usage to improve performance. DS-53012

### Resolved issues

- On Solaris servers where Integrity Monitoring was enabled and the rule: "Unix - Monitor Processes Running From '/tmp' Directories (ATT&CK T1059)" was assigned, a rule compile error was generated that referenced an "Unsupported Feature in Integrity Monitoring Rule". DS-55884

- When Integrity Monitoring was enabled, a high amount of CPU was used.  SEG-88619/03720485/DS-56613
- Application Control events occurred multiple times for the same incident. SEG-86213/SF03620055/DS-57298
- Security updates were not automatically performed on new machines. SEG-91484/SF03828068/DS-57688

## Deep Security Agent 20.0.0-1337 (20 LTS Update 2020-10-28)

Release date: October 28, 2020

Build number: 20.0.0.1337

### Resolved issues

- When using Deep Security Agent on Solaris, the Integrity Monitoring port scanning feature did not work because the agent did not have access to information on the user ID under which a given port was opened. This prevented storage of any listening port information. The port scanning feature on Solaris agents has been modified to store the string "n/a" for the userid. This allows the remaining port information to be stored and used in the port scanning function. However, exclusions and inclusions based on User ID still do not function correctly because this information is not available. DS-53922

## Deep Security Agent 20.0.0-1304 (20 LTS Update 2020-10-21)

Release date: October 21, 2020

Build number: 20.0.0.1304

### Enhancements

- Updated the Integrity Monitoring scan completion time in Deep Security Manager events to display in seconds with a thousands separator. DS-54680

### Resolved issues

- Deep Security Manager reported a security update timeout because Deep Security Agent received exceptions at security updates. SEG-82072/DS-54720
- Deep Security Manager sometimes showed the incorrect Log Inspection status. SEG-77081/DS-54719

## Deep Security Agent 20.0.0-1194 (20 LTS Update 2020-10-05)

Release date: October 5, 2020

Build number: 20.0.0.1194

### Enhancements

- Extended the scope of the "If a computer with the same name already exists" setting on **Administration > System Settings > Agents** to apply to existing unactivated computers. Previously, it only applied to existing activated computers. DS-51800
- Integrity Monitoring detects changes to the "setuid" and "setgid" attributes for Linux and Unix platforms. DS-52061

### Resolved issues

- Anti-Malware directory exclusion with wildcards didn't match subdirectories correctly. DS-50245
- Deep Security Agent crashed on Solaris 10 during upgrades. SEG-72634/SF02975849/DS-49295
- When Integrity Monitoring was enabled, the owner of a file was incorrectly changed to a user that did not exist. DS-52058

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-3704/DS-41233

Highest Common Vulnerability Scoring System (CVSS) score: 4.4

Highest severity: Medium

## Deep Security Agent 20 (long-term support release)

Release date: July 30, 2020

Build number: 20.0.0.877

### New features

#### Improved security

**SSL improvements**: Deep Security supports handshake hello_request (rfc5246) and Extension encrypt_then_mac (rfc7366) in SSL inspection.

**Agent integrity check**: Deep Security verifies your signature on the Deep Security Agent to ensure that the software files have not changed since the time of signing.

#### Improved quality and management

**Upgrade to supported paths**: The Upgrade on activation feature only upgrades the agent on the computer from the last two major releases. If the agent does not meet the criteria, you must upgrade the agent manually to a release within the last two major releases. Then the Upgrade on activation feature will detect the newer version and complete the upgrade to the designated release.

**Actionable recommendations for scan failures**: The Deep Security Agent provides actionable information about why a scheduled malware scan has been canceled, and the recommended actions that should be taken to remedy the failure. For more information, see "Anti-Malware scan failures and cancellations" on page 1054.

**Anti-Malware real-time file scan report**: Deep Security has the ability to determine the top 10 files that are scanned by Anti-Malware real-time scan. This provides a starting point for performance evaluating and tuning, as you can use this information to set file exclusions and avoid unnecessary scans. The 'AmTopNScan.txt' file with the collected data can be generated using the following methods:

- By the command `dsa_control --AmTopNScan`
- By the diagnostic service

**Improved process exceptions**: The process exception experience has been improved in the following ways:

- Information about why process exclusion items are not functioning correctly is now provided, so you can troubleshoot the issue and know which actions to take to resolve it.
- The process exception configuration workflow has been improved to make it more robust.

**Automate the upgrade of agents in your environment**: Deep Security gives you the flexibility to decide if new agents, when activated, should be upgraded to a newer version if one is available. This can be particularly useful in cases where application teams are using older golden images containing a version of the agent that is out of date. Simply enable upgrade on activation, define the lineup of agents you want to use in your environment using Agent Version Control, and as older agents come online and activate they are automatically upgraded for you.

## Enhancements

- Integrity Monitoring detects changes to the "setuid" and "setgid" attributes for Linux and Unix platforms.
- Improved the heartbeat handling for Amazon WorkSpaces deployments when the workspace sync feature is not turned on for the matching AWS connector.
- Extended the scope of the **If a computer with the same name already exists** setting on **Administration > System Settings > Agents** to apply to existing unactivated computers. Previously, it only applied to existing activated computers.
- Increased the scan engine's URI path length limitation.
- Added the ability for Deep Security Agent Anti-Malware to scan compressed files no matter their data types when IntelliScan is disabled.
- Streamlined event management for improved agent performance.
- Added the ability to enable or disable Common Scan Cache for each agent through a CLI command.

- Added the ability for Deep Security Agent Anti-Malware to scan compressed files no matter their data types when IntelliScan is disabled.

## Resolved issues

- After upgrading the Deep Security Agent, the "Sending Application Control Ruleset Failed" error sometimes occurred. DS-49828
- Application Control occasionally appeared offline when Application Control and Anti-Malware were enabled at the same time.
- The displayed packet header data contained redundant payload data. DS-45792
- Memory leaked during SSL decryption because of a flaw in the SSL processing. SEG-68263/DS-44360
- On specific Deep Security Agent servers the CPU usage spiked to 100% and pattern merges failed during the active update process. SEG-66210/02711299/DS-46429
- When a security update was triggered before Anti-Malware was ready, the security updates failed. DS-36952
- When real-time Integrity Monitoring was enabled with the rule "1002875: Unix Add/Remove Software" applied, the RPM database potentially locked. SEG-67275/SF02663756/DS-48524
- Web Reputation, Firewall, Intrusion Prevention, and Log Inspection couldn't be enabled correctly when the system locale was set to Turkish. SEG-71825/SF03021819/DS-48916
- Incorrect linking of certain libraries could lead to Deep Security Agent instability. SEG-72958/03071960/DS-49324
- Anti-Malware directory exclusion with wildcard didn't match subdirectories correctly. SF03131855/SEG-74892/DS-50245
- High CPU use occurred when Application Control was enabled and the host application was creating a high volume of non-executable files. SF02179544/SEG-55745/DS-41142
- Non-executable files that were opened with execute permissions resulted in security events and drift that should not have been generated. SF01780211/SEG-46616/DSSEG-3607

- Deep Security Agent did not add Python extension module (PYD) files to the inventory of Application Control. SF01804378/SEG-47425/DS-33690
- Unicode user names could not be displayed in real-time Integrity Monitoring file scan events. SF02187371/SEG-56645/DS-39398
- The Deep Security Agent network engine crashed because the working packet object was deleted accidentally. SF01526046/SF02159742/SEG-55453/DS-38812
- The ds_agent process would sometimes crash under certain conditions when Integrity Monitoring was enabled. SEG-50728/DS-35446
- Deep Security Agent sent invalid JSON objects in response to Deep Security Manager, which caused errors in Deep Security Manager's log file. SF01919585/SEG-48728/DS-34022
- The "Send Policy" action failed because of a GetDockerVersion error in Deep Security Agent. SF1939658/SEG-49191/DS-34222
- When multiple Smart Protection Servers were configured, the Deep Security Agent process would sometimes crash due to an invalid sps_index. SF01415702/SEG-42919/DS-33008
- For Web Reputation, Deep Security Agent sent the incorrect credentials to the proxy, which returned HTTP 407. (SF01704358/SEG-45004/DS-32077)
- Deep Security Agent's Intrusion Prevention module silently dropped zero payload UDP packets. SEG-39711/DS-32799
- Integrity Monitoring events showed an incorrect file path with Unicode encoding. SEG-45239/DS-33911
- The interface isolation feature was still on when Firewall was turned off. SEG-32926/DS-27099
- After applying rule 1006540, "Enable X-Forwarded-For HTTP Header Logging", Deep Security would extract the X-Forwarded-For header for Intrusion Prevention events correctly. However, a URL intrusion like "Invalid Traversal" would be detected in the HTTP request string before the header was parsed. The Intrusion Prevention engine has been enhanced to search X-Forwarded-For header after the header is parsed. SEG-60728/DS-42332
- Deep Security Agent sent invalid JSON objects in response to Deep Security Manager, which caused errors in Deep Security Manager's log file. SEG-48728/SF01919585/DS-34022

- On Solaris servers with clusters, the Deep Security Intrusion Prevention module would come under heavy load while inspecting the clusters' private traffic. The extra load caused latency issues, node evictions, and loss of synchronization events.

  You can now configure the Packet Processing Engine on the agent to bypass traffic inspection on a specified interface. Where a specific interface on a computer is dedicated to cluster private traffic, this configuration can be used to bypass inspection of packets sent to and received from this interface. This results in faster packet processing on the bypassed interface and other interfaces.

  Use of this configuration to bypass traffic inspection is a security risk. It is up to you to determine if the benefit of reduced latency outweighs the risk involved. It is also up to you to determine whether only the nodes in the cluster have access to the subnet whose interface is being bypassed.

  To implement the bypass, do the following:

1. Upgrade the Deep Security Agent to the latest build containing this fix.
2. Create a file under /etc directory named "ds_filter.conf".
3. Open the /etc/ds_filter.conf file.
4. Add the MAC addresses of all NIC cards used for cluster communication, as follows:

   ```
   MAC_EXCLUSIVE_LIST=XX:XX:XX:XX:XX,XX:XX:XX:XX:XX
   ```
5. Save.
6. Wait 60 seconds for your changes to take effect.

In the /etc/ds_filter.conf file:

- The MAC_EXCLUSIVE_LIST line must be the first line in the file.
- All letters in the MAC address must be uppercase.
- Leading zeros in each byte must be included.

  Valid MAC_EXCLUSIVE_LIST:

  ```
  MAC_EXCLUSIVE_LIST=0B:3A;12:F8:32:5E
  ```

  ```
  MAC_EXCLUSIVE_LIST=0B:3A;12:F8:32:5E,6A:23:F0:0F:AB:34
  ```

  Invalid MAC_EXCLUSIVE_LIST:

```
MAC_EXCLUSIVE_LIST=B:3A;12:F8:32:5E
```

```
MAC_EXCLUSIVE_LIST=0b:3a;12:F8:32:5e,6a:23:F0:0F:ab:34
```

```
MAC_EXCLUSIVE_LIST=0B:3A;12:F8:32:5E
```

If the MAC address is not valid, the interface is not bypassed. If the exact string "MAC_EXCLUSIVE_LIST=" is not present at the beginning of the line, no interfaces are bypassed. DSSEG-4055

### Security updates

Security updates are included in this release. For more information about how Trend Micro protects against vulnerabilities, visit Vulnerability Response. Note that in line with responsible disclosure practices, Common Vulnerabilities and Exposures (CVE) details will only be made available for select security updates once patches have been made available for all impacted releases. VRTS-3704/VRTS-3176

Highest Common Vulnerability Scoring System (CVSS) score: 7.8

Highest severity: High

- Updated NGINX to 1.16.1. DSSEG-4600
- Updated to curl 7.67.0.
- Updated to openssl-1.0.2t.
- Updated JRE to the latest Java Update (8.0.241/8.43.0.6).

**macOS** (supported for Cloud One Workload Security only)

# Compatibility

## System requirements

Each part of a Deep Security deployment has its own system requirements:

- "Deep Security Manager requirements" on the next page
- "Deep Security Agent requirements" on page 386

- "Deep Security Relay requirements" on page 388

Requirements vary by version: for older versions of Deep Security Manager, agents, relays, or virtual appliances, consult the corresponding documentation.

If you are planning to operate Deep Security in FIPS mode, see "FIPS 140 support" on page 1639 for additional requirements.

## Deep Security Manager requirements

For a list of agent versions that are compatible with this version of the manager, see "Agent platform compatibility" on page 389.

| System component | Requirements |
|---|---|
| Minimum memory (RAM) | Minimum RAM requirements depend on the number of agents that are being managed. See "Deep Security Manager sizing" on page 468.<br>On Linux, reserved system memory is separate from process memory. Therefore, although the installer's estimate might be similar, it detects less RAM than the computer actually has. To verify the computer's actual total RAM, log in with a superuser account and execute the following command: `grep MemTotal /proc/meminfo` |
| Minimum disk space | 1.5 GB (200 GB recommended) |
| Operating system | • Red Hat Enterprise Linux 10 (64-bit)<br>• Red Hat Enterprise Linux 9 (64-bit)<br>• Red Hat Enterprise Linux 8 (64-bit)<br>• Red Hat Enterprise Linux 7 (64-bit)<br>• Windows Server 2019 (64-bit)<br>• Windows Server 2016 (64-bit)<br>• Windows Server 2012 or 2012 R2 (64-bit)<br>• Windows Server 2022 (64-bit)<br>Windows operating systems running in a Server Core configuration are not currently supported. |

| System component | Requirements |
|---|---|
| | **Note:** If you are upgrading your Deep Security Manager and are currently using Windows Server 2008, you should add a new Deep Security Manager node on a supported operating system (see "Install Deep Security Manager on multiple nodes" on page 511). When done, decommission the node running on Windows Server 2008. |
| Database | • PostgreSQL 17.n (Core, Amazon RDS, Amazon Aurora distributions only)<br>• PostgreSQL 16.n (Core, Amazon RDS, Amazon Aurora distributions only)<br>• PostgreSQL 15.n (Core, Amazon RDS, Amazon Aurora distributions only)<br>• PostgreSQL 14.n (Core, Amazon RDS, Amazon Aurora distributions only)<br>• Microsoft SQL Server 2022 and its service packs<br>• Microsoft SQL Server 2019 and its service packs<br>• Microsoft SQL Server 2017 and its service packs<br>• Microsoft SQL Server 2016 and its service packs<br>• Microsoft SQL Relational Database Service (RDS)<br>• Azure SQL Database  multi-tenancy)<br>• Oracle 19c when deployed as software or when used with Amazon RDS<br>• Oracle 23c when deployed as software<br>Note the following:<br>• Microsoft SQL Server Express is only supported in limited deployments. See "Microsoft SQL Server Express considerations" on page 503.<br>• Microsoft SQL Server is only supported when database containment is set to NONE. For details, see Contained Databases.<br>• Oracle Database Express (XE) is not supported. |

| System component | Requirements |
|---|---|
| Web browser | Cookies must be enabled.<br>It is recommended to use the latest version of the following browsers:<br>• Firefox<br>• Microsoft Edge<br>• Google Chrome<br>• Apple Safari on a Mac |

# Deep Security Agent requirements

## Windows Agent

| System component | Requirements |
|---|---|
| CPU | • Physical server: Intel Pentium Dual-Core or equivalent minimum, 4-Core or greater recommended<br>• Virtual machine: 4 vCPU or greater recommended |
| RAM | 2 GB minimum, 4 GB recommended |
| Disk | 1 GB |

## Linux Agent

| System component | Requirements |
|---|---|
| CPU | • Physical server: Intel Pentium Dual-Core or equivalent minimum, 4-Core or greater recommended<br>• Virtual machine: 4 vCPU or greater recommended |
| RAM | 2 GB minimum, 5 GB recommended |

| System component | Requirements |
|---|---|
| Disk | 1 GB |

### Solaris Agent

| System component | Requirements |
|---|---|
| CPU | Oracle SPARC processors |
| RAM | 4 GB minimum, 4 GB recommended |
| Disk | 2 GB |

### AIX Agent

| System component | Requirements |
|---|---|
| CPU | IBM Power processors |
| RAM | 4 GB minimum, 4 GB recommended |
| Disk | 2 GB |

Installing the agent is only supported if the AIX Operating System is configured with the en_US locale.

### Red Hat OpenShift Agent

| System component | Requirements |
|---|---|
| CPU | • Physical server: Intel Pentium Dual-Core or equivalent minimum, 4-Core or greater recommended<br>• Virtual machine: 4 vCPU or greater recommended |
| RAM | 2 GB remaining memory in the node |
| Disk | 1.5 GB |

For information on supported operating systems, see "Agent platform compatibility" on the next page.

For information on supported features, see Supported Deep Security features vary by platform.

The agent installer permits installation on any supported platform. RAM and disk space requirements are not checked.

## Deep Security Relay requirements

Requirements are the same as those of the Deep Security Agent, with the following constraints:

- Relays are only supported on 64-bit operating systems.
- Relays are not supported on Solaris, AIX, or Red Hat OpenShift.
- Disk space requirements are greater for the Relay.

| Platform | Minimum RAM | Recommended RAM | Minimum disk space for relay |
|---|---|---|---|
| Windows | 2 GB | 4 GB | 30 GB |
| Linux | 2 GB | 4 GB | 30 GB |

If protected computers use VMware vMotion, add 10 GB of disk space to the Deep Security Relay to which the agent is connected.

Generally, relays require more disk space if you install Deep Security Agent on many different platforms, as relays store update packages for each platform. For details, see "Get Deep Security Agent software" on page 520.

In smaller deployments, relays can be co-located with a Deep Security Manager. However, if your deployment has a large number of agents (more than 10,000), then relays should be installed on separate, dedicated servers, as overloaded relays slow down update redistribution. See also "Plan the best number and location of relays" on page 1346.

# Agent requirements

## Agent platform compatibility

Deep Security Agent can be installed on cloud, virtual computers, or physical computers that support the container or operating system and kernel. Support is shown in the following table, with these indicators:

✓ – Supported. If support was added in an update, then the minimum required version is indicated in the footnote.

• – Support for these releases is ending soon. Upgrade as soon as possible.

Even though Deep Security Manager supports older versions of Deep Security Agent, you should still upgrade agents when possible. New agent releases provide more security and protection, higher quality, performance improvements, and updates to stay in sync with OS releases. Regular software upgrades also ensure that, if an agent fix is required, you can update once, as opposed to installing multiple updates along a supported upgrade path. Each agent has an end-of-life date. For details, see Deep Security Agent LTS lifecycle date and Deep Security Agent FR lifecycle dates.

Not all Deep Security features are available on all platforms. For more information, see "Supported features by platform" on page 425.

For details on extended support for legacy versions, see Deep Security LTS life cycle date - Support extensions.

For details on supported Windows 10 update releases, see Deep Security Support for Windows 10 and Deep Security Support for Windows Server Core.

For details on supported Windows 11 update releases, see Trend Cloud One - Endpoint & Workload Security and Deep Security Support for Windows 11.

Deep Security Agent and kernel support packages for Red Hat Enterprise Linux are also available for AlmaLinux, CentOS, Miracle Linux, and Rocky Linux.

| Operating System | Agent Version | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 20.0.3 LTS | 20.0.2 LTS | 20.0.1 LTS | 20.0.0 LTS | 12 LTS | 11 LTS | 10 LTS | 9.6 |
| AIX 6.1 TL 9 or later 3, 12 | | | | ✓ | ✓ 24 | | | |
| AIX 7.1 TL 3 or later 3, 59 | | ✓ | ✓ | ✓ | ✓ 24 | | | |
| AIX 7.2 TL 0 or later 3 | ✓ | ✓ | ✓ | ✓ | ✓ | | | |
| AIX 7.3 TL 0 or later 3 | ✓ | ✓ | ✓ | ✓ 35 | | | | |
| AlmaLinux 8 (64-bit) 6 | ✓ | ✓ | ✓ | ✓ 29 | | | | |
| AlmaLinux 9 (64-bit) 38 | ✓ | ✓ | ✓ | ✓ 37 | | | | |
| Amazon Linux (64-bit) 52 | | | ✓ | ✓ | ✓ | ✓ | | |
| Amazon Linux 2 (64-bit) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| Amazon Linux 2 (AWS Arm-based Graviton2) | ✓ | ✓ | ✓ | ✓ 27 | | | | |
| Amazon Linux 2 (AWS Arm-based Graviton3) | ✓ | ✓ | ✓ | ✓ 34 | | | | |
| Amazon | ✓ | ✓ | ✓ | ✓ 39 | | | | |

| Operating System | Agent Version | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 20.0.3 LTS | 20.0.2 LTS | 20.0.1 LTS | 20.0.0 LTS | 12 LTS | 11 LTS | 10 LTS | 9.6 |
| Linux 2023 (64-bit) | | | | | | | | |
| Amazon Linux 2023 (AWS Arm-based Graviton2) | ✓ | ✓ | ✓ | ✓ 39 | | | | |
| CentOS 5 (32-bit and 64-bit) | | | | | | | ✓ | |
| CentOS 6 (32-bit and 64-bit) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| CentOS 7 (64-bit) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| CentOS 8 (64-bit) | ✓ | ✓ | ✓ | ✓ | ✓ 23 | ✓ 32 | | |
| CloudLinux 5 (32-bit and 64-bit) | | | | | | | | ✓ |
| CloudLinux 6 (32-bit) | | | | | | | ✓ | |
| CloudLinux 6 (64-bit) | | | | | | ✓ 16 | | |
| CloudLinux 7 (64-bit) 52 | | | ✓ | ✓ | ✓ | ✓ | | |
| CloudLinux 8 (64-bit) | ✓ | ✓ | ✓ | ✓ | 26 | | | |

| Operating System | Agent Version | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 20.0.3 LTS | 20.0.2 LTS | 20.0.1 LTS | 20.0.0 LTS | 12 LTS | 11 LTS | 10 LTS | 9.6 |
| Debian Linux 6 (64-bit) | | | | | | | | ✓ |
| Debian Linux 7 (64-bit) | | | | | ✓ | ✓ | | |
| Debian Linux 8 (64-bit) [12] | | | | ✓ | ✓ | ✓ | | |
| Debian Linux 9 (64-bit) [52] | | | ✓ | ✓ | ✓ | ✓ | | |
| Debian Linux 10 (64-bit) [60] | | ✓ | ✓ | ✓ | ✓ [21] | ✓ [20] | | |
| Debian Linux 11 (64-bit) | ✓ | ✓ | ✓ | ✓ [31] | | | | |
| Debian Linux 12 (64-bit) | ✓ | ✓ | ✓ | ✓ [43] | | | | |
| Debian Linux 13 (64-bit) [57] | ✓ | ✓ | | | | | | |
| Miracle Linux 8 (64-bit) | ✓ | ✓ | ✓ | ✓ [40] | | | | |
| Miracle Linux 9 (64-bit) | ✓ | ✓ | ✓ | ✓ [42] | | | | |
| Oracle Linux 5 (32-bit and 64-bit) | | | | | | | ✓ | |
| Oracle Linux 6 (32-bit and 64-bit) [52] | | | ✓ | ✓ | ✓ | ✓ | | |
| Oracle Linux | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | |

| Operating System | Agent Version | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 20.0.3 LTS | 20.0.2 LTS | 20.0.1 LTS | 20.0.0 LTS | 12 LTS | 11 LTS | 10 LTS | 9.6 |
| 7 (64-bit) | | | | | | | | |
| Oracle Linux 8 (64-bit) | ✓ | ✓ | ✓ | ✓ | ✓ 22 | ✓ 20 | | |
| Oracle Linux 9 (64-bit) | ✓ | ✓ | ✓ | ✓ | | | | |
| Oracle Linux 10 (64-bit) | ✓ 56 | ✓ 56 | | | | | | |
| Red Hat Enterprise Linux 5 (32-bit and 64-bit) | | | | | | | ✓ | |
| Red Hat Enterprise Linux 6 (32-bit and 64-bit) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| Red Hat Enterprise Linux 7 (64-bit) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| Red Hat Enterprise Linux Workstation 7 (64-bit) | ✓ | ✓ | ✓ | ✓ 37 | | | | |
| Red Hat Enterprise Linux 8 (64-bit) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ 18 | | |

| Operating System | Agent Version | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 20.0.3 LTS | 20.0.2 LTS | 20.0.1 LTS | 20.0.0 LTS | 12 LTS | 11 LTS | 10 LTS | 9.6 |
| Red Hat Enterprise Linux 8 (AWS Arm-based Graviton2) | ✓ | ✓ | ✓ | ✓ 31 | | | | |
| Red Hat Enterprise Linux 8 (64-bit IBM Z (s390x)) | ✓ 57 | ✓ 57 | | | | | | |
| Red Hat Enterprise Linux 8.6 (PowerPC little-endian) | ✓ | ✓ | ✓ 41 | | | | | |
| Red Hat Enterprise Linux 9 (64-bit) | ✓ | ✓ | ✓ | ✓ 34 | | | | |
| Red Hat Enterprise Linux 9 (PowerPC little-endian) | ✓ | ✓ | ✓ 50 | | | | | |
| Red Hat Enterprise Linux 9 (64-bit Arm (aarch64)) | ✓ | ✓ | ✓ | ✓ 53 | | | | |
| Red Hat Enterprise Linux 9 (64-bit IBM Z | ✓ 57 | ✓ 57 | | | | | | |

Table Cell Outside Table: Rocky Linux 10 (64-bit) 57

Table Cell Outside Table: ✓

Table Cell Outside Table: ✓

Table Cell Outside Table:

Table Cell Outside Table:

| Operating System | Agent Version | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 20.0.3 LTS | 20.0.2 LTS | 20.0.1 LTS | 20.0.0 LTS | 12 LTS | 11 LTS | 10 LTS | 9.6 |
| (s390x)) | | | | | | | | |
| Red Hat Enterprise Linux 10 (64-bit) | ✓ | ✓ | ✓ | ✓ 55 | | | | |
| Table Cell Outside Table: Rocky Linux 10 (64-bit) 57 | | | | | | | | |
| Table Cell Outside Table: ✓ | | | | | | | | |
| Red Hat OpenShift supported versions | ✓ | ✓ | ✓ | ✓ 48 | | | | |
| Table Cell Outside Table: ✓ | | | | | | | | |
| Table Cell Outside Table: | | | | | | | | |
| Rocky Linux 8 (64-bit) 6 | ✓ | ✓ | ✓ | ✓ 29 | | | | |
| Table Cell Outside Table: | | | | | | | | |
| Table Cell Outside Table: | | | | | | | | |
| Rocky Linux 9 (64-bit) 7 | ✓ | ✓ | ✓ | ✓ 36 | | | | |
| Table Cell Outside Table: | | | | | | | | |
| Solaris 10 Updates 4-6 (64-bit or SPARC) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ 16 | | |
| Table Cell Outside Table: | | | | | | | | |
| Table Cell Outside Table: | | | | | | | | |
| Solaris 10 Updates 7-10 (64-bit or SPARC) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ 16 | | |
| Solaris 10 Update 11 (64-bit or SPARC) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ 16 | | |
| Solaris 11.0 (1111)-11.1 (64-bit or SPARC) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ 16 | | |
| Solaris 11.2-11.3 (64-bit | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ 16 | | |

Table Cell Outside Table: Rocky Linux 10 (64-bit) 57

Table Cell Outside Table: ✓

Table Cell Outside Table: ✓

Table Cell Outside Table:

Table Cell Outside Table:

Table Cell Outside Table:

Table Cell Outside Table:

| Operating System | Agent Version | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 20.0.3 LTS | 20.0.2 LTS | 20.0.1 LTS | 20.0.0 LTS | 12 LTS | 11 LTS | 10 LTS | 9.6 |
| or SPARC) | | | | | | | | |
| Solaris 11.4 (64-bit or SPARC) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ 17 | | |
| SUSE Linux Enterprise Server 11 (32-bit and 64-bit) | | | | | ✓ | ✓ | ✓ | |
| SUSE Linux Enterprise Server 12 (64-bit) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| SUSE Linux Enterprise Server 12 (PowerPC little-endian) | ✓ | ✓ | ✓ 44 | | | | | |
| SUSE Linux Enterprise Server 15 (64-bit) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ 19 | | |
| SUSE Linux Enterprise Server 15 (PowerPC little-endian) | ✓ | ✓ | ✓ 44 | | | | | |
| SUSE Linux Enterprise Server 15 (AWS Arm-based graviton2) | ✓ | ✓ | ✓ 46 | | | | | |

Table Cell Outside Table: Rocky Linux 10 (64-bit) 57

Table Cell Outside Table: ✓

Table Cell Outside Table: ✓

Table Cell Outside Table:

Table Cell Outside Table:

Table Cell Outside Table:

Table Cell Outside Table:

| Operating System | Agent Version | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 20.0.3 LTS | 20.0.2 LTS | 20.0.1 LTS | 20.0.0 LTS | 12 LTS | 11 LTS | 10 LTS | 9.6 |
| Ubuntu 10.04 (64-bit) | | | | | | | | ✓ |
| Ubuntu 12.04 (64-bit) | | | | | | | | ✓ |
| Ubuntu 14.04 (64-bit) | | | | | | | ✓ | |
| Ubuntu 16.04 (64-bit) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| Ubuntu 18.04 (64-bit) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ 14 | | |
| Ubuntu 18.04 (AWS Arm-based Graviton2) | ✓ | ✓ | ✓ | ✓ 28 | | | | |
| Ubuntu 20.04 (64-bit) | ✓ | ✓ | ✓ | ✓ | ✓ 25 | | | |
| Ubuntu 20.04 (AWS Arm-based Graviton2) | ✓ | ✓ | ✓ | ✓ 29 | | | | |
| Ubuntu 22.04 (64-bit) | ✓ | ✓ | ✓ | ✓ 33 | | | | |
| Ubuntu 22.04 (AWS Arm-based Graviton2) | ✓ | ✓ | ✓ | ✓ 35 | | | | |
| Ubuntu 24.04 (64-bit) | ✓ | ✓ | ✓ 49 | | | | | |

Table Cell Outside Table: Rocky Linux 10 (64-bit) 57

Table Cell Outside Table: ✓

Table Cell Outside Table: ✓

Table Cell Outside Table:

Table Cell Outside Table:

Table Cell Outside Table:

| Operating System | Agent Version | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 20.0.3 LTS | 20.0.2 LTS | 20.0.1 LTS | 20.0.0 LTS | 12 LTS | 11 LTS | 10 LTS | 9.6 |
| Ubuntu 24.04 (AWS Arm-based Graviton2) | ✓ 58 | ✓ 58 | | | | | | |
| Windows 2000 Service Pack 3 or 4 (32-bit) 4 | | | | | | | | ✓ 13 |
| Windows XP (32-bit and 64-bit) 4, 8 | | | | | | | ✓ | |
| Windows Server 2003 SP1 or SP2 (32-bit and 64-bit) 4, 9 | | | | | | | ✓ | |
| Windows Server 2003 R2 SP2 (32-bit and 64-bit) 4, 9 | | | | | | | ✓ | |
| Windows 7 (32-bit and 64-bit) 12 | | | | ✓ | ✓ | ✓ | | |
| Windows 7 Embedded (32-bit) 1, 5, 12 | | | | ✓ | ✓ | | | |
| Windows Server 2008 (32-bit and 64- | | | | ✓ | ✓ | ✓ | | |

Table Cell Outside Table: Rocky Linux 10 (64-bit) 57

Table Cell Outside Table: ✓

Table Cell Outside Table: ✓

Table Cell Outside Table:

Table Cell Outside Table:

Table Cell Outside Table:

| Operating System | Agent Version | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 20.0.3 LTS | 20.0.2 LTS | 20.0.1 LTS | 20.0.0 LTS | 12 LTS | 11 LTS | 10 LTS | 9.6 |
| bit) 2, 10, 12 | | | | | | | | |
| Windows Server 2008 R2 (64-bit) 2, 11, 54 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| Windows 8 (32-bit and 64-bit) 5, 12 | | | | ✓ | ✓ | ✓ | | |
| Windows 8.1 (32-bit and 64-bit) 12 | | | | ✓ | ✓ | ✓ | | |
| Windows 8.1 Embedded (32-bit) 1, 12 | | | | ✓ | ✓ | ✓ | | |
| Windows 10 (32-bit and 64-bit) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| Windows 10 IoT Enterprise 2019 LTSC (32-bit and 64-bit) 1 | ✓ | ✓ | ✓ | ✓ | ✓ | | | |
| Windows 10 IoT Enterprise 2021 LTSC (64-bit) 1 | ✓ | ✓ | ✓ | ✓ | ✓ | | | |
| Windows 10 Enterprise multi-session (64-bit) | ✓ | ✓ | ✓ | ✓ | | | | |

Table Cell Outside Table: Rocky Linux 10 (64-bit) [57]

Table Cell Outside Table: ✓

Table Cell Outside Table: ✓

Table Cell Outside Table:

Table Cell Outside Table: ✓

Table Cell Outside Tabl

| Operating System | Agent Version | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 20.0.3 LTS | 20.0.2 LTS | 20.0.1 LTS | 20.0.0 LTS | 12 LTS | 11 LTS | 10 LTS | 9.6 |
| Windows 11 (64-bit) | ✓ | ✓ | ✓ | ✓ | | | | |
| Windows Server 2012 (64-bit) [54] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| Windows Server 2012 R2 (64-bit) [54] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| Windows Server 2016 (LTSC, version 1607) (64-bit) [54] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| Windows Server Core (SAC, version 1709) (64-bit) [5] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| Windows Server 2019 (LTSC, version 1809) (64-bit) [54] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [15] | | |
| Windows Server 2022 (LTSC, version 21H2) (64-bit) [54] | ✓ | ✓ | ✓ | ✓ [30] | | | | |

Table Cell Outside Table: Rocky Linux 10 (64-bit) 57

Table Cell Outside Table: ✓

Table Cell Outside Table: ✓

Table Cell Outside Table:

Table Cell Outside Table:

Table Cell Outside Table:

Table Cell Outside Table:

Table Cell Outside Table:

Table Cell Outside Table:

| Operating System | Agent Version | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | 20.0.3 LTS | 20.0.2 LTS | 20.0.1 LTS | 20.0.0 LTS | 12 LTS | 11 LTS | 10 LTS | 9.6 |
| Windows Server 2025 (LTSC version 24H2) (64-bit) | ✓ 51 | ✓ 51 | | | | | | |

## Minor Linux version compatibility

Trend Micro releases agents for major Linux versions, such as Red Hat Enterprise Linux 9. Minor Linux versions, such as Red Hat Enterprise Linux 9.n, are also compatible if they use a kernel supported by the agent.

To determine if the computer has a supported kernel, see your OS provider's documentation and compare the computer's kernel version with "Linux kernel compatibility" on page 408.

## Docker compatibility

Deep Security Agent 10.0 and later can protect Docker hosts and containers running on Linux distributions. Windows is not supported.

Deep Security Agent releases support recent stable versions of Docker. Long-term support (LTS) DSA releases support only Docker versions that have not reached end-of-life. Deep Security does not support Docker Edge releases.

Do not upgrade to the latest stable release of Docker until Trend Micro announces support for it in the latest release of Deep Security.

Deep Security support for Docker releases includes any subversions of those releases. For example, Deep Security Agent 11.0 supports Docker 17.09-ce, including its subversions 17.09.0-ce and 17.09.1-ce.

| Agent Version | Docker | | Docker CE | | | | | | | | | | | | Docker EE | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | v1.12 | v1.13 | 17.03 | 17.09 | 17.12 | 18.03 | 18.06 | 18.09 | 19.03 | 20.10 | 23.0 | 24.0 | 25.0 | 26.0 | 17.06 | 18.03 | 18.06 | 18.09 | 19.03 | 20.10 |
| 10 LTS | ✓ | ✓ | | | | | | | | | | | | | | | | | | |
| 11 LTS | | | ✓ | ✓ | ✓ | | | | | | | | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 11.1 | | | | | ✓ | ✓ | | | | | | | | | ✓ | ✓ | | | | |
| 11.2 | | | | | | ✓ | ✓ | | | | | | | | ✓ | ✓ | | | | |
| 11.3 | | | | | | | ✓ | ✓ | | | | | | | ✓ | ✓ | | | | |
| 12 LTS | | | | | | | ✓ | ✓ | | | | | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 12 FR | | | | | | | | | ✓ | | | | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 20 LT | | | | | | | | | ✓ | ✓ | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

| Agent Version | Docker | | Docker CE | | | | | | | | | | | | Docker EE | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | v1.12 | v1.13 | 17.03 | 17.09 | 17.12 | 18.03 | 18.06 | 18.09 | 19.03 | 20.10 | 23.0 | 24.0 | 25.0 | 26.0 | 17.06 | 18.03 | 18.06 | 18.09 | 19.03 | 20.10 |
| S | | | | | | | | | | | | | | | | | | | | |

**Footnotes:**

1

Because embedded operating systems typically run on custom hardware (for example, on point-of-sale terminals), you should thoroughly test your hardware platform before deployment in a production environment. Trend Micro tests Windows Embedded platforms in a virtualized environment. If you need to create a service ticket for Trend Micro Support, try to reproduce the problem in a virtualized environment. If the issue cannot be reproduced in a virtualized environment, and is specific to your custom hardware, Trend Micro Support might require you to provide remote access to it for diagnostics.

Note that Windows 10 IoT was formerly named Windows 10 Embedded, and is therefore considered a Windows Embedded platform.

2

Requires a Full or Desktop Experience installation. Server Core is not supported.

3

Supported AIX configurations are AIX LPARs on a PowerVM Hypervisor on a Power Server and AIX as the bare metal OS on a Power Server.

4

In August 2019, Microsoft changed code signing requirements to stop using SHA-1 and use only SHA-2. Therefore, these legacy OS must have the patch installed to enable verification of SHA-2 signatures on later update releases of Deep Security Agent. See also:

- Updated guidance for use of Trend Micro Deep Security to protect Windows 2003, Windows XP, and Windows 2000 based systems

- New versions of Trend Micro Deep Security Agents for Windows will only be signed with SHA-2

5

In February 2023, Microsoft changed code signing requirements, but has not released a patch for this OS. Therefore the last supported update release for Deep Security Agent 20 is in January 2023.

6

AlmaLinux 8 and Rocky Linux 8 are supported by Deep Security Agent 20.0.0-3288 and later for Red Hat Enterprise Linux 8.

7

Rocky Linux 9 is supported on Deep Security Agent 20.0.0-6313 and later for Red Hat Enterprise Linux 9.

8

Windows XP support requires Deep Security Agent 10.0 Update 25 or earlier.

9

Windows Server 2003 support requires either Deep Security Agent 10.0 Update 25 or earlier, or Deep Security Agent 10.0 Update 29 or later. It is not supported with Updates 26, 27, and 28. See also Deep Security Agent version 10 update 26 cannot be used for installation or upgrade on Windows XP/2003.

10

Windows Server 2008 support requires the SP2 service pack.

11

Windows Server 2008 R2 support requires the SP1 service pack.

12

In the second half of 2023, Deep Security Agent 20 for Windows Server 2008, AIX 6.1, and Debian Linux 8 reached end of standard support. For more information, see Platform support updates for Deep Security Agent (DSA) version revision in January 2024 Update Release.

13

Requires Deep Security Agent 9.6.2-8436 U17 (2018-05-03) or later.

14
Requires Deep Security Agent 11.0.0-390 U2 (2018-09-18) or later.

15

Requires Deep Security Agent 11.0.0-514 U4 (2018-12-04) or later.

16

Requires Deep Security Agent 11.0.0-582 U6 (2019-01-23) or later.

17

Requires Deep Security Agent 11.0.0-615 U7 (2019-02-22) or later.

18

Requires Deep Security Agent 11.0.0-796 U12 (2019-06-22) or later.

19

Requires Deep Security Agent 11.0.0-871 U13 (2019-07-26) or later.

20

Requires Deep Security Agent 11.0.0-946 U14 (2019-08-29) or later.

21

Requires Deep Security Agent 12.0.0-481 U1 (2019-08-09) or later.

22

Requires Deep Security Agent 12.0.0-563 U2 (2019-09-13) or later.

23

Requires Deep Security Agent 12.0.0-682 U3 (2019-11-05) or later.

24

Requires Deep Security Agent 12.0.0-767 U5 (2019-12-16) or later.

25

Requires Deep Security Agent 12.0.0-1090 U10 (2020-05-28) or later.

26

Requires Deep Security Agent 12.5.0-936 FR (2020-05-19) or later.

**27**

Requires Deep Security Agent 20.0.0-1822 (20 LTS Update 2021-01-18) or later.

**28**

Requires Deep Security Agent 20.0.0-3165 (20 LTS Update 2021-10-08) or later.

**29**

Requires Deep Security Agent 20.0.0-3288 (20 LTS Update 2021-10-28) or later.

**30**

Requires Deep Security Agent 20.0.0-3445 (20 LTS Update 2021-11-24) or later.

**31**

Requires Deep Security Agent 20.0.0-3964 (20 LTS Update 2022-03-01) or later.

**32**

Requires Deep Security Agent 11.0.0-328 U17 (2022-06-15) or later.

**33**

Requires Deep Security Agent 20.0.0-4959 (20 LTS Update 2021-07-04) or later.

**34**

Requires Deep Security Agent 20.0.0-5137 (20 LTS Update 2022-07-26) or later.

**35**

Requires Deep Security Agent 20.0.0-5394 (20 LTS Update 2022-08-29) or later.

**36**

Requires Deep Security Agent 20.0.0-6313 (20 LTS Update 2023-01-31) or later.

**37**

Requires Deep Security Agent 20.0.0-6912 (20 LTS Update 2023-05-02) or later.

**38**

AlmaLinux 9 is supported by Deep Security Agent 20.0.0-6912 and later for Red Hat Enterprise Linux 9.

**39**

Requires Deep Security Agent 20.0.0-7303 (20 LTS Update 2023-06-28) or later.

40

Miracle Linux 8 is supported by Deep Security Agent 20.0.0-7719 (20 LTS Update 2023-08-29) or later for Red Hat Enterprise Linux 8.

41

Requires Deep Security Agent 20.0.0-7943 (20 LTS Update 2023-09-26) or later.

42

Miracle Linux 9 is supported by Deep Security Agent 20.0.0-8137 (20 LTS Update 2023-10-26) or later for Red Hat Enterprise Linux 9.

43

Requires Deep Security Agent 20.0.0-8438 (20 LTS Update 2023-12-12) or later.

44

Requires Deep Security Agent 20.0.1-7380 (20 LTS Update 2024-04-24) or later.

45

Requires Deep Security Agent 20.0.1-12510 (20 LTS Update 2024-06-26) or later.

46

Requires Deep Security Agent 20.0.1-14610 (20 LTS Update 2024-07-20) or later.

47

Requires Deep Security Agent 20.0.0-8268 (20 LTS Update 2023-11-21) or later.

48

See Deep Security Agent version for Red Hat OpenShift

49

Requires Deep Security Agent 20.0.1-19250 (20 LTS Update 2024-09-18) or later.

50

Requires Deep Security Agent 20.0.1-21510 (20 LTS Update 2024-10-16) or later.

51

Requires Deep Security Agent 20.0.2-1390 (20 LTS Update 2025-01-15) or later.

52

Deep Security Agent 20 no longer supports Amazon Linux 1, Cloud Linux 7, Debian Linux 9 or Oracle Linux 6. For more information, see Platform support updates for Deep Security Agent (DSA) in January 2025 Update Release.

53

Requires Deep Security Agent 20.0.2-7600 (20 LTS Update 2025-04-16) or later.

54

The Window OS patch update is required due to enforcement of Azure Code Signing (ACS) by Microsoft. For details, see The agent minimum Windows version requirements for updated binaries.

55

Requires Deep Security Agent 20.0.2-14431 (20 LTS Update 2025-07-09) or later.

56

Requires Deep Security Agent 20.0.2-20480 (20 LTS Update 2025-09-24) or later.

57

Requires Deep Security Agent 20.0.2-26670 (20 LTS Update 2025-11-20) or later.

58

Requires Deep Security Agent 20.0.2-29370 (20 LTS Update 2025-12-09) or later.

59

Deep Security Agent 20 no longer supports AIX 7.1. See Limited Support for Debian 10 and AIX 7.1 in 2026 Product Release.

60

Deep Security Agent 20 no longer supports Debian Linux 10. See Limited Support for Debian 10 and AIX 7.1 in 2026 Product Release.

## Linux kernel compatibility

Deep Security supports the following Linux kernel scopes:

- General kernel, which includes general-purpose Linux kernels available to all customers. These kernels are provided by supported operating system partners listed in Deep Security Agent platform compatibility.
- Select extended support kernel, which includes the following:
  - Red Hat Enterprise Linux (RHEL). For information, see Extended Update Support (EUS).
  - SuSE Enterprise Server (SLES). For information, see Long-Term Service Pack Support (LTSS).

When a new kernel is detected, new kernel support packages are typically released within two weeks. If new kernels require driver modifications, additional development, or extended testing cycles, the release time frame might be extended.

Supported Linux kernels vary by the agent version:

- Deep Security Agent 20 Linux kernel support
- Deep Security Agent Feature Releases (12.5) Linux kernel support
- Deep Security Agent 12.0 Linux kernel support
- Deep Security Agent 11.3 Linux kernel support
- Deep Security Agent 11.2 Linux kernel support
- Deep Security Agent 11.1 Linux kernel support
- Deep Security Agent 11.0 Linux kernel support
- Deep Security Agent 10.3 Linux kernel support
- Deep Security Agent 10.2 Linux kernel support
- Deep Security Agent 10.1 Linux kernel support
- Deep Security Agent 10.0 Linux kernel support
- Deep Security Agent 9.6 SP1 Linux kernel support
- Deep Security Agent 9.5 SP1 Linux kernel support

You can also use a JSON list of Linux kernels that the agent supports with scripts and automated workflows.

## Disable optional Linux kernel support package updates

When Deep Security Agent has any of the following security modules enabled, compatible kernel modules must be installed on localhost in order for the agent to load and provide security protection:

- Anti-Malware
- Application Control
- Firewall
- Integrity Monitoring
- Intrusion Prevention
- Web Reputation Service

If compatible kernel modules have not been installed, then Deep Security Agent downloads and installs the latest kernel support package, regardless of whether or not the **Automatically update kernel package when agent restarts** setting is enabled.

If compatible kernel modules have already been installed and the **Automatically update kernel package when agent restarts** setting is enabled, then Deep Security Agent downloads and installs the latest kernel support package.

When a Deep Security Agent upgrades, the previously installed kernel modules become incompatible with the agent because the agent version is newer than the kernel support package. Thus, the agent downloads and installs the latest kernel support package regardless of whether or not the **Automatically update kernel package when agent restarts** setting is enabled.

When upgrading the Linux kernel to a new version, the previously installed kernel modules become incompatible with Linux kernel. Thus, the agent downloads and installs the latest kernel support package regardless whether or not the **Automatically update kernel package when agent restarts** setting is enabled.

In previous agent versions, the kernel driver update process always downloaded the latest kernel support package from the relay when an agent was restarted or the computer rebooted. For agent 20.0.0-3067 or later with Deep Security Manager 20.0.503 or later, you can disable optional kernel support package updates to improve performance. For details, see "Supported features by platform" on page 425.

### Disable kernel support package updates on one computer

1. In Deep Security Manager, go to **Computers**.
2. Double-click the computer where you want to disable kernel support package updates (or select the computer and then select **Details**).
3. Select **Settings**. From **Automatically update kernel package when agent restarts**, select **No**.
4. Save your changes.

### Disable kernel support package updates on multiple computers

1. In Deep Security Manager, go to **Policies**.
2. Double-click the policy that protects multiple computers where you want to disable kernel support package updates (or select the policy and then **Details**).
3. Select **Settings**. From **Automatically update kernel package when agent restarts**, select **No**.
4. Save your changes.

## Linux file system compatibility

Real-time Anti-Malware scans require compatible file system hooks. On Linux platforms, various file systems can be used. Compatible file systems are shown in the following table.

**Note:** To protect network file systems, you must select **Enable network directory scan** in the malware scan configuration. For information, see "Scan a network directory (real-time scan only)" on page 759.

| File System Type | | Agent Version | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 20 | 12 FR | 12.0 | 11.3 | 11.2 | 11.1 | 11.0 | 10.3 | 10.2 | 10.1 | 10.0 | 9.6 |
| Disk file systems | ext2 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | ext3 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | ext4 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | XFS | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | Btrfs | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | VFAT | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Optical discs | ISO 9660 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Special file systems | tmpfs | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | aufs | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| | OverlayFS | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Network file systems (see Note, below) | NFSv3 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | NFSv4 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | SMB | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | CIFS | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | FTP | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

## Linux systemd support

Some agent versions support systemd for Linux.

✓ – Supported. If support was added in an update, then the minimum required version is indicated in the footnote.

• – Support for these releases is ending soon. Upgrade as soon as possible.

| Operating System | Agent Version | | | |
|---|---|---|---|---|
| | 20 LTS | 12 FR | 12 LTS | 11 LTS |
| AlmaLinux 8 (64-bit) | ✓ 9 | | | |
| AlmaLinux 9 (64-bit) | ✓ 16 | | | |
| Amazon Linux 2 (64-bit) | | | | |
| Amazon Linux 2 (AWS ARM-Based Graviton 2) | ✓ 7 | | | |
| Amazon Linux 2 (AWS ARM-Based Graviton 3) | ✓ 12 | | | |
| Amazon Linux 2023 (64-bit) | ✓ 17 | | | |
| Amazon Linux 2023 (AWS ARM-Based Graviton 2) | ✓ 17 | | | |
| CloudLinux 8 (64-bit) | ✓ | ✓ 5 | | |
| Debian Linux 10 (64-bit) | ✓ | ✓ | ✓ 3 | ✓ 4 |
| Debian Linux 11 (64-bit) | ✓ 10 | | | |
| Debian Linux 12 (64-bit) | ✓ 21 | | | |
| Debian Linux 13 (64-bit) | ✓ 30 | | | |
| Miracle Linux 8 (64-bit) | ✓ 18 | | | |
| Miracle Linux 9 (64-bit) | ✓ 20 | | | |
| Oracle Linux 7 (64-bit) | ✓ | ✓ | ✓ 3 | ✓ 2 |
| Oracle Linux 8 (64-bit) | ✓ | ✓ | ✓ 6 | ✓ 4 |
| Oracle Linux 9 (64-bit) | ✓ 15 | | | |
| Oracle Linux 10 (64-bit) | ✓ 29 | | | |
| Red Hat Enterprise Linux 7 (64-bit) | ✓ | ✓ | ✓ 3 | ✓ 2 |
| Red Hat Enterprise Linux 8 (64-bit) | ✓ | ✓ | ✓ | ✓ 1 |

| Operating System | Agent Version | | | |
|---|---|---|---|---|
| | 20 LTS | 12 FR | 12 LTS | 11 LTS |
| Red Hat Enterprise Linux 8 (AWS ARM-Based Graviton 2) | ✓ 10 | | | |
| Red Hat Enterprise Linux 8.6 (PowerPC little-endian) | ✓ 19 | | | |
| Red Hat Enterprise Linux 9 (64-bit) | ✓ 12 | | | |
| Red Hat Enterprise Linux 9 (PowerPC little-endian) | ✓ 26 | | | |
| Red Hat Enterprise Linux 9 (64-bit Arm (aarch64)) | ✓ 27 | | | |
| Red Hat Enterprise Linux 10 (64-bit) | ✓ 28 | | | |
| Rocky Linux 8 (64-bit) | ✓ 9 | | | |
| Rocky Linux 9 (64-bit) | ✓ 14 | | | |
| Rocky Linux 10 (64-bit) | ✓ 30 | | | |
| SUSE Linux Enterprise Server 12 (PowerPC little-endian) | ✓ 22 | | | |
| SUSE Linux Enterprise Server 15 (64-bit) | ✓ | ✓ | ✓ | ✓ 2 |
| SUSE Linux Enterprise Server 15 (PowerPC little-endian) | ✓ 22 | | | |
| SUSE Linux Enterprise Server 15 SP5 (AWS Arm-based Graviton2) | ✓ 24 | | | |
| Ubuntu 18.04 (64-bit) | ✓ | ✓ | | |
| Ubuntu 18.04 (AWS ARM-Based Graviton 2) | ✓ 9 | | | |
| Ubuntu 20.04 (64-bit) | ✓ | | | |
| Ubuntu 20.04 (AWS ARM-Based Graviton 2) | ✓ 9 | | | |
| Ubuntu 22.04 (64-bit) | ✓ 11 | | | |
| Ubuntu 22.04 (AWS ARM-Based Graviton 2) | ✓ 13 | | | |

| Operating System | Agent Version | | | |
|---|---|---|---|---|
| | 20 LTS | 12 FR | 12 LTS | 11 LTS |
| Ubuntu 24.04 (64-bit) | ✓ 25 | | | |
| Ubuntu 24.04 (AWS Arm-based Graviton2) | ✓ 31 | | | |

**Footnotes:**

1

Requires Deep Security Agent 11.0.0-796 U12 (2019-06-22) or later.

2

Requires Deep Security Agent 11.0.0-871 U13 (2019-07-26) or later.

3

Requires Deep Security Agent 12.0.0-481 U1 (2019-08-09) or later.

4

Requires Deep Security Agent 11.0.0-946 U14 (2019-08-29) or later.

5

Requires Deep Security Agent 12.5.0-936 FR (2020-05-19) or later.

6

Requires Deep Security Agent 12.0.0-563 U2 (2019-09-13) or later.

7

Requires Deep Security Agent 20.0.0-1822 (20 LTS Update 2021-01-18) or later.

8

Requires Deep Security Agent 20.0.0-3165 (20 LTS Update 2021-10-08) or later.

9

Requires Deep Security Agent 20.0.0-3288 (20 LTS Update 2021-10-28) or later.

10

Requires Deep Security Agent 20.0.0-3964 (20 LTS Update 2022-03-01) or later.

[11] Requires Deep Security Agent 20.0.0-4959 (20 LTS Update 2021-07-04) or later.

[12] Requires Deep Security Agent 20.0.0-5137 (20 LTS Update 2022-07-26) or later.

[13] Requires Deep Security Agent 20.0.0-5394 (20 LTS Update 2022-08-29) or later.

[14] Requires Deep Security Agent 20.0.0-6313 (20 LTS Update 2023-01-31) or later.

[15] Requires Deep Security Agent 20.0.0-6658 (20 LTS Update 2023-03-22) or later.

[16] Requires Deep Security Agent 20.0.0-6912 (20 LTS Update 2023-05-02) or later.

[17] Requires Deep Security Agent 20.0.0-7303 (20 LTS Update 2023-06-28) or later.

[18] Miracle Linux 8 is supported by Deep Security Agent 20.0.0-7719 (20 LTS Update 2023-08-29) or later for Red Hat Enterprise Linux 8.

[19] Requires Deep Security Agent 20.0.0-7943 (20 LTS Update 2023-09-26) or later.

[20] Miracle Linux 9 is supported by Deep Security Agent 20.0.0-8137 (20 LTS Update 2023-10-26) or later for Red Hat Enterprise Linux 9.

[21] Requires Deep Security Agent 20.0.0-8438 (20 LTS Update 2023-12-12) or later.

[22] Requires Deep Security Agent 20.0.1-7380 (20 LTS Update 2024-04-24) or later.

23
Requires Deep Security Agent 20.0.1-12510 (20 LTS Update 2024-06-26) or later.

24

Requires Deep Security Agent 20.0.1-14610 (20 LTS Update 2024-07-20) or later.

25

Requires Deep Security Agent 20.0.1-19250 (20 LTS Update 2024-09-18) or later.

26

Requires Deep Security Agent 20.0.1-21510 (20 LTS Update 2024-10-16) or later.

27

Requires Deep Security Agent 20.0.2-7600 (20 LTS Update 2025-04-16) or later.

28

Requires Deep Security Agent 20.0.2-14431 (20 LTS Update 2025-07-09) or later.

29

Requires Deep Security Agent 20.0.2-20480 (20 LTS Update 2025-09-24) or later.

30

Requires Deep Security Agent 20.0.2-26670 (20 LTS Update 2025-11-20) or later.

31

Requires Deep Security Agent 20.0.2-29370 (20 LTS Update 2025-12-09) or later.

## Linux Secure Boot support

Some versions of Deep Security Agent (DSA) for Linux support Secure Boot. See also Configure Linux Secure Boot for agents.

In DSA 20 LTS, each Linux operating system is associated with corresponding Secure Boot public keys, such as DS2022.der, DS20_V2.der, and so on. These keys have different expiration dates. For more information, see "Update the Trend Micro public key - The public key has expired" in Configure Linux Secure Boot for agents.

See also Deep Security release strategy and life cycle policy.

## Deep Security Agent 20 LTS

The following table lists Linux operating systems on which DSA 20 LTS provides support for Secure Boot.

VMware and physical machines are supported on all operating systems included in the table. Azure, AWS, and GCP support is limited to certain operating systems.

| Operating System | Secure Boot public key | Required DSA build | Support on Azure VM [1] |
|---|---|---|---|
| AlmaLinux 9 (64-bit) | DS2022.der | 20.0.0-6912 (20 LTS Update 2023-05-02) or later | ✓ |
| CentOS 7 (64-bit) | DS2022.der [2] | | |
| CentOS 8 (64-bit) | DS2022.der [2] | | |
| Debian Linux 10 (64-bit) | DS2022.der [2] | | |
| Debian Linux 11 (64-bit) | DS2022.der | | |
| Debian Linux 12 (64-bit) | DS2022.der | 20.0.0-8438 (20 LTS Update 2023-12-12) or later | ✓ |
| Debian Linux 13 (64-bit) | DS2022.der | 20.0.2-26670 (20 LTS Update 2025-11-20) or later | ✓ |
| Miracle Linux 9 (64-bit) | DS2022.der | 20.0.0-8137 (20 LTS Update 2023-10-26) or later for Red Hat Enterprise Linux 9 | |
| Oracle Linux 7 (64-bit) | DS20_V2.der | 20.0.0-3165 (20 LTS Update 2021-10-08) or later | |
| Oracle Linux 8 (64-bit) | DS20_V2.der | 20.0.0-3288 (20 LTS Update 2021-10-28) or later | ✓ [3] |
| Oracle Linux 9 (64-bit) | DS2022.der | | ✓ [3] |
| Oracle Linux 10 (64- | DS2022.der | 20.0.2-20480 (20 LTS Update 2025- | ✓ [3] |

| Operating System | Secure Boot public key | Required DSA build | Support on Azure VM [1] |
|---|---|---|---|
| bit) | | 09-24) or later | |
| Red Hat Enterprise Linux 7 (64-bit) | DS2022.der [2] | | |
| Red Hat Enterprise Linux 8 (64-bit) | DS2022.der [2] | | ✓ |
| Red Hat Enterprise Linux 9 (64-bit) | DS2022.der | | ✓ |
| Red Hat Enterprise Linux 10 (64-bit) | DS2022.der | | ✓ |
| Red Hat Enterprise Linux Workstation 7 (64-bit) | DS2022.der [2] | 20.0.0-6912 (20 LTS Update 2023-05-02) or later | |
| Rocky Linux 9 (64-bit) | DS2022.der | 20.0.0-6313 (20 LTS Update 2023-01-31) or later | |
| Rocky Linux 10 (64-bit) | DS2022.der | 20.0.2-26670 (20 LTS Update 2025-11-20) or later | |
| SUSE Linux Enterprise Server 12 (64-bit) | DS2022.der [2] | | |
| SUSE Linux Enterprise Server 15 (64-bit) | DS2022.der, DS20_V2.der [2] | | ✓ |
| Ubuntu 16.04 (64-bit) | DS2022.der [2] | | |
| Ubuntu 18.04 (64-bit) | DS2022.der [2] | | ✓ |
| Ubuntu 20.04 (64-bit) | DS2022.der [2] | | ✓ |
| Ubuntu 22.04 (64-bit) | DS2022.der | 20.0.0-6658 (20 LTS Update 2023-03-22) or later | ✓ |

| Operating System | Secure Boot public key | Required DSA build | Support on Azure VM [1] |
|---|---|---|---|
| Ubuntu 24.04 (64-bit) | DS2022.der | 20.0.1-19250 (20 LTS Update 2024-09-18) or later | |

## Deep Security Agent 12 FR

The following table lists Linux operating systems on which DSA 12 FR provides support for Secure Boot.

VMware and physical machines are supported on all operating systems included in the table, whereas AWS, GCP, and Azure are not supported. See also Secure Boot support.

| Operating System |
|---|
| CentOS 7 (64-bit) |
| CentOS 8 (64-bit) |
| Debian Linux 10 (64-bit) |
| Red Hat Enterprise Linux 7 (64-bit) |
| Red Hat Enterprise Linux 8 (64-bit) |
| SUSE Linux Enterprise Server 12 (64-bit) |
| SUSE Linux Enterprise Server 15 (64-bit) |
| Ubuntu 16.04 (64-bit) |
| Ubuntu 18.04 (64-bit) |

Note that the information about the public keys and required DSA build is not applicable to this DSA release.

## Deep Security Agent 12 LTS

The following table lists Linux operating systems on which DSA 12 LTS provides support for Secure Boot.

VMware and physical machines are supported on all operating systems included in the table, whereas AWS, GCP, and Azure are not supported. See also Secure Boot support.

| Operating System | Secure Boot public key |
|---|---|
| CentOS 7 (64-bit) | DS12.der |
| Red Hat Enterprise Linux 7 (64-bit) | DS12.der |

Note that the information about the required DSA build is not applicable.

## Deep Security Agent 11 LTS

The following table lists Linux operating systems on which DSA 11 LTS provides support for Secure Boot.

VMware and physical machines are supported on all operating systems included in the table, whereas AWS, GCP, and Azure are not supported. See also Secure Boot support.

| Operating System | Secure Boot public key |
|---|---|
| CentOS 7 (64-bit) | DS11_2022.der |
| Red Hat Enterprise Linux 7 (64-bit) | DS11_2022.der |

Note that the information about the required DSA build is not applicable.

---

**Footnotes:**

[1] For details, see Trusted Launch for Azure virtual machines - Operating systems supported

[2] DS20.der expired on November 26, 2024. It has been replaced with DS2022.der.

3
Support for Red Hat Compatible Kernel (RHCK) only. There is no support for Unbreakable Enterprise Kernel (UEK).

## SELinux support

Security-Enhanced Linux (SELinux) enforcing mode is supported on specific OS and agent combinations, using the default SELinux policies.

✓ – Supported. If support was added in an update, then the minimum required version is indicated in the footnote.

• – Support for these releases is ending soon. Upgrade as soon as possible.

| Operating System | Agent Version | | |
|---|---|---|---|
| | 20 LTS | 12 FR | 12 LTS |
| AlmaLinux 8 (64-bit) | ✓ | | |
| AlmaLinux 9 (64-bit) | ✓ | | |
| Amazon Linux (64-bit) | ✓ | | |
| Amazon Linux 2 (64-bit) | ✓ | | |
| Amazon Linux 2 (AWS Arm-based Graviton2) | ✓ | | |
| Amazon Linux 2 (AWS Arm-based Graviton3) | ✓ | | |
| Amazon Linux 2023 (64-bit) | ✓ | | |
| Amazon Linux 2023 (AWS Arm-based Graviton2) | ✓ | | |
| CentOS 6 (64-bit) | ✓ | | |
| CentOS 7 (64-bit) | ✓ | | |
| CentOS 8 (64-bit) | ✓ | | |
| CloudLinux 8 (64-bit) | ✓ | | |

| Operating System | Agent Version | | |
|---|---|---|---|
| | 20 LTS | 12 FR | 12 LTS |
| Miracle Linux 8 (64-bit) | ✓ | | |
| Miracle Linux 9 (64-bit) | ✓ | | |
| Oracle Linux 6 (32-bit) | ✓ | | |
| Oracle Linux 6 (64-bit) | ✓ | | |
| Oracle Linux 7 (64-bit) | ✓ | | |
| Oracle Linux 8 (64-bit) | ✓ | | |
| Oracle Linux 9 (64-bit) | ✓ | | |
| Oracle Linux 10 (64-bit) | ✓ | | |
| Red Hat Enterprise Linux 6 (32-bit and 64-bit) | ✓ | | |
| Red Hat Enterprise Linux 7 (64-bit) | ✓ | ✓ 1 | ✓ 2 |
| Red Hat Enterprise Linux Workstation 7 (64-bit) | ✓ | | |
| Red Hat Enterprise Linux 8 (64-bit) | ✓ | ✓ 1 | ✓ 2 |
| Red Hat Enterprise Linux 8 (AWS Arm-based Graviton2) | ✓ | | |
| Red Hat Enterprise Linux 8.6 (PowerPC little-endian) | ✓ | | |
| Red Hat Enterprise Linux 9 (64-bit) | ✓ | | |
| Red Hat Enterprise Linux 9 (PowerPC little-endian) | ✓ | | |
| Red Hat Enterprise Linux 9 (64-bit Arm (aarch64)) | ✓ | | |
| Red Hat Enterprise Linux 10 (64-bit) | ✓ | | |
| Rocky Linux 8 (64-bit) | ✓ | | |

| Operating System | Agent Version | | |
|---|---|---|---|
| | 20 LTS | 12 FR | 12 LTS |
| Rocky Linux 9 (64-bit) | ✓ | | |
| Rocky Linux 10 (64-bit) | ✓ | | |
| SUSE Linux Enterprise Server 15 (64-bit) | ✓ | | |
| SUSE Linux Enterprise Server 15 SP5 (AWS Arm-based Graviton2) | ✓ | | |

Note that anti-malware software such as the agent must run in an unconfined domain in order to protect the whole computer. Any additional SELinux policy customization or configuration could block the agent. If any alerts occur, see Troubleshoot SELinux alerts.

**Footnotes:**

[1] Requires Deep Security Agent 12.5.0-936 FR (2020-05-19) or later.

[2] Requires Deep Security Agent 12.0.0-1026 U9 (2020-05-04) or later.

# Supported features by platform

The following tables list security features available in Deep Security Agent 20 for each operating system.

> **Note:**
> Earlier versions of agents are compatible with other operating systems. These agents do not support new features. For details, see "Agent platform compatibility" on page 389.
>
> To access information about features in earlier agent versions:

## AIX

For a list of supported AIX versions, see "Agent platform compatibility" on page 389.

| | Anti-Malware | | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommendation Scan | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | | | On-demand | | | | | | Real-time | | | On-demand | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring | Predictive Machine Learning | Feature Set 1 [1] | | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | FileScans | Directory Scans | Scans of Running Processes, Listening Ports | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports | | | | | | |
| AIX 6.1 | | | | | ✓ [7] | | ✓ | ✓ | ✓ | | | | ✓ | ✓ | | ✓ | ✓ | | ✓ | | | |

| | Anti-Malware | | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommendation Scan | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | | | On-demand | | | | | | Real-time | | | On-demand | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring | Predictive Machine Learning | Feature Set 1 [1] | | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | FileScans | Directory Scans | Scans of Running Processes, Listening Ports | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports | | | | | | |
| TL 9 or later | | | | | | | | | | | | | | | | | | | | | | |
| AIX 7.1 TL 3 or later | | | | | ✓ [6] | | ✓ | ✓ | ✓ | | | | ✓ | ✓ | | ✓ | ✓ | | ✓ | | | |
| AIX 7.2 TL 0 or later | | | | | ✓ [6] | | ✓ | ✓ | ✓ | | | | ✓ | ✓ | | ✓ | ✓ | | ✓ | | | |
| AIX 7.3 TL 0 or | | | | | ✓ [13] | | ✓ | ✓ | ✓ | | | | ✓ | ✓ | | ✓ | ✓ | | ✓ | | | |

Trend Micro Deep Security for Azure Marketplace 20

| | Anti-Malware | | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommen-dation Scan | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | | | On-demand | | | | | | Real-time | | | On-demand | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring | Predictive Machine Learning | Feature Set 1 [1] | | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | FileScans | Directory Scans | Scans of Running Processes, Listening Ports | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports | | | | | | |
| later | | | | | | | | | | | | | | | | | | | | | | |

## AlmaLinux

| | Anti-Malware | | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommen-dation Scan | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | | | On-demand | | | | | | Real-time | | | On-demand | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring | Predictive Machine Learning | Feature Set 1 [1] | | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection [11] | File Scans [5] | Directory Scans | Scans of Running Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports | | | | | | |
| AlmaLinux 8 (64-bit) [10] | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | | ✓ | |
| AlmaLinux 8 (64-bit) [10] | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | | ✓ | |
| AlmaLinux 9 (64-bit) [18] | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | | ✓ | |

## Amazon Linux

Real-time Anti-Malware requires a compatible file system. See "Linux file system compatibility" on page 411.

| | Anti-Malware | | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommen-dation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | | | On-demand | | | | | | Real-time | | | On-demand | | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring | Predictive Machine Learning [8] | Feature Set 1 [1] | | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans | Directory Scans | Scans of Running Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports | | | | | | | |
| Amazon Linux (64-bit) | ✓ | | ✓ [6] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ [5] | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | |
| Amazon Linux 2 (64-bit) | ✓ | | ✓ [6] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [11] | ✓ [5] | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ [9] |
| Amazon Linux 2 (AWS Arm-based Graviton 2) [6] and Amazon Linux 2 (AWS | ✓ [7] | | ✓ [7] | ✓ | ✓ [7] | ✓ [6] | ✓ [6] | ✓ [6] | ✓ [6] | | ✓ [8] | | ✓ [8] | ✓ [8] | | ✓ [8] | ✓ [7] | ✓ [8] | ✓ [7] | ✓ [8] | | ✓ [8] | |

| | Anti-Malware | | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommen-dation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | | | On-demand | | | | | | Real-time | | | On-demand | | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring | Predictive Machine Learning [8] | Feature Set 1 [1] | | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans | Directory Scans | Scans of Running Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports | | | | | | | |
| ARM-Based Graviton 3) [12] | | | | | | | | | | | | | | | | | | | | | | | |
| Amazon Linux 2023 (64-bit)[20] | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [5] | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ |
| Amazon Linux 2023 (AWS Arm-based Graviton 2) [20] | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | |

## CentOS Linux

Real-time Anti-Malware requires a compatible file system. See "Linux file system compatibility" on page 411.

| | Anti-Malware | | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommendation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | | | On-demand | | | | | | Real-time | | | On-demand | | | | | | | | | |
| | Feature Set 1[1] | Process memory scan, Registry scan | Behavior monitoring[6] | Predictive Machine Learning[8] | Feature Set 1[1] | | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans | Directory Scans | Scans of Running Processes, Listening Ports[37] | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports | | | | | | | |
| CentOS 6 (32-bit) | ✓ | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | | | | ✓ | ✓ | | ✓ | ✓ | | ✓ | | | ✓ | |
| CentOS 6 (64-bit) | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓[5] | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | |
| CentOS 7 (64-bit) | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓[11] | ✓[5] | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ |
| CentOS | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓[11] | ✓[5] | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | |

|  | Anti-Malware |  |  |  |  | Web Reputation Service | Firewall | Intrusion Prevention System |  |  | Integrity Monitoring |  |  |  |  |  | Log Inspection | Application Control | Recommendation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
|  | Real-time |  |  |  | On-demand |  |  |  |  |  | Real-time |  |  | On-demand |  |  |  |  |  |  |  |  |  |
|  | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring [6] | Predictive Machine Learning [8] | Feature Set 1 [1] |  |  | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans | Directory Scans | Scans of Running Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports |  |  |  |  |  |  |  |
| 8 (64-bit) |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

## CloudLinux

Real-time Anti-Malware requires a compatible file system. See "Linux file system compatibility" on page 411.

| | Anti-Malware | | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommen-dation Scan | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | | | On-demand | | | | | | Real-time | | | On-demand | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring [6] | Predictive Machine Learning [8] | Feature Set 1 [1] | | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection [11] | File Scans [5] | Directory Scans | Scans of Running Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports | | | | | | |
| CloudLinux 7 (64-bit) | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | | ✓ | |
| CloudLinux 8 (64-bit) | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | | ✓ | |

## Debian Linux

Real-time Anti-Malware requires a compatible file system. See "Linux file system compatibility" on page 411.

| | Anti-Malware | | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommen-dation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | | | On-demand | | | | | | Real-time | | | On-demand | | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring [6] | Predictive Machine Learning [8] | Feature Set 1 [1] | | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans [5] | Directory Scans | Scans of Running Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports | | | | | | | |
| Debian Linux 8 (64-bit) | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | |
| Debian Linux 9 (64-bit) | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [11] | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | |
| Debian Linux 10 (64-bit) | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [11] | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ |
| Debian Linux 11 (64-bit) | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ |
| Debian Linux | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | |

| | Anti-Malware | | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommen-dation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | | | On-demand | | | | | | Real-time | | | On-demand | | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring [6] | Predictive Machine Learning [8] | Feature Set 1 [1] | | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans [5] | Directory Scans | Scans of Running Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports | | | | | | | |
| 12 (64-bit) [24] | | | | | | | | | | | | | | | | | | | | | | | |
| Debian Linux 13 (64-bit) [41] | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ |

## Miracle Linux

Real-time Anti-Malware requires a compatible file system. See "Linux file system compatibility" on page 411.

| | Anti-Malware | | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommendation Scan | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | | | On-demand | | | | | | Real-time | | | On-demand | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring [6] | Predictive Machine Learning [8] | Feature Set 1 [1] | | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection [11] | File Scans [5] | Directory Scans | Scans of Running Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports | | | | | | |
| Miracle Linux 8 (64-bit) [23] | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ |
| Miracle Linux 9 (64 bit) [25] | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ |

## Oracle Linux

Real-time Anti-Malware requires a compatible file system. See "Linux file system compatibility" on page 411.

| | Anti-Malware | | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommendation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | | | On-demand | | | | | | Real-time | | | On-demand | | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring | Predictive Machine Learning | Feature Set 1 [1] | | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans | Directory Scans | Scans of Running Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports | | | | | | | |
| Oracle Linux 6 (32-bit) | | | | | ✓ | | ✓ | ✓ | ✓ | | | | ✓ | ✓ | | ✓ | ✓ | | ✓ | | | | |
| Oracle Linux 6 (64-bit) | ✓ | | ✓ [6] | ✓ [8] | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ [5] | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | |
| Oracle Linux 7 (64-bit) | ✓ | | ✓ [6] | ✓ [8] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [11] | ✓ [5] | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [14] | ✓ | |
| Oracle Linux 8 (64-bit) | ✓ | | ✓ [6] | ✓ [8] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [11] | ✓ [5] | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ [15] |
| Oracle Linux 9 (64-bit) | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [20] | ✓ [5] | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ |

| | Anti-Malware | | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommendation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | | | On-demand | | | | | | Real-time | | | On-demand | | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring | Predictive Machine Learning | Feature Set 1 [1] | | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans | Directory Scans | Scans of Running Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports | | | | | | | |
| Oracle Linux 10 (64-bit) | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [20] | ✓ [5] | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ [40] |

**Note:** Inspecting TLS traffic when Oracle Linux 8 is in FIPS mode requires using Advanced TLS traffic inspection to support the ciphers applied by its predefined cryptographic policy.

## Red Hat Enterprise Linux

Real-time Anti-Malware requires a compatible file system. See "Linux file system compatibility" on page 411.

| | Anti-Malware | | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommen-dation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | | | On-demand | | | | | | Real-time | | | On-demand | | | | | | | | | |
| | Feature Set 1[1] | Process memory scan, Registry scan | Behavior monitoring[6] | Predictive Machine Learning[8] | Feature Set 1[1] | | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans | Directory Scans | Scans of Running Processes, Listening Ports[37] | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports | | | | | | | |
| Red Hat Enterprise Linux 6 (32-bit) | ✓ | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | | | | ✓ | ✓ | | ✓ | ✓ | | ✓ | | | ✓ | |
| Red Hat Enterprise Linux 6 (64-bit) | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ [5] | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | |
| Red Hat Enterprise Linux 7 (64-bit) | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [11] | ✓ [5] | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Red Hat Enterprise Linux Workstati | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [5] | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | |

| | Anti-Malware | | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommendation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | | | On-demand | | | | | | Real-time | | | On-demand | | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring [6] | Predictive Machine Learning [8] | Feature Set 1 [1] | | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans | Directory Scans | Scans of Running Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports | | | | | | | |
| on 7 (64-bit) [18] | | | | | | | | | | | | | | | | | | | | | | | |
| Red Hat Enterprise Linux 8 (64-bit) | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [11] | ✓ [5] | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [9] |
| Red Hat Enterprise Linux 8 (AWS Arm-based Graviton2) | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ [5] | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | |
| Red Hat Enterprise | | | | | ✓ [41] | | | | | | | | | | | | | | | | | | |

| | Anti-Malware | | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommen-dation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | | | On-demand | | | | | | Real-time | | | On-demand | | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring [6] | Predictive Machine Learning [8] | Feature Set 1 [1] | | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans | Directory Scans | Scans of Running Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports | | | | | | | |
| Linux 8 (64-bit IBM Z (s390x)) | | | | | | | | | | | | | | | | | | | | | | | |
| Red Hat Enterprise Linux 8.6 (PowerPC little-endian) [28] | ✓ | | ✓ | ✓ | ✓ [22] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| Red Hat Enterprise Linux 9 (PowerPC little-endian) | ✓ [33] | | ✓ [33] | ✓ [33] | ✓ [33] | ✓ [33] | ✓ [33] | ✓ [33] | ✓ [33] | ✓ [35] | ✓ [35] | | ✓ [35] | ✓ [35] | ✓ [35] | ✓ [35] | ✓ [35] | ✓ [35] | ✓ [33] | ✓ [35] | ✓ [33] | | |

| | Anti-Malware | | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommen-dation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | | | On-demand | | | | | | Real-time | | | On-demand | | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring [6] | Predictive Machine Learning [8] | Feature Set 1 [1] | | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans | Directory Scans | Scans of Running Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports | | | | | | | |
| Red Hat Enterprise Linux 9 (64-bit) | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [20] | ✓ [5] | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [26] | ✓ | ✓ |
| Red Hat Enterprise Linux 9 (64-bit Arm (aarch64)) | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ [5] | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | |
| Red Hat Enterprise Linux 9 (64-bit IBM Z (s390x)) | | | | | ✓ [41] | | | | | | | | | | | | | | | | | | |

| | Anti-Malware | | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommen-dation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | | | On-demand | | | | | | Real-time | | | On-demand | | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring [6] | Predictive Machine Learning [8] | Feature Set 1 [1] | | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans | Directory Scans | Scans of Running Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports | | | | | | | |
| Red Hat Enterprise Linux 10 (64-bit) [39] | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [20] | ✓ [5] | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ |

## Red Hat OpenShift

Real-time Anti-Malware requires a compatible file system. See "Linux file system compatibility" on page 411.

| | Anti-Malware | | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommendation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | | | On-demand | | | | | | Real-time | | | On-demand | | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring [6] | Predictive Machine Learning [8] | Feature Set 1 [1] | | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans | Directory Scans | Scans of Running Processes, Listening Ports | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports | | | | | | | |
| OpenShift supported versions [31] | ✓ | | ✓ | ✓ | | | | | | | | | | | | | | | | | | | |

## Rocky Linux

Real-time Anti-Malware requires a compatible file system. See "Linux file system compatibility" on page 411.

| | Anti-Malware | | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommendation Scan | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | | | On-demand | | | | | | Real-time | | | On-demand | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring | Predictive Machine Learning | Feature Set 1 [1] | | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection [11] | File Scans [5] | Directory Scans | Scans of Running Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports | | | | | | |
| Rocky Linux 8 (64-bit) [10] | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | | ✓ | |
| Rocky Linux 9 (64-bit) [17] | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ |
| Rocky Linux 10 (64-bit) [41] | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ |

## Solaris

For a list of supported Solaris versions, see "Agent platform compatibility" on page 389. For more information, see "How does agent protection work for Solaris zones?" on page 1688

| | Anti-Malware | | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommen-dation Scan | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | | | On-demand [4] | | | | | | Real-time | | | On-demand | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring | Predictive Machine Learning | Feature Set 1 [1] | | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans | Directory Scans | Scans of Running Processes, Listening Ports | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports | | | | | | |
| Solaris | | | | | ✓ | ✓ | ✓ | ✓ | ✓ | | | | ✓ | ✓ | | ✓ | ✓ | | ✓ | | | |

## SUSE Linux

Real-time Anti-Malware requires a compatible file system. See "Linux file system compatibility" on page 411.

| | Anti-Malware | | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommen-dation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | | | On-demand | | | | | | Real-time | | | On-demand | | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring [6] | Predictive Machine Learning [8] | Feature Set 1 [1] | | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection [11] | File Scans [5] | Directory Scans | Scans of Running Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports | | | | | | | |
| SUSE Linux Enterprise Server 12 SP1 and later (64-bit) [27] | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [14] |
| SUSE Linux Enterprise Server 12 SP5 and later (PowerPC little-endian) | ✓ [27] | | ✓ [27] | ✓ [27] | ✓ [27] | ✓ [27] | ✓ [27] | ✓ [27] | ✓ [27] | ✓ [27] | ✓ [28] | | ✓ [28] | ✓ [28] | | ✓ [28] | ✓ [27] | ✓ [28] | ✓ [27] | ✓ [27] | ✓ [27] | | |

| | Anti-Malware | | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommendation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | | | On-demand | | | | | | Real-time | | | On-demand | | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring [6] | Predictive Machine Learning [8] | Feature Set 1 [1] | | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection [11] | File Scans [5] | Directory Scans | Scans of Running Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports | | | | | | | |
| SUSE Linux Enterprise Server 15 SP1 and later (64-bit) | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [14] |
| SUSE Linux Enterprise Server 15 SP2 and later (PowerPC little-endian) | ✓ [27] | | ✓ [27] | ✓ [27] | ✓ [27] | ✓ [27] | ✓ [27] | ✓ [27] | ✓ [27] | ✓ [27] | ✓ [28] | | ✓ [28] | ✓ [28] | | ✓ [28] | ✓ [27] | ✓ [28] | ✓ [27] | ✓ [27] | ✓ [27] | | |
| SUSE | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | | |

| | Anti-Malware | | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommen-dation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | | | On-demand | | | | | | Real-time | | | On-demand | | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring [6] | Predictive Machine Learning [8] | Feature Set 1 [1] | | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection [11] | File Scans [5] | Directory Scans | Scans of Running Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports | | | | | | | |
| Linux Enterprise Server 15 SP5 and later (AWS Arm-based Graviton 2) [29] [32] | | | | | | | | | | | | | | | | | | | | | | | |

In general, feature support for SUSE Linux is aligned and compatible with every minor version (SP). Any incompatibility is noted.

## Ubuntu Linux

Real-time Anti-Malware requires a compatible file system. See "Linux file system compatibility" on page 411.

| | Anti-Malware | | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommen-dation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | | | On-demand | | | | | | Real-time | | | On-demand | | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring | Predictive Machine Learning | Feature Set 1 [1] | | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans [5] | Directory Scans | Scans of Running Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports | | | | | | | |
| Ubuntu 16.04 (64-bit) | ✓ | | ✓ [6] | ✓ [8] | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | |
| Ubuntu 18.04 (64-bit) | ✓ | | ✓ [6] | ✓ [8] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [11] | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ |
| Ubuntu 18.04 (AWS Arm-based Graviton 2) [10] | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | |
| Ubuntu 20.04 (64-bit) | ✓ | | ✓ [6] | ✓ [8] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [11] | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ |

| | Anti-Malware | | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommendation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | | | On-demand | | | | | | Real-time | | | On-demand | | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring | Predictive Machine Learning | Feature Set 1 [1] | | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans [5] | Directory Scans | Scans of Running Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports | | | | | | | |
| Ubuntu 20.04 (AWS Arm-based Graviton 2) [10] | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | |
| Ubuntu 22.04 (64-bit) | ✓ | | ✓ [6] | ✓ [8] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [20] | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ |
| Ubuntu 22.04 (AWS Arm-based Graviton 2) [13] | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | | |

Trend Micro Deep Security for Azure Marketplace 20

| | Anti-Malware | | | | | Web Reputation Service | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommendation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time | | | | On-demand | | | | | | Real-time | | | On-demand | | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring | Predictive Machine Learning | Feature Set 1 [1] | | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans [5] | Directory Scans | Scans of Running Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Processes, Listening Ports | | | | | | | |
| Ubuntu 24.04 (64-bit) [32] | ✓ | | ✓ [6] | ✓ [8] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [20] | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | | | | |
| Ubuntu 24.04 (AWS Arm-based Graviton 2) [42] | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | | |

## Microsoft Windows

For details on supported Windows 10 update releases, see Deep Security Support for Windows 10 and Deep Security Support for Windows Server Core.

For details on supported Windows 11 update releases, see Trend Cloud One - Endpoint & Workload Security and Deep Security Support for Windows 11.

For Windows 2012 and later, both Desktop Experience and Server Core installations are supported (any exceptions are mentioned in the table). For Windows Server 2008 and 2008 R2, only Full Installations are supported.

| | Anti-Malware | | | | | Web Reputation Service | | | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommendation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode | Device Control |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time scan | | | | On-demand scan | | Browser Extension | | | | | | Real-time | | | On-demand | | | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring | Predictive Machine Learning | Feature Set 1 [1] | | Chrome | Edge | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans | Directory Scans | Scans of Running Services, Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Services, Processes, Listening Ports | | | | | | | | |
| Windows 7 (32-bit) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [34] | ✓ | | | ✓ | | ✓ [8] |
| Windows 7 (64-bit) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [34] | ✓ | ✓ | | ✓ | | ✓ [8] |
| Windows 7 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ | | | | | ✓ | ✓ | ✓ | ✓ | | ✓ | | | | | ✓ [8] |

| | Anti-Malware | | | | | Web Reputation Service | | | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommendation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode | Device Control |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time scan | | | | On-demand scan | | Browser Extension | | | | | | Real-time | | | On-demand | | | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring | Predictive Machine Learning | Feature Set 1 [1] | | Chrome | Edge | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans | Directory Scans | Scans of Running Services, Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Services, Processes, Listening Ports | | | | | | | | |
| Embedded (32-bit) [2] | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Windows 8 (32-bit) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [34] | ✓ | | | ✓ | | ✓ [8] |
| Windows 8 (64-bit) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [34] | ✓ | ✓ | | ✓ | | ✓ [8] |
| Window | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [34] | ✓ | | | ✓ | | ✓ [8] |

| | Anti-Malware | | | | | Web Reputation Service | | | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommendation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode | Device Control |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time scan | | | | On-demand scan | | Browser Extension | | | | | | Real-time | | | On-demand | | | | | | | | | | |
| | Feature Set 1[1] | Process memory scan, Registry scan | Behavior monitoring | Predictive Machine Learning | Feature Set 1[1] | | Chrome | Edge | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans | Directory Scans | Scans of Running Services, Processes, Listening Ports[37] | File and Directory Scans | Registry Scans | Scans of Running Services, Processes, Listening Ports | | | | | | | | |
| s 8.1 (32-bit) | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Windows 8.1 (64-bit) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [34] | ✓ | ✓ | | ✓ | | ✓ [8] |
| Windows 8.1 Embedded (32-bit) [2] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ | | | | | ✓ | ✓ | ✓ | ✓ | | ✓ | | | ✓ | | ✓ [8] |

| | Anti-Malware | | | | | Web Reputation Service | | | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommendation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode | Device Control |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time scan | | | | On-demand scan | | Browser Extension | | | | | | Real-time | | | On-demand | | | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring | Predictive Machine Learning | Feature Set 1 [1] | | Chrome | Edge | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans | Directory Scans | Scans of Running Services, Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Services, Processes, Listening Ports | | | | | | | | |
| Windows 10 (32-bit) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [34] | ✓ | | | ✓ | | ✓ [8] |
| Windows 10 (64-bit) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [17] | ✓ [22] | ✓ | ✓ | ✓ | ✓ [16] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [34] | ✓ | ✓ | | ✓ | | ✓ [8] |
| Windows 10 IoT Enterprise 2019 LTSC (32- and | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | | ✓ [8] |

| | Anti-Malware | | | | | Web Reputation Service | | | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommendation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode | Device Control |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time scan | | | | On-demand scan | | Browser Extension | | | | | | Real-time | | | On-demand | | | | | | | | | | |
| | Feature Set 1[1] | Process memory scan, Registry scan | Behavior monitoring | Predictive Machine Learning | Feature Set 1[1] | | Chrome | Edge | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans | Directory Scans | Scans of Running Services, Processes, Listening Ports[37] | File and Directory Scans | Registry Scans | Scans of Running Services, Processes, Listening Ports | | | | | | | | |
| 64-bit)[2] | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Windows 10 IoT Enterprise 2021 LTSC (64-bit)[2] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | | ✓[8] |
| Windows 10 Enterprise multi- | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓[34] | ✓ | ✓ | | ✓ | | ✓[8] |

| | Anti-Malware | | | | | Web Reputation Service | | | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommendation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode | Device Control |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time scan | | | | On-demand scan | | Browser Extension | | | | | | Real-time | | | On-demand | | | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring | Predictive Machine Learning | Feature Set 1 [1] | | Chrome | Edge | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans | Directory Scans | Scans of Running Services, Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Services, Processes, Listening Ports | | | | | | | | |
| session (64-bit) | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Windows 11 (64-bit) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [17] | ✓ [22] | ✓ | ✓ | ✓ | ✓ [16] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [34] | ✓ | ✓ | | ✓ | | ✓ [8], [19] |
| Windows Server 2008 (32-bit) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | | | | | ✓ [17] |
| Windows Server | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | | ✓ [17] |

| | Anti-Malware | | | | | Web Reputation Service | | | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommendation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode | Device Control |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time scan | | | | On-demand scan | | Browser Extension | | | | | | Real-time | | | On-demand | | | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring | Predictive Machine Learning | Feature Set 1 [1] | | Chrome | Edge | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans | Directory Scans | Scans of Running Services, Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Services, Processes, Listening Ports | | | | | | | | |
| 2008 (64-bit) | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Windows Server 2008 R2 (64-bit) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ | | ✓ 5 | ✓ 5 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ 17 |
| Windows Server 2012 (64-bit) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ | | ✓ 3, 5 | ✓ 3, 5 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ 3 | ✓ | ✓ | | ✓ | ✓ | ✓ 17 |
| Window | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ | ✓ 11 | ✓ | ✓ 5 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ 3 | ✓ | ✓ | ✓ |

| | Anti-Malware | | | | | Web Reputation Service | | | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommendation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode | Device Control |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time scan | | | | On-demand scan | | Browser Extension | | | | | | Real-time | | | On-demand | | | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring | Predictive Machine Learning | Feature Set 1 [1] | | Chrome | Edge | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans | Directory Scans | Scans of Running Services, Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Services, Processes, Listening Ports | | | | | | | | |
| s Server 2012 R2 (64-bit) | | | | | | | | | | | | | 5 | | | | | | | | | | | | | 17 |
| Windows Server 2016 (LTSC, version 1607) (64-bit) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ 17 | ✓ 22 | ✓ | ✓ | ✓ | ✓ 11 | ✓ 5 | ✓ 5 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ 17 |
| Windows Server | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ | | ✓ 5 | ✓ 5 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | |

| | Anti-Malware | | | | | Web Reputation Service | | | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommen-dation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode | Device Control |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time scan | | | | On-demand scan | | Browser Extension | | | | | | Real-time | | | On-demand | | | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring | Predictive Machine Learning | Feature Set 1 [1] | | Chrome | Edge | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans | Directory Scans | Scans of Running Services, Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Services, Processes, Listening Ports | | | | | | | | |
| Core (SAC, version 1709) (64-bit) | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Windows Server 2019 (LTSC, version 1809) (64-bit) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [17] | ✓ [22] | ✓ | ✓ | ✓ | ✓ [11] | ✓ [5] | ✓ [5] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [17] |

| | Anti-Malware | | | | | Web Reputation Service | | | Firewall | Intrusion Prevention System | | | Integrity Monitoring | | | | | | Log Inspection | Application Control | Recommendation Scan | Relay | Scanner | Vision One (XDR) | FIPS mode | Device Control |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Real-time scan | | | | On-demand scan | | Browser Extension | | | | | | Real-time | | | On-demand | | | | | | | | | | |
| | Feature Set 1 [1] | Process memory scan, Registry scan | Behavior monitoring | Predictive Machine Learning | Feature Set 1 [1] | | Chrome | Edge | | Unencrypted Traffic | SSL Encrypted Traffic | Advanced TLS Traffic Inspection | File Scans | Directory Scans | Scans of Running Services, Processes, Listening Ports [37] | File and Directory Scans | Registry Scans | Scans of Running Services, Processes, Listening Ports | | | | | | | | |
| Windows Server 2022 (LTSC, version 21H2) (64-bit) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [21] | ✓ [22] | ✓ | ✓ | ✓ | ✓ [27] | ✓ [5] | ✓ [5] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ [17] |
| Windows Server 2025 (LTSC, version 24H2) (64-bit) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ [38] | ✓ [38] | ✓ | ✓ | ✓ | ✓ [27] | ✓ [5] | ✓ [5] | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ [36] | ✓ [17] |

**Note:** FIPS mode for Windows Desktop platforms might work, but is not officially supported.

---

**Footnotes:**

1

**Feature Set 1** includes signature-based file scanning, spyware scanning, and document exploit protection.

2

Because embedded operating systems typically run on custom hardware (for example, on point-of-sale terminals), you should thoroughly test your hardware platform before deployment in a production environment. Trend Micro tests Windows Embedded platforms in a virtualized environment. If you need to create a service ticket for Trend Micro Support, try to reproduce the problem in a virtualized environment. If the issue cannot be reproduced in a virtualized environment, and is specific to your custom hardware, Trend Micro Support might require you to provide remote access to it for diagnostics.

Note that Windows 10 IoT was formerly named Windows 10 Embedded, and is therefore considered a Windows Embedded platform.

3

Requires a Full or Desktop Experience installation. Server Core is not supported.

4

Anti-Malware on-demand scans are supported on all Solaris file systems.

5

Supports enhanced real-time integrity monitoring, which uses the application control driver to get information about who changed a monitored file.

6

Requires Deep Security Agent 20.0.0-1822 (20 LTS Update 2021-01-18) or later.

[7] Requires Deep Security Agent 20.0.0-2204 (20 LTS Update 2021-04-12) or later.

[8] Requires Deep Security Agent 20.0.0-4959 (20 LTS Update 2022-07-04) or later.

[9] Requires Deep Security Agent 20.0.0-2921 (20 LTS Update 2021-08-30) or later.

[10] Requires Deep Security Agent 20.0.0-3288 (20 LTS Update 2021-10-28) or later.

[11] Requires Deep Security Agent 20.0.0-4185 (20 LTS Update 2022-04-06) or later.

[12] Requires Deep Security Agent 20.0.0-5137 (20 LTS Update 2022-07-26) or later.

[13] Requires Deep Security Agent 20.0.0-5394 (20 LTS Update 2022-08-29) or later.

[14] Requires Deep Security Agent 20.0.0-5761 (20 LTS Update 2022-10-21) or later.

[15] Requires Deep Security Agent 20.0.0-5953 (20 LTS Update 2022-11-22) or later.

[16] Requires Deep Security Agent 20.0.0-5995 (20 LTS Update 2022-11-28) or later.

Trend Micro Deep Security for Azure Marketplace 20

[17] Requires Deep Security Agent 20.0.0-6313 (20 LTS Update 2023-01-31) or later.

[18] Requires Deep Security Agent 20.0.0-6912 (20 LTS Update 2023-05-02) or later.

[19] For Windows 11 systems, the Mobile (MTP/PTP) read-only protocol for Device Control requires Deep Security Agent 20.0.0-5810 (20 LTS Update 2022-10-27) or later.

[20] Requires Deep Security Agent 20.0.0-7303 (20 LTS Update 2023-06-28) or later.

[21] Requires Deep Security Agent 20.0.0-7719 (20 LTS Update 2023-08-29) or later.

[22] Requires Deep Security Agent 20.0.0-7943 (20 LTS Update 2023-09-26) or later.

[23] Miracle Linux 8 is supported by Deep Security Agent 20.0.0-7719 (20 LTS Update 2023-08-29) or later for Red Hat Enterprise Linux 8.

[24] Requires Deep Security Agent 20.0.0-8438 (20 LTS Update 2023-12-12) or later.

[25] Miracle Linux 9 is supported by Deep Security Agent 20.0.0-8137 (20 LTS Update 2023-10-26) or later for Red Hat Enterprise Linux 9.

[26] Requires Deep Security Agent 20.0.1-4540 (20 LTS Update 2024-03-20) or later.

Trend Micro Deep Security for Azure Marketplace 20

**27**

Requires Deep Security Agent 20.0.1-7380 (20 LTS Update 2024-04-24) or later.

**28**

Requires Deep Security Agent 20.0.1-12510 (20 LTS Update 2024-06-26) or later.

**29**

Requires Deep Security Agent 20.0.1-14610 (20 LTS Update 2024-07-20) or later.

**30**

Requires Deep Security Agent 20.0.0-8268 (20 LTS Update 2023-11-21) or later.

**31**

See Deep Security Agent version for Red Hat OpenShift

**32**

Requires Deep Security Agent 20.0.1-19250 (20 LTS Update 2024-09-18) or later.

**33**

Requires Deep Security Agent 20.0.1-21510 (20 LTS Update 2024-10-16) or later.

**34**

Requires Deep Security Agent 20.0.0-5512 (20 LTS Update 2022-09-22) or later.

**35**

Requires Deep Security Agent 20.0.1-23340 (20 LTS Update 2024-11-13) or later.

**36**

Requires Deep Security Agent 20.0.2-1390 (20 LTS Update 2025-01-15) or later.

37

There are two types of real-time support in Integrity Monitoring:

- True real-time, when a real-time event is triggered by the driver event detection.

- Pseudo real-time (caused by a lack of driver support), when a seemingly real-time event is triggered by a periodic execution of the scan thread, which consumes more CPU and memory. The user and process information is not reported.

38

Requires Deep Security Agent 20.0.2-7600 (20 LTS Update 2025-04-16) or later.

39

Requires Deep Security Agent 20.0.2-14431 (20 LTS Update 2025-07-09) or later.

40

Requires Deep Security Agent 20.0.2-20480 (20 LTS Update 2025-09-24) or later.

41

Requires Deep Security Agent 20.0.2-26670 (20 LTS Update 2025-11-20) or later.

42

Requires Deep Security Agent 20.0.2-29370 (20 LTS Update 2025-12-09) or later.

## Sizing

Sizing guidelines for Deep Security deployments vary by the scale of your network, hardware, and software. See also "Sizing for Azure Marketplace" on page 475.

# Deep Security Manager sizing

Sizing recommendations for Deep Security Manager depend on the number of agents it needs to manage.

For best performance, it is important to allocate enough Java Virtual Machine (JVM) memory to the Deep Security Manager process. See "Configure Deep Security Manager memory usage" on page 1559.

Recommendation scans are CPU-intensive for Deep Security Manager. Consider the performance impact when determining how often to run recommendation scans. See "Manage and run recommendation scans" on page 639.

Resource spikes may occur if a large number of virtual machines are rebooted simultaneously and agents re-establish their connection with Deep Security Manager at the same time.

## Multiple server nodes

For better availability and scalability, use a load balancer and install the same version of Deep Security Manager on tw0 servers (nodes) connected to the same database.

To avoid high load on database servers, do not connect more than two Deep Security Manager nodes to each database server.

Each manager node is capable of all tasks. No node is more important than any of the others. You can log in to any node; agents, appliances, and relays can connect with any node. If one node fails, other nodes can provide service without any loss of data.

# Database sizing

The required database CPU, memory, and disk space depend on the following:

- The number of protected computers.
- The number of events (logs) recorded per second. This is related to the specific security features that are enabled.

- The amount of time during which events are retained.
- The size of the database transaction log.

Minimum disk space = (2 x Deep Security data size) + transaction log

For example, if the size of your database and the transaction log is 40 GB, you must have 80 GB (40 x 2) of free disk space during database schema upgrades.

To free disk space, delete any unnecessary agent packages for unused platforms (see "Delete a software package from the Deep Security database" on page 526), transaction logs, and unnecessary event records.

Event retention is configurable. For security events, retention is configured in the policy, individual computer settings, or both. See "Policies, inheritance, and overrides" on page 634 and "Log and event storage best practices" on page 1050.

You can minimize disk usage due to events as follows:

- Store events remotely, not locally. If you need to keep events longer (such as for compliance), forward them to a SIEM or Syslog server and then use pruning to delete the local copy. See "Forward Deep Security events to a Syslog or SIEM server" on page 1067.

  Some Application Control and Integrity Monitoring operations (Rebuild Baseline, Scan for Integrity Changes, and Scan for Inventory Changes) retain all records locally, and are never pruned or forwarded.

- Patch the protected computer's software *before* you enable Intrusion Prevention. Recommendation scans assign more IPS rules to protect a vulnerable OS. More security events increase local or remote disk usage.
- Disable unnecessary security features that log frequently, such as stateful Firewall for TCP, UDP, and ICMP.

High-traffic computers that use Deep Security Firewall or Intrusion Prevention features might record more events per second, requiring a database with better performance. You might also need to adjust local event retention.

If you anticipate many Firewall events, consider disabling Out of Allowed Policy events. See "Firewall settings" on page 878.

### Database disk space estimates

The following table estimates database disk space with default event retention settings. If the total disk space for the enabled protection modules exceeds the value of `2 or more modules`, use the smaller estimate. For example, you could deploy 750 agents with Deep Security Anti-Malware, Intrusion Prevention System, and Integrity Monitoring. The total of the individual recommendations is 320 GB (20 GB + 100 GB + 200 GB), but the `2 or more modules` recommendation is 300 GB. Therefore, you would estimate 300 GB.

Database disk space also increases with the number of separate Deep Security Agent platforms. For example, if you have 30 agents (maximum 5 versions per agent platform), this increases the database size by approximately 5 GB.

## Deep Security Agent sizing and resource consumption

To ensure optimal performace, Deep Security Agents and relays need to have certain amount of CPU, RAM, and disk space allocated to them.

### Deep Security Agent and Relay sizing

For Deep Security Agent and relay requirements with regards to CPU, RAM, and disk space allocation, see Deep Security Agent requirements and Deep Security Relay requirements.

### Estimated Deep Security Agent resource consumption

The following tables show the estimated RAM consumption for deployments using common feature combinations.

## Windows Agent

| Modules enabled | | | | | | | RAM |
|---|---|---|---|---|---|---|---|
| Anti-Malware | Web Reputation Service | Application Control | Integrity Monitoring | Log Inspection | Firewall | Intrusion Prevention | |
| ✓ | | | | | | | 156 MB |
| | | | | | | ✓ | 148 MB |
| ✓ | ✓ | | | | | | 150 MB |
| ✓ | ✓ | | | | | ✓ | 308 MB |
| ✓ | | | ✓ | ✓ | | ✓ | 280 MB |
| ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | 390 MB |
| ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | 361 MB |

## Linux Agent

| Modules enabled | | | | | | | | RAM |
|---|---|---|---|---|---|---|---|---|
| Anti-Malware | Web Reputation Service | Activity Monitoring | Application Control | Integrity Monitoring | Log Inspection | Firewall | Intrusion Prevention | |
| ✓ | | | | | | | | 315 MB |
| | | | | | | ✓ | ✓ | 172 MB |

| Modules enabled | | | | | | | | RAM |
|---|---|---|---|---|---|---|---|---|
| Anti-Malware | Web Reputation Service | Activity Monitoring | Application Control | Integrity Monitoring | Log Inspection | Firewall | Intrusion Prevention | |
| ✓ | | | | | | | ✓ | 399 MB |
| ✓ | ✓ | ✓ | | | | | | 312 MB |
| ✓ | ✓ | ✓ | | | | | ✓ | 448 MB |
| ✓ | | | | ✓ | ✓ | | ✓ | 413 MB |
| ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | 492 MB |
| ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | 538 MB |

## CPU sizing for Anti-Malware Solution Platform service

Deep Security Agent triggers a security update automatically when the Anti-Malware Solution Platform (AMSP) service is ready, which occurs if at least one of the following modules is enabled:

- Anti-Malware
- Activity Monitoring
- Application Control
- Integrity Monitoring

Based on the testing of agents on Linux conducted by Trend Micro, the following can be concluded:

- The overall CPU usage by AMSP is around 10%. This includes the process creation, file operation, and network operation events.
- Different CPU consumption calculation methods may lead to greater CPU usage results, therefore it is recommended to take a per-core approach (CPU consumption divided by the number of cores).

The following table provides detailed test results of the Linux agents' AMSP CPU consumption and event handling capabilities for different VM combinations, all using common policies (such as AM, SENSOR, WRS).

| VM specifications | CPU usage by AMSP | Workload events per second |
|---|---|---|
| vCPU: 2<br>RAM: 4 GB | Overall: 23%<br>CPU usage per core: 12.5% | 3,523 events per second, consisting of the following:<br>• async process: 550 per second<br>• sync process: 280 per second<br>• async file: 1,295 per second<br>• sync file: 1,397 per second<br>• asyncNetwork: 1.2 per second |
| vCPU: 4<br>RAM: 8 GB | Overall: 43%<br>CPU usage per core: 10.75% | 4,651 events per second, consisting of the following:<br>• async process: 751 per second<br>• sync process: 377 per second<br>• async file: 1,705 per second<br>• sync file: 1,817 per second<br>• asyncNetwork: 0.9 per second |
| vCPU: 8 | Overall: 70% | 5,841 events per second, consisting of the following: |

| VM specifications | CPU usage by AMSP | Workload events per second |
|---|---|---|
| RAM: 16 GB | CPU usage per core: 8.75% | • async process: 970 per second<br>• sync process: 485 per second<br>• async file: 2,128 per second<br>• sync file: 2,257 per second<br>• asyncNetwork: 0.9 per second |
| vCPU: 16<br>RAM: 32 GB | Overall: 127%<br>CPU usage per core: 7.9% | 6,275 events per second, consisting of the following:<br>• async process: 1,011 per second<br>• sync process: 505 per second<br>• async file: 2,308 per second<br>• sync file: 2,450 per second<br>• asyncNetwork: 1 per second |
| vCPU: 32<br>RAM: 64 GB | Overall: 120%<br>CPU usage per core: 3.75% | 4,425 events per second, consisting of the following:<br>• async process: 749 per second<br>• sync process: 375 per second<br>• async file: 1,603 per second<br>• sync file: 1,697 per second<br>• asyncNetwork: 1 per second |
| vCPU: 64 | Overall: 96% | 4,346 events per second, consisting of the following: |

| VM specifications | CPU usage by AMSP | Workload events per second |
|---|---|---|
| RAM: 128 GB | CPU usage per core: 1.5% | • async process: 703 per second<br>• sync process: 352 per second<br>• async file: 1,600 per second<br>• sync file: 1,690 per second<br>• asyncNetwork: 1 per second |

## Sizing for Azure Marketplace

Sizing guidelines for Deep Security in Azure Marketplace depend on the type of environment and other factors such as network, hardware, and software.

The recommendations have been classified into **Small** (1-10 000), **Medium** (10 000-20 000) and **Large** (20 000+) deployments.

### Deep Security Manager

| Number of agents | Instance type | Number of Deep Security Manager nodes |
|---|---|---|
| 1 - 10 000 | Standard D2 v2 | 1 - 2 |
| 10 000 - 20 000 | Standard D3 v2 | 2 |
| 20 000 + | Standard D12 v2 | 3 |

## Database

The default Azure SQL database is Standard S3 with a storage size of 20 GB, but if you have more than 10 000 agents, to improve performance, we recommend that you change the database scale to Premium P1 with the following recommended sizes:

| Number of agents | Hard drive size |
|---|---|
| 1 - 10 000 | 10 - 20 GB |
| 10 000 - 20 000 | 20 - 30 GB |
| 20 000 + | 30 - 40 GB |

The table above helps determine the initial database size to set for the Deep Security Database. These estimates are based on these assumptions:

- Log inspection and web reputation service (WRS) are not enabled.
- Intrusion prevention (IPS) is enabled efficiently with very few false positive events.
- Anti-malware (AM) events are insignificant in terms of size and are not part of the calculation. Anti-malware only logs events occasionally, unless there is an outbreak occurring.
- Log retention period is 30 days.
- Firewall events are around 50 per day.

**Note:** You can also change the service tier and the pricing tier of a SQL database.

## Notes

1. Other factors, such as the modules in use, items such as the number of security updates held, the number of policies will affect database size. In general, centrally collected firewall and intrusion prevention event logs form the bulk of the database volume. Event retention (**Administration > System Settings > Storage**) is relevant

to maintain a reasonably sized database. Make sure to review these settings as this will help determine how much space is needed.

2. For environments in which a significant number of firewall events are anticipated, consider disabling "Out of allowed policy" events. This can be configured for each agent or applied to at the Base policy level. (Open the **Computer** or **Policy** details page and go to **Firewall > Advanced**).
3. Environments with large retention requirements should consider SIEM or Syslog server for log storage. When logs are stored in SIEM or Syslog, less storage is required in the Deep Security database (see "Forward Deep Security events to a Syslog or SIEM server" on page 1067).
4. Imported Deep Security software in the Deep Security Manager can affect database size. Always review the number of software versions you plan to keep in the database and remove unnecessary versions.

# Deep Security Manager performance features

## Performance profiles

Deep Security Manager uses an optimized concurrent job scheduler that considers the impacts of each job on CPU, database and agents or appliances. By default, new installations use the Higher Capacity performance profile optimized for a dedicated manager. If Deep Security Manager is installed on a system with other resource-intensive software, it might be preferable to use the Standard performance profile. To modify the performance profile, navigate to **Administration > Manager Nodes**, select a manager node, open **Properties**, and then use the menu to make changes.

The performance profile also controls the number of agent- or appliance-initiated connections that the manager accepts. The default of each of the performance profiles effectively balances the amount of accepted, delayed, and rejected heartbeats.

## Low disk space alerts

### Low disk space on the database

If Deep Security Manager receives a Disk Full error message from the database, it starts to write events to its own hard drive and sends an email message to all users informing them of the situation. This behavior is not configurable.

Once the disk space issue on the database has been resolved, the manager writes the locally stored data to the database.

### Low disk space on the manager

If the available disk space on the computer where Deep Security Manager is installed falls below 10%, the manager generates a Low Disk Space alert. This alert is part of the regular alert system and is configurable. For more information, see "Configure alerts" on page 1180.

When the manager's available disk space falls below 5 MB, the manager sends an email message to all users and the manager shuts down. The manager cannot be restarted until the available disk space is greater than 5 MB.

You must restart the manager manually.

If you are running multiple nodes, only the node that has run out of disk space is shut down. The other manager nodes continue operating.

# Port numbers, URLs, and IP addresses

This document provides information on Deep Security default port numbers, URLs, IP addresses, and protocols. If a port, URL or IP address is configurable, a link is provided to the relevant configuration page.

- "Deep Security port numbers" below
- "Deep Security URLs" on page 483

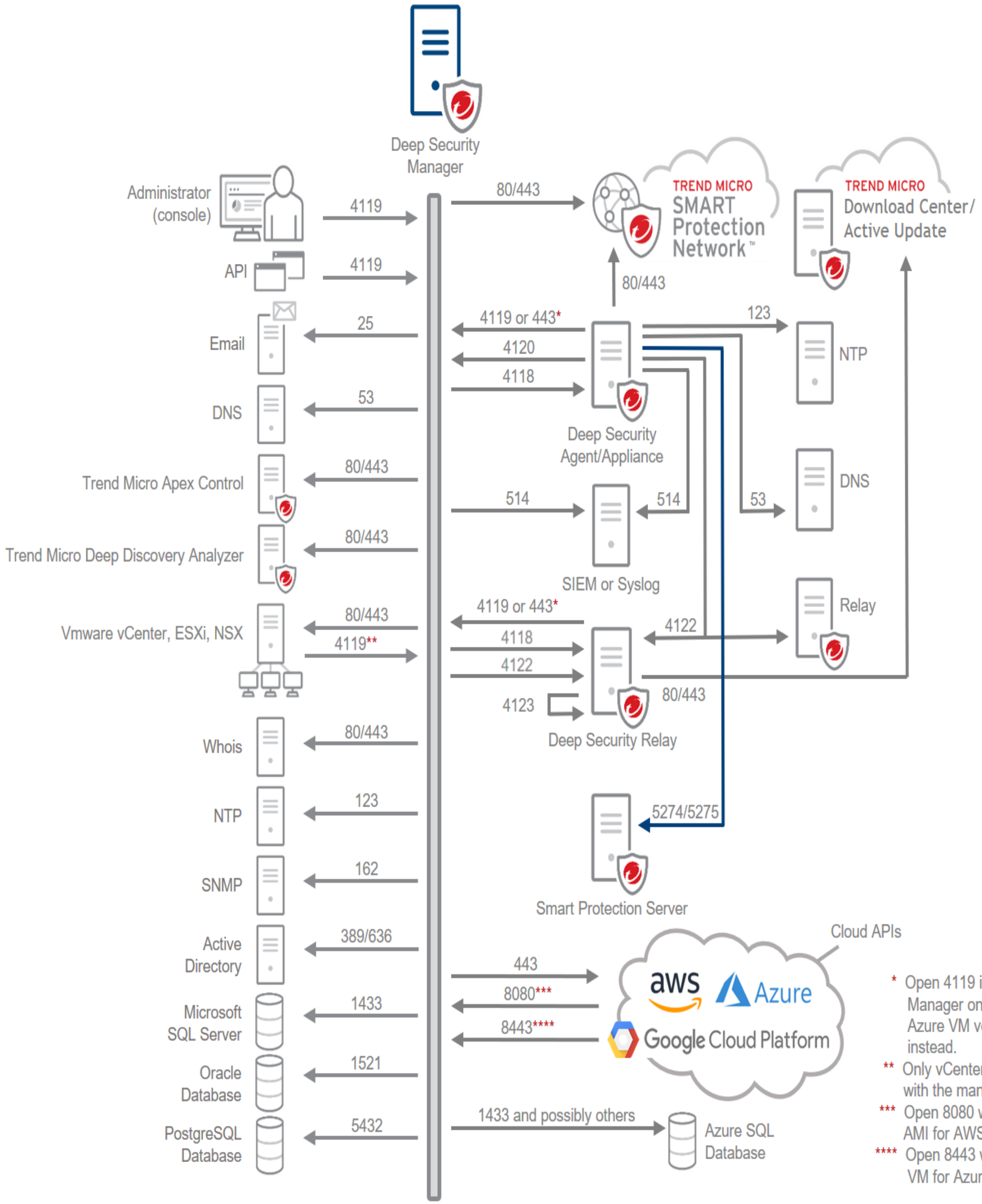
**Note:** If your network uses a proxy or load balancer, you can configure Deep Security to connect to it instead of directly to the components listed on this page. For details, see "Configure proxies" on page 1335 and "Load Balancers" on page 1482.

**Note:** In addition to the ports on this page, Deep Security uses ephemeral ports when opening a socket (source port). Under rare circumstances these may be blocked, causing connectivity issues. For details, see "Blocked port" on page 1312.

## Deep Security port numbers

The following diagram shows the default ports in a Deep Security system:

Trend Micro Deep Security for Azure Marketplace 20



* Open 4119 if you're using Deep Security Manager on-premises. For the AWS AMI and Azure VM versions of the manager, open 443 instead.

** Only vCenter and NSX (not ESXi) communicate with the manager over 4119.

*** Open 8080 with Deep Security AMI for AWS Marketplace.

**** Open 8443 with Deep Security VM for Azure Marketplace.

The following table provides details about the default ports. In this table, ports listed as mandatory must be opened to ensure the proper functioning of the Deep Security system; ports listed as optional may be opened depending on the feature or component you want to deploy; port numbers are referred to as ports.

| Port type | Default port number and protocol |
|---|---|
| Deep Security Agent listening (inbound) port | Mandatory port:<br>- 4118/HTTPS – Deep Security Agent port. Leave 4118/HTTPS closed if you plan on using agent-initiated communication. Only open it if you plan on using bidirectional or manager-initiated communication. By default, bidirectional communication is used, which is why 4118/HTTPS is listed here as 'mandatory'. See "Agent-manager communication" on page 1374 for details. |
| Deep Security Agent outbound ports | Mandatory ports:<br>- 53/DNS over TCP or UDP – DNS server port<br>- 80/HTTP, 443/HTTPS – Smart Protection Network port, Smart Protection Server for File Reputation , Deep Security Manager port<br>- 123/NTP over UDP – NTP server port<br>- 4120/HTTPS – Deep Security Manager agent heartbeat port. Allow 4120/HTTPS if you are using bidirectional or agent-initiated communication. Close it if you are using manager-initiated communication. By default, bidirectional communication is used, which is why 4120/HTTPS is listed here as 'mandatory'. See "Agent-manager communication" on page 1374 for details.<br>- 4122/HTTPS – Deep Security Relay port.<br>**Note:**<br>When using the AWS AMI and Azure VM versions of the manager, open port 443 instead of port 4119.<br>Optional ports:<br>- 514/Syslog over UDP – SIEM or syslog server port. Allow port 514 if you want the agent to send its security events directly to your SIEM or syslog server. The port number is configurable in the manager. |

| Port type | Default port number and protocol |
|---|---|
| | • 5274/HTTP, 5275/HTTPS – Smart Protection Server ports for Web Reputation. Ports 5274 and 5275 are only required for Web Reputation, not Firewall. Allow ports 5274 and 5275 if you are hosting a Smart Protection Server in your local network or Virtual Private Network (VPC), instead of having your agents connect to the cloud-based Smart Protection Network over 80/HTTP and 443/HTTPS. For details, see the Smart Protection Server documentation. |
| Deep Security Relay listening (inbound) ports | • Allow the agent listening port, since it applies to the relay too<br>• 4122/HTTPS – Deep Security Replay port.<br>• 4123 – This port is for communication between the agent and its own internal relay. |
| Deep Security Relay outbound ports | • 80/HTTP, 443/HTTPS – Trend Micro Update Server/Active Update and Download Center ports<br>• 4119/HTTPS – Deep Security Manager GUI and API port.<br>• 4122 – Port of other Deep Security Relays. |
| Deep Security Manager listening (inbound) ports | Mandatory ports:<br>• 443/HTTPS – Deep Security VM for Azure Marketplace port<br>• 4120/HTTPS – Deep Security Manager agent heartbeat port. Allow 4120/HTTPS if you are using bidirectional or agent-initiated communication. Close it if you are using manager-initiated communication. By default, bidirectional communication is used, which is why 4120/HTTPS is listed here as 'mandatory'. See "Agent-manager communication" on page 1374 for details.<br>• 8443/HTTPS – Azure web installer port |
| Deep Security | Mandatory ports: |

| Port type | Default port number and protocol |
|---|---|
| Manager (outbound ports) | • 53/DNS over TCP or UDP – DNS server port<br>• 80/HTTP, 443/HTTPS – These ports are used by various Deep Security cloud services, Smart Protection Network services, Whois server, AWS API, and Azure API, and Google Cloud Platform (GCP) API) 80 and 443 are configurable depending on the service being accessed. the Whois port.<br>• 123/NTP over UDP – NTP server port number. The NTP server can be Trend Micro Apex Central.<br>• Deep Security Manager's database server port numbers. Select from:<br>    • 1433/SQL over TCP or UDP – Microsoft SQL database port<br>    • 1433/SQL over TCP – Azure SQL Database port<br>    • 1521/SQL over TCP – Oracle database port<br>    • 5432/SQL over TCP – PostgreSQL database port<br>    • 11000-11999/SQL and 14000-14999/SQL over TCP – These are additional Azure SQL Database ports. Allow ports 11000-11999 and 14000-14999–in addition to 1433–if you are using Azure SQL Database and your Deep Security Manager runs *within* the Azure cloud boundary. If your manager runs *outside* the Azure cloud boundary, you only need to allow port 1433 to Azure SQL Database. For details, see this Azure document.<br>• 4118/HTTPS – Deep Security Agent port. Leave 4118/HTTPS closed if you plan on using agent-initiated communication. Only open it if you plan on using bidirectional or manager-initiated communication. By default, bidirectional communication is used, which is why 4118/HTTPS is listed here as 'mandatory'. See "Agent-manager communication" on page 1374 for details.<br>• 4122/HTTPS – Deep Security Relay port.<br><br>Optional ports:<br><br>• 25/SMTP over TCP – Email server port. Allow port 25 if you want email notifications. 25 is configurable in the manager.<br>• 162/SNMP over TCP or UDP – SNMP manager port. Allow port 162 if you want to "Forward system events to a remote computer via SNMP" on page 1180. |

| Port type | Default port number and protocol |
|---|---|
| | • 514/Syslog over UDP – SIEM or syslog server port. Allow port 514 if you want to forward Deep Security events to an external SIEM or syslog server. 514 is configurable in the manager.<br>• 389/LDAP, 636/LDAPS, both over TCP – Active Directory ports. Allow ports 389 and 636 if you want to add computers from Active Directory to the manager. 389 and 636 are configurable in the manager if your Active Directory server uses a different port. |

## Deep Security URLs

To restrict the URLs that are allowed in your environment, you need to ensure that your firewall allows traffic from the source to the destinations, as described in the following table. For each FQDN, you have to allow access to its associated HTTP and HTTPS URLs. For example, for the FQDN `files.trendmicro.com`, allow access to `http://files.trendmicro.com:80` and `https://files.trendmicro.com:443`.

| Source | Destination server or service name | Destination fully-qualified domain name (FQDN) |
|---|---|---|
| API clients | Deep Security APIs | • <manager FQDN or IP>:443/webservice/Manager?WSDL<br>• <manager FQDN or IP>:443/api<br>• <manager FQDN or IP>:443/rest |
| Legacy REST API clients | Deep Security legacy REST API's Status Monitoring API | • <manager FQDN or IP>:443/rest/status/manager/ping |
| Deep Security Manager, Deep Security Agent, Deep Security Relay | Download Center or web server<br>Hosts software. | • files.trendmicro.com |
| Deep Security Manager | Smart Protection Network - | • grid-global.trendmicro.com |

| Source | Destination server or service name | Destination fully-qualified domain name (FQDN) |
|---|---|---|
| | Certified Safe Software Service (CSSS)<br>Used for event tagging with Integrity Monitoring. | |
| Deep Security Manager | Trend Micro Vision One<br>Used to "Integrate with Trend Vision One (XDR)" on page 1682. | • *.xdr.trendmicro.com:443<br>• *.xbc.trendmicro.com:443<br>• *.mgcp.trendmicro.com:443<br>• *.manage.trendmicro.com:443<br>• *.xdr.trendmicro.co.jp:443 (for Japanese regions) |
| Deep Security Agent | Smart Protection Network - Global Census Service<br>Used for behavior monitoring, and predictive machine learning. | 20.0 and later agents connect to:<br>• ds2000-en-census.trendmicro.com<br>• ds2000-jp-census.trendmicro.com<br>12.0 and later agents connect to:<br>• ds1200-en-census.trendmicro.com<br>• ds1200-jp-census.trendmicro.com<br>11.0 and later agents connect to:<br>• ds1100-en-census.trendmicro.com<br>• ds1100-jp-census.trendmicro.com<br>10.2 and 10.3 agents connect to: |

| Source | Destination server or service name | Destination fully-qualified domain name (FQDN) |
|---|---|---|
| | | - ds1020-en-census.trendmicro.com<br>- ds1020-jp-census.trendmicro.com<br>- ds1020-sc-census.trendmicro.com<br>10.1 and 10.0 agents connect to:<br>- ds1000-en.census.trendmicro.com<br>- ds1000-jp.census.trendmicro.com<br>- ds1000-sc.census.trendmicro.com<br>- ds1000-tc.census.trendmicro.com |
| Deep Security Agent | Smart Protection Network -<br>Good File Reputation Service<br>Used for behavior monitoring, predictive machine learning, and process memory scans. | 20.0 and later agents connect to:<br>- deepsec20-en.gfrbridge.trendmicro.com<br>- deepsec20-jp.gfrbridge.trendmicro.com<br>12.0 and later agents connect to:<br>- deepsec12-en.gfrbridge.trendmicro.com<br>- deepsec12-jp.gfrbridge.trendmicro.com<br>11.0 and later agents connect to:<br>- deepsec11-en.gfrbridge.trendmicro.com<br>- deepsec11-jp.gfrbridge.trendmicro.com<br>10.2 and 10.3 agents connect to: |

| Source | Destination server or service name | Destination fully-qualified domain name (FQDN) |
|---|---|---|
| | | - deepsec102-en.gfrbridge.trendmicro.com<br>- deepsec102-jp.gfrbridge.trendmicro.com<br>10.1 and 10.0 agents connect to:<br>- deepsec10-en.grid-gfr.trendmicro.com<br>- deepsec10-jp.grid-gfr.trendmicro.com<br>- deepsec10-cn.grid-gfr.trendmicro.com |
| Deep Security Agent | Smart Protection Network - Smart Feedback | 20.0 and later agents connect to:<br>- ds200-en.fbs25.trendmicro.com<br>- ds200-jp.fbs25.trendmicro.com<br>12.0 and later agent connect to:<br>- ds120-en.fbs25.trendmicro.com<br>- ds120-jp.fbs25.trendmicro.com<br>11.0 and later agents connect to:<br>- deepsecurity1100-en.fbs25.trendmicro.com<br>- deepsecurity1100-jp.fbs25.trendmicro.com<br>10.0 agents connect to:<br>- deepsecurity1000-en.fbs20.trendmicro.com |

| Source | Destination server or service name | Destination fully-qualified domain name (FQDN) |
|---|---|---|
| | | • deepsecurity1000-jp.fbs20.trendmicro.com<br>• deepsecurity1000-sc.fbs20.trendmicro.com |
| Deep Security Agent | Smart Protection Network - Smart Scan Service | 20.0 and later agents connects to:<br>• ds20.icrc.trendmicro.com<br>• ds20-jp.icrc.trendmicro.com<br>12.0 and later agents connect to:<br>• ds120.icrc.trendmicro.com<br>• ds120-jp.icrc.trendmicro.com<br>11.0 and later agents connect to:<br>• ds110.icrc.trendmicro.com<br>• ds110-jp.icrc.trendmicro.com<br>10.2 and 10.3 agents connect to:<br>• ds102.icrc.trendmicro.com<br>• ds102-jp.icrc.trendmicro.com<br>• ds102-sc.icrc.trendmicro.com.cn<br>10.1 and 10.0 agents connect to:<br>• ds10.icrc.trendmicro.com |

| Source | Destination server or service name | Destination fully-qualified domain name (FQDN) |
|---|---|---|
| | | • ds10.icrc.trendmicro.com/tmcss/<br>• ds10-jp.icrc.trendmicro.com/tmcss/<br>• ds10-sc.icrc.trendmicro.com.cn/tmcss/<br>9.6 and 9.5 agents connect to:<br>• iaufdbk.trendmicro.com<br>• ds96.icrc.trendmicro.com<br>• ds96-jp.icrc.trendmicro.com<br>• ds96-sc.icrc.trendmicro.com.cn<br>• ds95.icrc.trendmicro.com<br>• ds95-jp.icrc.trendmicro.com<br>• ds95-sc.icrc.trendmicro.com.cn |
| Deep Security Agent | Smart Protection Network - predictive machine learning | 20.0 and later agents connect to:<br>• ds20-en-b.trx.trendmicro.com<br>• ds20-jp-b.trx.trendmicro.com<br>• ds20-en-f.trx.trendmicro.com<br>• ds20-jp-f.trx.trendmicro.com<br>12.0 and later agents connect to:<br>• ds120-en-b.trx.trendmicro.com<br>• ds120-jp-b.trx.trendmicro.com |

| Source | Destination server or service name | Destination fully-qualified domain name (FQDN) |
|---|---|---|
| | | • ds120-en-f.trx.trendmicro.com<br>• ds120-jp-f.trx.trendmicro.com<br>11.0 and later agents connect to:<br>• ds110-en-b.trx.trendmicro.com<br>• ds110-jp-b.trx.trendmicro.com<br>• ds110-en-f.trx.trendmicro.com<br>• ds110-jp-f.trx.trendmicro.com<br>10.2 and 10.3 agents connect to:<br>• ds102-en-f.trx.trendmicro.com<br>• ds102-jp-f.trx.trendmicro.com<br>• ds102-sc-f.trx.trendmicro.com |
| Deep Security Agent | Smart Protection Network - Web Reputation Service | 20.0 and later agents connect to:<br>• ds20-0-en.url.trendmicro.com<br>• ds20-0-jp.url.trendmicro.com<br>12.0 and later agents connect to:<br>• ds12-0-en.url.trendmicro.com<br>• ds12-0-jp.url.trendmicro.com<br>The 11.0 and later agents connect to: |

| Source | Destination server or service name | Destination fully-qualified domain name (FQDN) |
|---|---|---|
| | | - ds11-0-en.url.trendmicro.com<br>- ds11-0-jp.url.trendmicro.com<br>10.2 and 10.3 agents connect to:<br>- ds10-2-en.url.trendmicro.com<br>- ds10-2-sc.url.trendmicro.com.cn<br>- ds10-2-jp.url.trendmicro.com<br>10.1 and 10.0 agents connect to:<br>- ds100-en.url.trendmicro.com<br>- ds100-sc.url.trendmicro.com<br>- ds100-jp.url.trendmicro.com<br>9.6 and 9.5 agents connect to:<br>- ds96-en.url.trendmicro.com<br>- ds96-jp.url.trendmicro.com<br>- ds95-en.url.trendmicro.com<br>- ds95-jp.url.trendmicro.com |
| Deep Security Manager | Help and support | - help.deepsecurity.trendmicro.com<br>- success.trendmicro.com/product-support/deep-security |

| Source | Destination server or service name | Destination fully-qualified domain name (FQDN) |
|---|---|---|
| Deep Security Manager | Licensing and registration servers | • licenseupdate.trendmicro.com<br>• clp.trendmicro.com<br>• olr.trendmicro.com |
| Deep Security Manager | News feed | • news.deepsecurity.trendmicro.com<br>• news.deepsecurity.trendmicro.com/news.atom<br>• news.deepsecurity.trendmicro.com/news_ja.atom |
| Browser on Deep Security Agent computers, and the computer used to log in to Deep Security Manager | Site Safety | Optional. There are links to the URLs below within the manager UI and on the agent's 'Your administrator has blocked access to this page for your safety' page.<br>• sitesafety.trendmicro.com<br>• jp.sitesafety.trendmicro.com |
| Deep Security Relay, and Deep Security Agent | Update Server (also called Active Update)<br>Hosts security updates. | • iaus.activeupdate.trendmicro.com<br>• iaus.trendmicro.com<br>• ipv6-iaus.trendmicro.com<br>• ipv6-iaus.activeupdate.trendmicro.com |
| Deep Security Manager | AWS and Azure URLs<br>Used for adding AWS accounts, Azure accounts and | AWS URLs<br>• URLs of AWS endpoints listed on this AWS page, under these headings: |

| Source | Destination server or service name | Destination fully-qualified domain name (FQDN) |
|---|---|---|
| | Google Cloud Platform (GCP) service accounts to Deep Security Manager. | - Amazon Elastic Compute Cloud (Amazon EC2)<br>- AWS Security Token Service (AWS STS)<br>- AWS Identity and Access Management (IAM)<br>- Amazon WorkSpaces<br>Azure URLs<br>- login.windows.net (authentication)<br>- login.microsoftonline.com (authentication)<br>- management.azure.com (Azure API)<br>- login.microsoftonline.us (authentication to Azure Government)<br>- management.usgovcloudapi.net (authentication to Azure Government)<br>- management.core.windows.net (Azure API)<br>**Note:** The management.core.windows.net URL is only required if you used the v1 Azure connector available in Deep Security Manager 9.6 to add an Azure account to the manager. With Deep Security Manager 10.0 and later, a v2 connector is used, and does not require access to this URL.<br>GCP URLs<br>- oauth2.googleapis.com (authentication) |

| Source | Destination server or service name | Destination fully-qualified domain name (FQDN) |
|---|---|---|
| | | • googleapis.com (GCP API)<br>• cloudresourcemanager.googleapis.com (GCP API) |
| Deep Security Manager | Telemetry service<br>Used for protected "Deep Security Product Usage Data Collection" on page 1671. | • telemetry.deepsecurity.trendmicro.com |
| Deep Security Manager | Activation<br>Used for activating Deep Security Manager with an activation code and for integrating with Trend Vision One. | • flywheel.xdr.trendmicro.com |

# Get Started

## Check digital signatures on software packages

Before installing Deep Security, check the digital signature on the software ZIP packages and installer files. A correct digital signature indicates that the software is authentically from Trend Micro and has not been corrupted or tampered with.

- "Check the signature on software ZIP packages" below
- "Check the signature on installer files (EXE, MSI, RPM or DEB files)" on page 496

You can also validate the software's checksums, as well as the security updates' and Deep Security Agent modules' digital signature. See "How Deep Security validates update integrity" on page 1532 and "Configure Linux Secure Boot for agents" on page 527.

### Check the signature on software ZIP packages

The Deep Security Agent and online help are made available in ZIP packages. These packages are digitally signed. You can check the digital signature on the ZIP file in the following ways:

By importing or exporting the ZIP to or from the manager

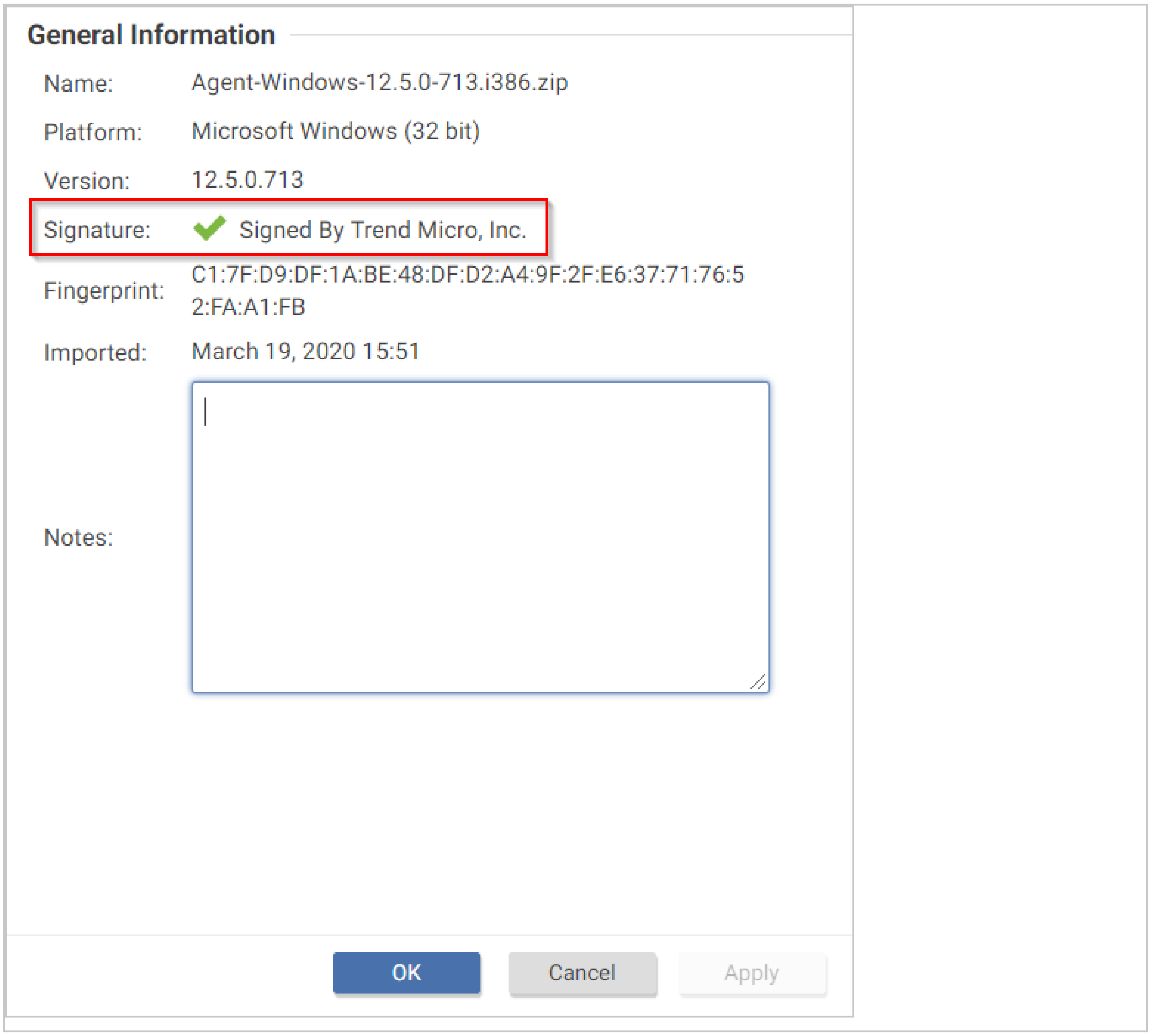
> Import or export a ZIP file following the instructions in "Import agent software" on page 522 or "Export the agent installer" on page 524.
>
> On import or export, the manager checks the digital signature on the ZIP file. If the signature is valid, the manager allows the import or export to proceed. If the signature is invalid or missing, the manager disallows the action, deletes the ZIP, and logs an event.

By viewing the ZIP's properties file

1. Log in to Deep Security Manager.
2. Click **Administration** at the top.
3. On the left, expand **Updates > Software > Local**.

4. Find the ZIP package whose digital signature you want to check and double-click it. If it is not there, import it.

The **Properties** page for the ZIP file opens, and the manager checks the digital signature. If the signature is valid, you will see a green check mark in the **Signature** field, as shown in the following illustration. If the signature is not valid or does not exist, the manager deletes the ZIP and logs an event.



General Information

Name: Agent-Windows-12.5.0-713.i386.zip

Platform: Microsoft Windows (32 bit)

Version: 12.5.0.713

Signature: ✓ Signed By Trend Micro, Inc.

Fingerprint: C1:7F:D9:DF:1A:BE:48:DF:D2:A4:9F:2F:E6:37:71:76:52:FA:A1:FB

Imported: March 19, 2020 15:51

Notes:

By using jarsigner

Use the jarsigner Java utility to check a signature on a ZIP when you cannot check it through the manager. For example, suppose you obtained an agent ZIP package from a non-manager source, such as the Deep Security Software page, and then wanted to install the agent manually. In this scenario, you would use the jarsigner utility since the manager is not involved.

To check a signature using jarsigner:

1. Install the latest Java Development Kit on your computer.
2. Download the ZIP.
3. Use the jarsigner utility within the JDK to check the signature. The command is:

   ```
   jarsigner -verify -verbose -certs -strict <ZIP_file>
   ```

   Example:

   ```
   jarsigner -verify -verbose -certs -strict Agent-RedHat_EL7-
   11.2.0-124.x86_64.zip
   ```

4. Read any errors as well as the content of the certificate to determine if the signature can be trusted.

## Check the signature on installer files (EXE, MSI, RPM or DEB files)

The installers for the Deep Security Agent and Deep Security Notifier are digitally signed using RSA. The installer is an EXE or MSI file on Windows, an RPM file on Linux operating systems (Amazon, CloudLinux, Oracle, Red Hat, and SUSE), or a DEB file on Debian and Ubuntu.

> **Note:** The instructions below describe how to check a digital signature manually on an installer file. If you'd like to automate this check, you can include it in your agent deployment scripts. For more on deployment scripts, see "Use deployment scripts to add and protect computers" on page 1623.

Follow the instructions that correspond to the type of installer file you want to check.

- "Check the signature on an EXE or MSI file" on the next page
- "Check the signature on an RPM file" on the next page

- "Check the signature on a DEB file" on page 499

## Check the signature on an EXE or MSI file

1. Right-click the EXE or MSI file and select **Properties**.
2. Click the **Digital Signatures** tab to check the signature.

## Check the signature on an RPM file

First, install GnuPG

> If not already installed, install GnuPG on the agent computer where you intend to check the signature. This utility includes the GPG command-line tool, which you need in order to import the signing key and check the digital signature.
>
> Note that GnuPG is installed by default on most Linux distributions.

Next, import the signing key

1. Look for the `3trend_public.asc` file in the root folder of the agent's ZIP file. The ASC file contains a GPG public signing key that you can use to verify the digital signature.
2. Optionally, verify the SHA-256 hash digest of the **ASC** file using any hashing utility. The hash is:

   `c59caa810a9dc9f4ecdf5dc44e3d1c8a6342932ca1c9573745ec9f1a82c118d7` - for agent version 20.0.0-2593 or earlier

   `bd3b00763db11cee2a6b990428d506f11cf86c68354388fe9cc41fa7e6c9ddae` - for agent version 20.0.0-2971 or later

   `7a7509c5458c762f6a341820a93e09f0f1b9dd3258608753e18d26575e9c730f` - for agent version 20.0.1-3180 or later
3. On the agent computer where you intend to check the signature, import the ASC file. Use this command:

   > **Note:** Commands are case-sensitive.

```
gpg --import 3trend_public.asc
```

The following messages appear:

```
gpg: directory `/home/build/.gnupg' created
gpg: new configuration file `/home/build/.gnupg/gpg.conf'
created
gpg: WARNING: options in `/home/build/.gnupg/gpg.conf' are not
yet active during this run
gpg: keyring `/home/build/.gnupg/secring.gpg' created
gpg: keyring `/home/build/.gnupg/pubring.gpg' created
gpg: /home/build/.gnupg/trustdb.gpg: trustdb created
gpg: key E1051CBD: public key "Trend Micro (trend linux sign)
<alloftrendetscodesign@trendmicro.com>" imported
gpg: Total number processed: 1
gpg: imported: 1 (RSA: 1)
```

4. Export the GPG public signing key from the ASC file:

   ```
   gpg --export -a 'Trend Micro' > RPM-GPG-KEY-CodeSign
   ```

5. Import the GPG public signing key to the RPM database:

   ```
   sudo rpm --import RPM-GPG-KEY-CodeSign
   ```

6. Verify that the GPG public signing key has been imported:

   ```
   rpm -qa gpg-pubkey*
   ```

7. The fingerprints of imported GPG public keys appear. The Trend Micro key is:

   `gpg-pubkey-e1051cbd-5b59ac99` - for agent version 20.0.0-2593 or earlier

   `gpg-pubkey-e1051cbd-6030cc3a` - for agent version 20.0.0-2971 or later

   `gpg-pubkey-e1051cbd-659d0a3e` - for agent version 20.0.1-3180 or later

The signing key has now been imported and can be used to check the digital signature on the agent RPM file.

Finally, verify the signature on the RPM file

You can either verify the signature on the RPM file manually or have a deployment script to perform the check, as described in "Use deployment scripts to add and protect computers" on page 1623.

To perform a manual check, execute the following command:

```
rpm -K Agent-PGPCore-<OS agent version>.rpm
```

Example:

```
rpm -K Agent-PGPCore-RedHat_EL7-11.0.0-950.x86_64.rpm
```

Ensure that you run the preceding command on the `Agent-PGPCore-<...>.rpm` file, because running it on `Agent-Core-<...>.rpm` does not work. If you cannot find the `Agent-PGPCore-<...>.rpm` file in the agent ZIP, use a newer ZIP, specifically:

- Deep Security Agent 11.0 update 15 or a later update

  or

- Deep Security Agent 12 update 2 or later

  or

- Deep Security Agent 20 or later

If the signature verification is successful, the following message appears:

```
Agent-PGPCore-RedHat_EL7-11.0.0-950.x86_64.rpm: rsa sha1 (md5) pgp md5
OK
```

## Check the signature on a DEB file

First, install the dpkg-sig utility

Install dpkg-sig on the agent computer where you intend to check the signature, if it is not already installed. This utility includes the GPG command-line tool, which you need in order to import the signing key and check the digital signature.

Next, import the signing key

1. Look for the `3trend_public.asc` file in the root folder of the agent's ZIP file. The ASC file contains a GPG public signing key that you can use to verify the digital signature.
2. Optionally, verify the SHA-256 hash digest of the **ASC** file using any hashing utility. The hash is:

   `c59caa810a9dc9f4ecdf5dc44e3d1c8a6342932ca1c9573745ec9f1a82c118d7` - for agent version 20.0.0-2593 or earlier

   `bd3b00763db11cee2a6b990428d506f11cf86c68354388fe9cc41fa7e6c9ddae` - for agent version 20.0.0-2971 or later

   `7a7509c5458c762f6a341820a93e09f0f1b9dd3258608753e18d26575e9c730f` - for agent version 20.0.1-3180 or later
3. On the agent computer where you intend to check the signature, import the ASC file to the GPG keyring. Use the following command:

   ```
   gpg --import 3trend_public.asc
   ```

   The following message appears:

   ```
   gpg: key E1051CBD: public key "Trend Micro (trend linux sign)
   <alloftrendetscodesign@trendmicro.com>" imported

   gpg: Total number processed: 1

   gpg: imported: 1 (RSA: 1)
   ```
4. Optionally, display the Trend Micro key information. Use the following command:

   ```
   gpg --list-keys
   ```

   A message similar to the following appears:

   ```
   /home/user01/.gnupg/pubring.gpg
   --------------------------------
   pub 2048R/E1051CBD 2018-07-26 [expires: 2021-07-25]
   uid Trend Micro (trend linux sign)
   <alloftrendetscodesign@trendmicro.com>
   ```

```
sub 2048R/202C302E 2018-07-26 [expires: 2021-07-25]
```

Finally, verify the signature on the DEB file

You can either verify the signature on the DEB file manually or have a deployment script to perform the check, as described in "Use deployment scripts to add and protect computers" on page 1623.

To perform a manual check, enter the following command:

```
dpkg-sig --verify <agent_deb_file>
```

where `<agent_deb_file>` is the name and path of the agent DEB file. For example:

```
dpkg-sig --verify Agent-Core-Ubuntu_16.04-12.0.0-563.x86_64.deb
```

A processing message appears:

```
Processing Agent-Core-Ubuntu_16.04-12.0.0-563.x86_64.deb...
```

If the signature is verified successfully, the following message appears:

```
GOODSIG _gpgbuilder CF5EBBC17D8178A7776C1D365B09AD42E1051CBD
1568153778
```

# Deploy Deep Security Manager

## Prepare a database

### Database requirements

Deep Security Manager uses a database server. Before you install Deep Security Manager, you must install a database server that meets the following requirements:

Tip: You should use use the Deep Security Manager VM for Azure Marketplace to deploy Deep Security Manager and its database on Azure automatically. If you use this method, you can disregard the database installation and configuration steps because the VM deployment wizard takes care of these tasks for you. For information on the VM deployment, see "Deploy Deep Security Manager VM for Azure Marketplace" on page 506.

- "Software requirements" below
- "Hardware requirements" on the next page
- "Network requirements" on the next page
- "Scaling requirements" on page 504

After reviewing the requirements, you are ready to install the database server.

## Software requirements

Deep Security supports the following databases:

- PostgreSQL 17.n (Core, Amazon RDS, Amazon Aurora distributions only)
- PostgreSQL 16.n (Core, Amazon RDS, Amazon Aurora distributions only)
- PostgreSQL 15.n (Core, Amazon RDS, Amazon Aurora distributions only)
- PostgreSQL 14.n (Core, Amazon RDS, Amazon Aurora distributions only)
- Microsoft SQL Server 2022 and its service packs
- Microsoft SQL Server 2019 and its service packs
- Microsoft SQL Server 2017 and its service packs
- Microsoft SQL Server 2016 and its service packs
- Microsoft SQL Relational Database Service (RDS)
- Azure SQL Database  multi-tenancy)
- Oracle 19c when deployed as software or when used with Amazon RDS
- Oracle 23c when deployed as software

Note the following:

- Microsoft SQL Server Express is only supported in limited deployments. See "Microsoft SQL Server Express considerations" on the next page.
- Microsoft SQL Server is only supported when database containment is set to NONE. For details, see Contained Databases.
- Oracle Database Express (XE) is not supported.

#### Microsoft SQL Server Express considerations

Some deployments might be able to use Microsoft SQL Server Express for the Deep Security Manager database. If you think your deployment cannot operate within the following limitations, use another database or migrate to the Enterprise edition.

- Express edition size limitations: Microsoft SQL Server Express has a 10 GB maximum database size and other important limits. High load scenarios are not supported by Express. Symptoms can include database connection errors.
- Express edition LocalDB preset: Express has a LocalDB preset. Additional configuration may be required to accept remote connections.
- Limited number of protected computers: Do not use Microsoft SQL Server Express if your deployment has more than 50 protected computers. More events generated from the computer result in a larger database which Microsoft SQL Server Express cannot handle.
- Lack of multi-node support: Multi-node Deep Security Manager, required for larger deployments, is not supported by Express.
- Security module limitations: Only Deep Security Anti-Malware and Intrusion Prevention modules are supported with a Microsoft SQL Server Express database due to its limitations. If you require any other protection modules, use another supported database.

> Warning: Exceeding these limits can result in a service outage. You would need to upgrade to a paid version of Microsoft SQL Server.

### Hardware requirements

- The database CPU, memory, and disk space should conform to the recommendations in "Database sizing" on page 468.
- The database should be installed on a dedicated server that is separate from the manager nodes.

### Network requirements

- The database should be located on the same network as Deep Security Manager. The network should have a 1 GB LAN connection to ensure unhindered communication between the two (WAN connections are not recommended). The same applies to additional Deep Security Manager nodes. 2 milliseconds latency or less is recommended for the connection from the manager to the database.

- Databases hosted in the cloud should not use multiple availability zones ("multi-AZ"), which can increase network latency.

### Scaling requirements

- You should use database load balancing, mirroring, and high availability (HA) mechanisms for scalability and service uptime. Consult your database vendor's documentation for setup details.
- If you decide to replicate the database, you should use database mirroring over database replication. Database replication technologies sometimes add columns to the database tables during replication. This changes the Deep Security database schema and can result in critical failures. Deep Security works with any failover protection technology that does not change its schema.

## Install a database server

After reviewing the database requirements, you are ready to install a database server.  Refer to your database provider's documentation for instructions.

Tip: For a quick and easy setup, use postgreSQL. It's free, and can be downloaded from this link: PostgreSQL software download page.

After installing the database server, you are ready to configure it.

## Configure the database

After installing the database, you are ready to configure it for Deep Security Manager.

First, configure a database instance, a database user, and several other vendor-specific settings. See one of the following sections:

Configure PostgreSQL

#### Basic configuration

1. Connect to the PostgreSQL database server using a client program, such as psql or pgAdmin.
2. Create an empty database instance and a database user with the appropriate permissions by executing the following commands:

```
CREATE DATABASE "<database-name>";
```

```
CREATE ROLE "<dsm-username>" WITH PASSWORD '<password>' LOGIN;
```

```
GRANT ALL ON DATABASE "<database-name>" TO "<dsm-username>";
```

```
GRANT CONNECT ON DATABASE "<database-name>" TO "<dsm-username>";
```

```
ALTER DATABASE "<database-name>" OWNER TO "<dsm-username>";
```

This user will be used by Deep Security Manager to connect to the database instance.

### Optional PostgreSQL tuning

See "Maintain PostgreSQL" on page 1449.

## Configure Microsoft SQL Server

### Basic configuration

1. Connect to Microsoft SQL Server by opening Microsoft SQL Server Management Studio (SSMS).
2. Create an empty database instance. This database instance will be used by Deep Security Manager.
3. Create a database account with **db_owner** rights. This account will be used by Deep Security Manager to connect to the database.
4. Enable the TCP/IP protocol for the database instance (see https://docs.microsoft.com/en-us/previous-versions/bb909712(v=vs.120)?redirectedfrom=MSDN).
5. Configure connection timeouts. Go **SQL management studio > SQL Server properties > Connections > Remote query timeout** and select **0 (No Timeout)**. This setting prevents database connection timeouts that can occur when you upgrade if each database schema migration operation takes a long time to complete.

## Configure Oracle Database

#### Basic configuration

1. Connect to Oracle Database using a client program such as SQL*Plus or SQL Developer.
2. Start the "Oracle Listener" service. Verify that it accepts TCP connections.
3. Create an empty database instance. This database instance will be used by Deep Security Manager.
4. Create a database account that will be used by Deep Security Manager to connect to the database. When creating the account, follow these guidelines:
   - Assign the **CONNECT** and **RESOURCE** roles and **UNLIMITED TABLESPACE**, **CREATE SEQUENCE**, **CREATE TABLE** and **CREATE TRIGGER** permissions.
   - Don't use special characters in Deep Security Manager's database user name. Although Oracle allows special characters when configuring the database user object if they are surrounded by quotes, Deep Security does not support special characters for the database user.

#### Oracle RAC configuration

If you're using Oracle RAC, disable the Firewall module or customize the Firewall settings according to the instructions in "Firewall settings with Oracle RAC" on page 884.

Next, perform the following configurations:

1. Synchronize both time and time zone. Use the same time source on both the database and Deep Security Manager servers.
2. Allow network connections between Deep Security Manager and the database server. See "Port numbers, URLs, and IP addresses" on page 478.
3. Optionally, configure encryption. See "Encrypt communication between the Deep Security Manager and the database" on page 1506.

# Deploy Deep Security Manager VM for Azure Marketplace

To start protecting your Azure virtual machines (VM) with Deep Security Manager VM for Azure Marketplace, basic steps include:

1. "Buy Deep Security from the Azure Marketplace" on the next page.
2. "Add a Microsoft Azure account to Deep Security" on page 510.
3. "Allow the inbound SSH port of the DSM virtual machine" on page 509.

4. "Create a policy" on page 510.
5. "Deploy Deep Security Agents" on page 510.

If you are upgrading an existing Deep Security Manager VM for Azure Marketplace, see "Upgrade Deep Security Manager VM for Azure Marketplace" on page 1549

## Buy Deep Security from the Azure Marketplace

You can buy Deep Security from the Azure Marketplace as *Deep Security Manager (BYOL)*.

> **Note:** To buy Deep Security Manager (BYOL) , you need to have already obtained a license for Deep Security. If you need a license, contact azure@trendmicro.com for help with obtaining one.

1. Log in to your Azure portal and click **All Services > General > Marketplace**.
2. Search for `Deep Security Manager (BYOL)`.
3. In the search results, click **Deep Security Manager (BYOL)**.
4. Review the information provided and click **Create**.
5. Follow the steps of the Create Deep Security Manager journey to create a Deep Security virtual machine.
   a. Specify the name of the Deep Security Manager VM and configure other general settings on the Basics blade and then click **OK**.
      - The credentials you specify in this blade are what you will use to log on to the Deep Security Manager virtual machine.
      - Depending on the type of authentication you select, you have to enter a strong password or an SSH public key.
      - Type in a name into **Resource group** to create a new Resource group.

        > **Note:** Azure does not allow Deep Security Manager VM to be deployed on existing resource groups. A new resource group must be created.

      - Select an Azure region from the **Location** list.

   b. Select a virtual machine size, configure the Deep Security Manager URL and port numbers on the Deep Security Manager VM blade, and then click **OK**.

- Use the DNS name you enter in **Deep Security Manager URL** such as `azurevmdemo01`.
- Enter the port number for the **Deep Security Manager console port** to access and log into Deep Security Manager, such as `https://azurevmdemo01.eastus.cloudapp.azure.com:443`.
- Enter the heartbeat port number used by the Deep Security Agents to communicate with Deep Security Manager.

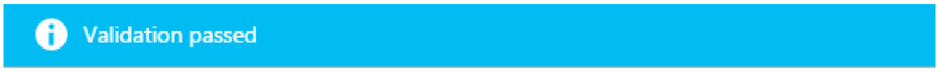
c. Create a new database or enter the name of an existing one on the Database Settings blade and then click **OK**.

- Do not type anything into **Database Hostname** if you create a new database. However, if you click **Use Existing**, then the database hostname is required.
- You can view the names of existing Azure SQL databases by going to the SQL databases blade and viewing the properties of a database (**Settings blade > Properties blade > Server name**).

d. Enter the name of the administrator account that you will use to sign in to Deep Security Manager on the Deep Security Credentials blade and enter and confirm the password for that account and click **OK**.

e. Click the arrows to review the settings for the new virtual network and the subnet for the Deep Security Manager VM on the Network Settings blade and click **OK** twice.

f. Review the information on the Summary blade and click **OK** when "Validation passed" appears at the top of the summary to finish creating the virtual machine.



Validation passed

g. Click **Terms of use**, **privacy policy**, and **Azure Marketplace Terms** on the Buy blade to review them and then click **Create**.

It will take approximately 30-40 minutes before your new virtual machine is running.

6. When installation is complete, open a browser and go to:

   `https://<DNS name>:8443`

   where the DNS name is the name you specified on the Deep Security Manager blade (for example, `azurevmdemo01.eastus.cloudapp.azure.com`). To view the DNS name for your Deep Security virtual machine, select the virtual machine in the **Public IP address** blade, and then click **Overview**. It will be in the **DNS name** field.

7. Enter the Subscription ID for the virtual machine and click **Sign in**.

   If the installation succeeded, you will be redirected to Deep Security Manager. If the installation failed you will see an error message. If this happens, click **Install Deep Security Manager again** and verify all settings as you step through the installation again.

## Allow the inbound SSH port of the DSM virtual machine

1. Go to the Deep Security Manager deployed resource group.
2. Select the type of the **Network security group**.
3. Select the **Inbound security rules** from the left navigation pane.
4. Select **+ Add > Add inbound security rules**.
5. Select the **Source** from the drop-down.
6. Enter the **Source IP addresses** or **CIDR ranges**, as needed.

   Provide an address range using CIDR notation (for example, 192.168.99.0/24 or 2001:1234::/64), or an IP address (for example, 192.168.99.0 or 2001:1234::) . You can also provide a comma-separated list of IP addresses or address ranges using either IPv4 or IPv6.

7. Enter the **Source port range**.

   Provide a single port, such as 80; a port range, such as 1024-65535; or a comma-separated list of single ports and/or port ranges, such as 80,1024-65535. This specifies on which ports traffic will be allowed or denied by this rule. Use an asterisk to allow traffic on any port.

8. Use the **Destination** drop-down to limit the Destination as required. We recommend you use the default of Any.
9. On the **Service** drop-down, select SSH.
10. Enter the **Destination port ranges**.

Provide a single port, such as 80; a port range, such as 1024-65535; or a comma-separated list of single ports and/or port ranges, such as 80,1024-65535. This specifies on which ports traffic will be allowed or denied by this rule. Use an asterisk to allow traffic on any port.

11. You can change the **Priority** or **Name** of the rule. (Optional)
12. Add a **Description** of the rule. (Optional)
13. Select **Add** to create the rule.

## Add a Microsoft Azure account to Deep Security

Once you've installed Deep Security Manager, you can add and protect Microsoft Azure virtual machines by connecting a Microsoft Azure account to the Deep Security Manager. For instructions, see "Add a Microsoft Azure account to Deep Security" on page 602.

## Create a policy

After you have added Microsoft Azure virtual machines to Deep Security, you need to create a policy that specifies how Deep Security should protect them.

You have two options for creating a policy:

- You can make a duplicate copy of one of the server policies that comes with Deep Security and modify it as required.
- You can build your own policy using the Base Policy as your starting point.

For more information on how to create a policy, see "Create policies" on page 630.

For more information on how policies work in Deep Security, see "Policies, inheritance, and overrides" on page 634.

## Deploy Deep Security Agents

To start protecting your Microsoft Azure virtual machines with Deep Security, you need to deploy Deep Security Agents to them. You can do this in multiple ways. See "Install the agent on Azure VMs" on page 564 for details.

# Add activation codes

You must enter one or more activation codes into the manager .

**Note:** An activation code is also known as a license.

To enter your activation code or codes:

1. Log in to Deep Security Manager.
2. At the top, click **Administration**.
3. On the left, click **Licenses**.
4. In the main pane, click **Enter New Activation Code**.
5. Enter the activation code or codes you obtained from your sales representative.
6. Click **Next** and close the wizard when you have finished.

# Set up multiple nodes

## Install Deep Security Manager on multiple nodes

Instead of running Deep Security Manager on *one* server, you can install Deep Security Manager on *multiple* servers ("nodes") and connect them to one shared database. This provides better:

- Reliability
- Availability
- Scalability
- Performance

You can log in to any node. Each node can do all types of tasks. No node is more important than any of the others. A node failure does not cause service downtime, and does not result in data loss. Deep Security Manager processes many concurrent activities in a distributed pool that all online nodes execute. All activity that does not happen due to user input is packaged as a job, and runs on any available manager (with some exceptions for "local" jobs that are executed on each node, like cache clearing).

**Each node must run the same Deep Security Manager software version.** When you upgrade, the first manager you upgrade will temporarily take over all duties and shut down the other nodes. On **Administration > Manager Nodes**, other nodes' status will be "Offline" with an indication that an upgrade is required. Once upgraded, nodes will automatically return online and begin processing again.

## Set up a load balancer

If you are deploying multiple server nodes of Deep Security Manager for a large scale deployment, a load balancer can help distribute connections with agents and appliances. Load balancers with virtual IPs can also provide a single inbound port number such as TCP 443, instead of the multiple port numbers that Deep Security normally requires.

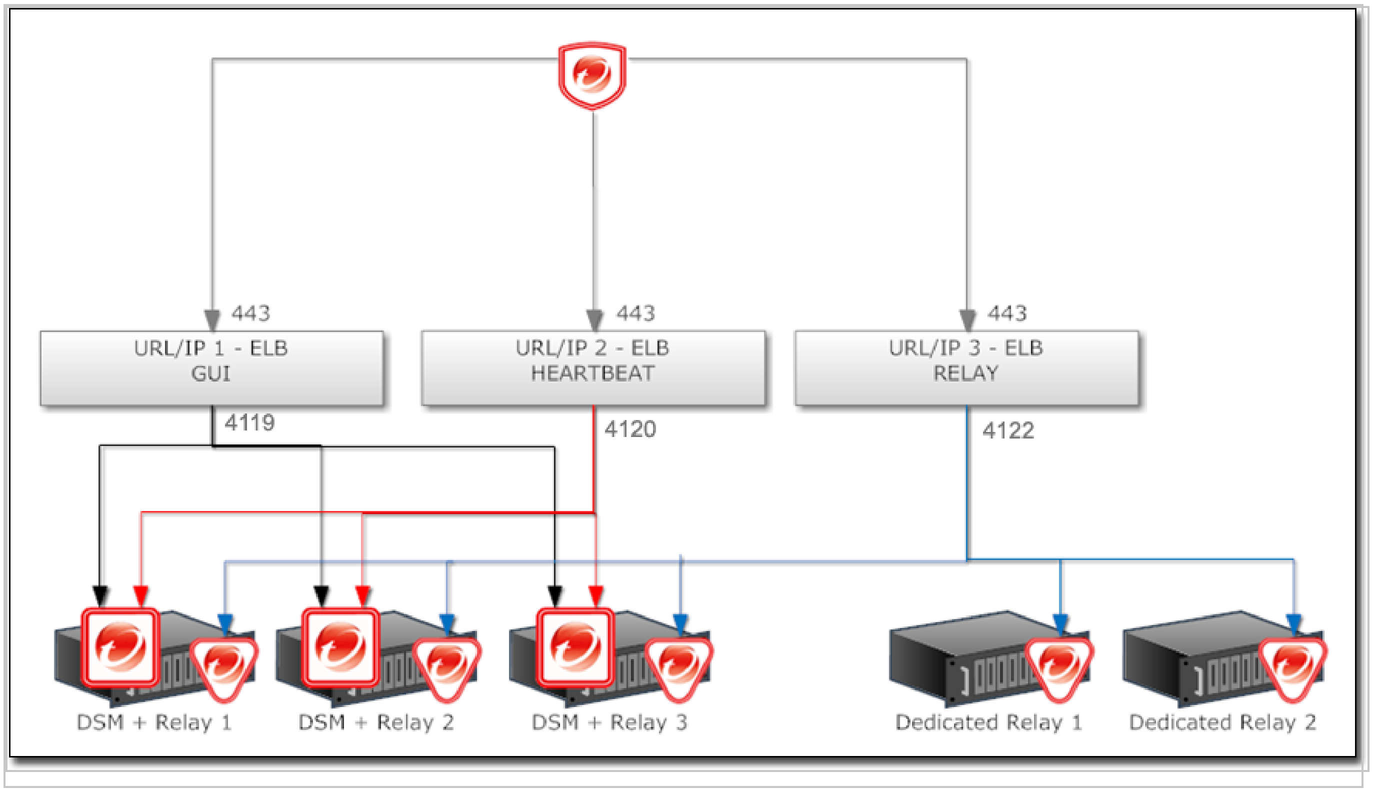
Balance load based upon TCP connections; do not use SSL termination. This ensures that an entire connection occurs with the same manager node. The next connection may be distributed to a different node.

For more Deep Security Manager deployment recommendations, see the "Deep Security Best Practice Guide" on page 1733.

## Configure the load balancer in Deep Security

By default, a multi-node manager gives the address of all nodes to all agents and virtual appliances. The agents and virtual appliances randomly select a node from the list when they try to connect. If they cannot, then they try another node on the list, continuing this process until either a connection succeeds, or no nodes can be reached. If they can't reach any node, then they wait until the next heartbeat to try again.

Each time a node is added or removed, an updated list is sent to all agents and virtual appliances. Until then, connections to old nodes may fail, and the new node will be unused. This causes slow communications and increased network traffic. To avoid this, instead configure agents and virtual appliances to connect via the load balancer's address.



## Add a node

1. "Set up a load balancer" on the previous page.
2. After you have installed Deep Security Manager on one server node, deploy another Deep Security Manager VM in Azure. Make sure you follow the guidelines below.
   - Install the same version of the manager on all nodes.
   - Never launch more than one Deep Security Manager VM at the same time. Doing so can lead to unpredictable results including corruption of the database.
   - Connect all nodes to the same database.
   - Make sure all nodes use the same master key (if configured).
   - Have the master key always available so that all nodes can decrypt and read the encrypted configuration properties and personal data when required. For more information, see masterkey.
   - If the installer shows a **Master Key** page with the following text: **Type the local secret used to access the master key. All nodes that belong to the same Deep Security Manager must be configured with the same local secret.** On this page, enter the secret that you specified when you set up the first node.

- Set the system clock of each manager node to use the same time zone. The database must also use the same time zone. If the time zone is different, this causes Manager Time Out of Sync errors.

## Remove a node

Before you remove or replace a server, you should remove it from the pool of Deep Security Manager nodes.

1. Halt the service or uninstall Deep Security Manager on the node that you want to remove.

   Its status must change to "Offline".

2. Log into Deep Security Manager on another node.
3. Go to **Administration > Manager Nodes**.
4. Double-click the node that you want to remove.

   The node's Properties window should appear.

5. In the **Options** area, click **Decommission**.

## Upgrade a node

Follow the instructions in "Upgrade Deep Security Manager VM for Azure Marketplace" on page 1549 for details on upgrading manager nodes.

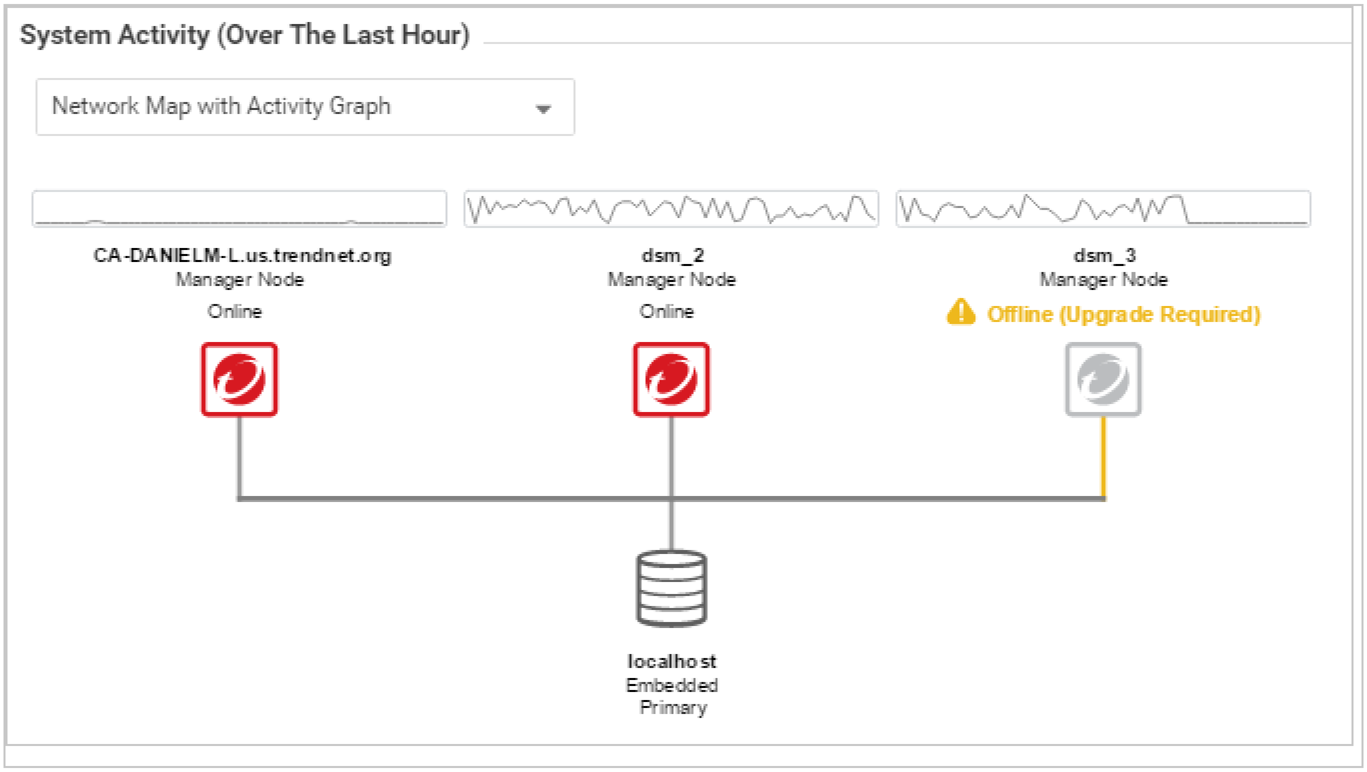
## Viewing node statuses

To display all Deep Security Manager nodes along with their status, combined activity, and jobs being processed, go to **Administration > System Information**. From the drop-down menu, select which graph you want to view.

### Network Map with Activity Graph

The **Network Map with Activity Graph** in the **System Activity** area displays a map of all installed manager nodes and their current status as well their relative activity over the last hour. The nodes can be in the following states:

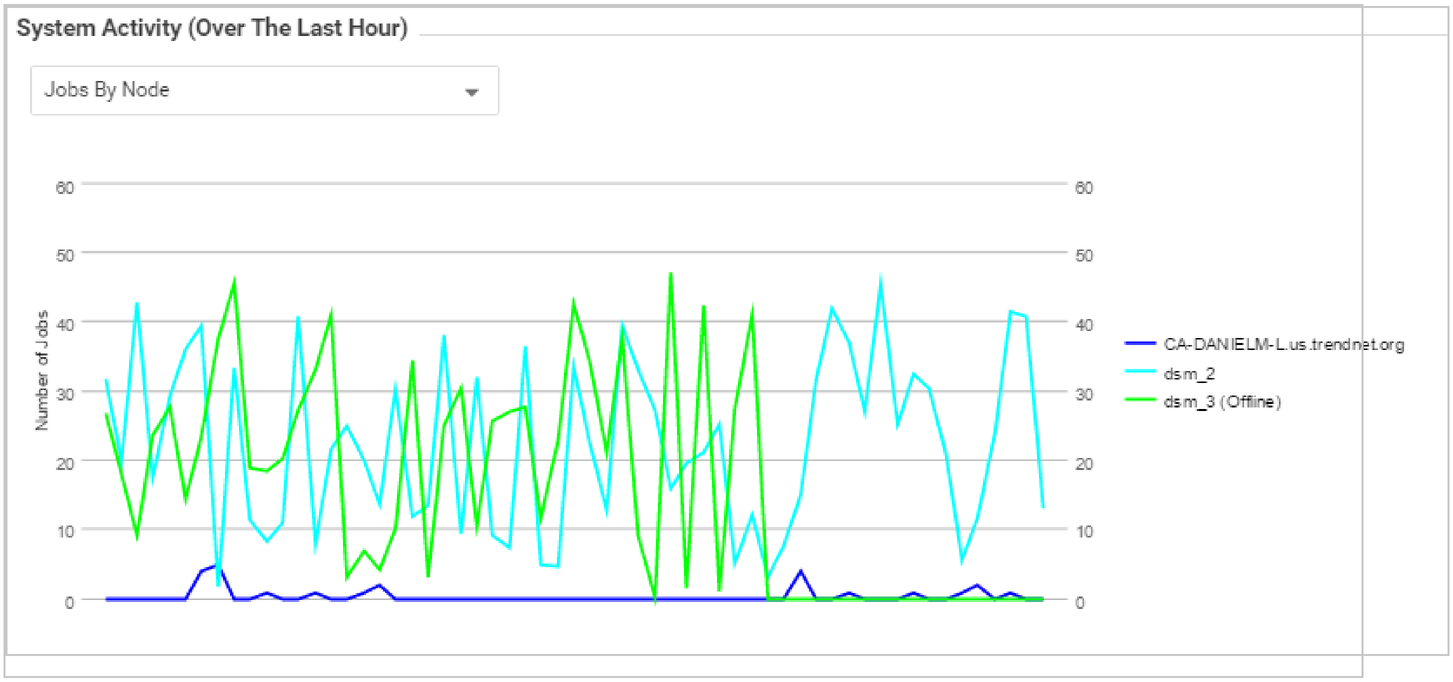
- **Online**
- **Offline**
- **Offline (Upgrade Required)**


System Activity (Over The Last Hour)
Network Map with Activity Graph
CA-DANIELM-L.us.trendnet.org
Manager Node
Online
dsm_2
Manager Node
Online
dsm_3
Manager Node
Offline (Upgrade Required)
localhost
Embedded
Primary

**Note:** All Deep Security Manager nodes periodically check the health of all other nodes. If any manager node loses network connectivity for more than 3 minutes, it is considered offline. The remaining nodes assume its tasks.

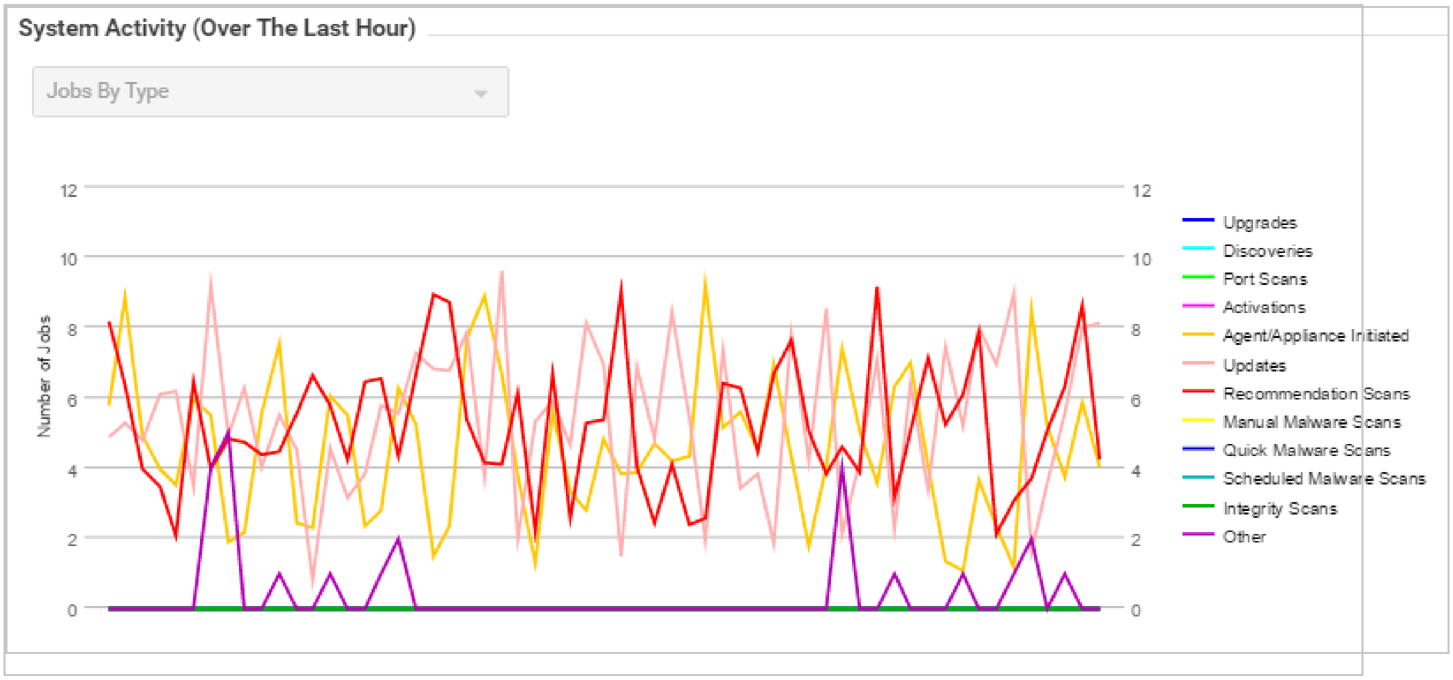
### Jobs by Node

This chart displays the number of jobs carried out over the last hour by each node.


System Activity (Over The Last Hour)
Jobs By Node
Number of Jobs
60
50
40
30
20
10
0
CA-DANIELM-L.us.trendnet.org
dsm_2
dsm_3 (Offline)

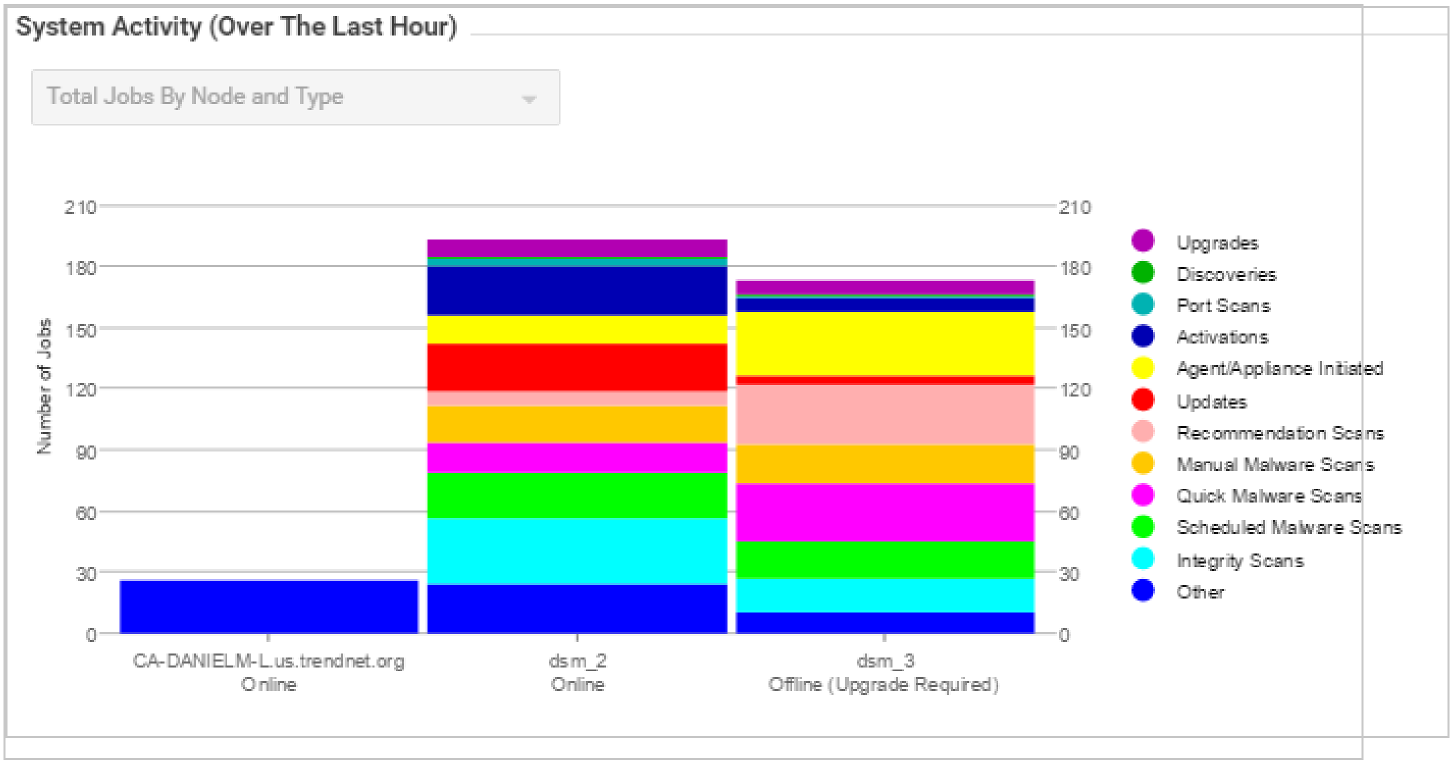
### Jobs by Type

This chart displays the jobs carried out over the last hour by type.



## Total jobs by node and type

This chart displays the number of job types for each node over the last hour.



## View active Deep Security Manager nodes

To display a list of all active Deep Security Manager nodes, go to **Administration > Manager Nodes** . See also "Install Deep Security Manager on multiple nodes" on page 511.

To display details about one of the manager nodes, double-click its row in the list. The Properties window displays the following:

- **Hostname:** The hostname of the computer on which Deep Security Manager is installed.
- **Description:** A description of the manager node.
- **Performance Profile:** Deep Security Manager's performance can be affected by several factors including number of CPUs, available bandwidth, and database responsiveness. The manager's default performance settings are designed to be suited for most installation environments. However, if you experience performance issues, your support provider may suggest that you change the performance profile assigned to one or more of your Deep Security Manager nodes; you should not change these settings without first consulting your support provider.

**Note:** The Simultaneous Endpoint Disk and Network Jobs operation listed in the following tables includes anti-malware scans, integrity monitoring scans, reconnaissance scans, sending policy updates to computers, and distributing security updates.

- **Aggressive**: This performance profile is optimized for installations where Deep Security Manager is on a dedicated server. For example, this is how some common concurrent operations could be distributed per manager node using the **Aggressive** performance profile:

| Operation | 2-core system | 8-core system |
|---|---|---|
| Activations | 10 | 20 |
| Updates | 25 | 50 |
| Recommendation Scans | 10 | 20 |
| Check Status | 100 | Same (100) |
| Agent- or Appliance-Initiated Heartbeats | 20 Active<br>40 Queued | 50 Active<br>40 Queued |
| Simultaneous Endpoint Disk and Network Jobs | 50 | 50 |
| Simultaneous Endpoint Disk and Network Jobs per ESXi | 3 | 3 |

- **Standard**: This Performance Profile is optimized for installations where Deep Security Manager and the database are on the same computer. For example, this is how some common concurrent operations could be distributed per manager node using the **Standard** performance profile:

| Operation | 2-core system | 8-core system |
|---|---|---|
| Activations | 5 | 10 |
| Updates | 16 | 46 |
| Recommendation Scans | 3 | 9 |
| Check Status | 65 | 100 |
| Agent- or Appliance-Initiated Heartbeats | 20 Active<br>40 Queued | 50 Active<br>40 Queued |
| Simultaneous Endpoint Disk and Network Jobs | 50 | 50 |
| Simultaneous Endpoint Disk and Network Jobs per ESXi | 3 | 3 |

- **Unlimited Agent Disk and Network Usage**: This setting is identical to **Aggressive**, but has no limit on computer disk and network usage operations.

| Operation | 2-core system | 8-core system |
|---|---|---|
| Activations | 10 | 20 |
| Updates | 25 | 50 |
| Recommendation Scans | 10 | 20 |
| Check Status | 100 | Same (100) |
| Agent- or Appliance-Initiated Heartbeats | 20 Active | 50 Active |

| Operation | 2-core system | 8-core system |
|---|---|---|
| | 40 Queued | 40 Queued |
| Simultaneous Endpoint Disk and Network Jobs | Unlimited | Unlimited |
| Simultaneous Endpoint Disk and Network Jobs per ESXi | Unlimited | Unlimited |

- **Higher Capacity**: This setting has higher capacity than **Aggressive** or **Unlimited Agent Disk and Network Usage**, as it can consume more jobs simultaneously. With this performance profile, larger memory usage is predictable. If necessary, you can increase memory or JVM size.

| Operation | 2-core system | 8-core system |
|---|---|---|
| Activations | 15 | 45 |
| Updates | 39 | 114 |
| Recommendation Scans | 15 | 45 |
| Check Status | 259 | Same (259) |
| Agent- or Appliance-Initiated Heartbeats | 20 Active<br>40 Queued | 50 Active<br>40 Queued |
| Simultaneous Endpoint Disk and Network Jobs | 100 | 100 |
| Simultaneous Endpoint Disk and Network Jobs per ESXi | 3 | 3 |

All performance profiles limit the number of concurrent component updates to 100 per relay group.

- **Status**: Indicates the node's online and active status from the perspective of the Deep Security Manager node in which you are currently logged in.
- **Options**: You may decommission a manager node. The node must be offline (uninstalled or service halted) to be decommissioned.

# Deploy Deep Security Relay

A Deep Security Relay is an agent that is configured to redistribute Deep Security software and security updates to other agents. This helps your deployment scale.

You need at least one relay in your environment, and it might already be installed if you co-deployed it with Deep Security Manager. To check:

1. Log in to Deep Security Manager.
2. Click **Administration** at the top.
3. Click **Relay Management** on the left navigation pane.
4. If you see a relay icon ( ) in the main pane, a relay is already deployed.

To deploy your first relay:

1. Make sure the relay computer meets the requirements. See "Deep Security Agent sizing and resource consumption" on page 470 and "Deep Security Relay requirements" on page 388.
2. Make sure you allow inbound and outbound communication to and from the relay on the appropriate port numbers. See "Deep Security port numbers" on page 478.
3. If the relay must connect through a proxy, see "Connect to the Primary Security Update Source via proxy" on page 1336.
4. Deploy an agent on the chosen computer. See "Get Deep Security Agent software" below and "Install the agent" on page 548.
5. Enable the agent as a relay:
   a. Log in to Deep Security Manager.
   b. Click **Administration** at the top.
   c. Click **Relay Management** in the left navigation pane.
   d. If you are using Linux, before enabling the relay, create a user **nobody** and a relay group **nogroup**.
   e. Select the relay group into which the relay will be placed. If a relay group does not exist, create one. If you are using Linux, create a user **nobody** and a relay group **nogroup**.
   f. Click **Add Relay**.
   g. In **Available Computers**, select the agent you just deployed.
   h. Click **Enable Relay and Add to Group**.

   The agent is enabled as a relay and is displayed with a relay icon ( ).

**Note:** Trend Micro recommends using more than one relay. This can be set up after you get your basic Deep Security deployment running. For details, see "Deploy additional relays" on page 1345.

# Deploy Deep Security Agent

## Get Deep Security Agent software

To install Deep Security Agent, you must download the agent installer and load packages for the agent's protection modules into Deep Security Manager.

**Warning:** Even if you use a third party deployment system, you must import all installed Deep Security Agent software into the Deep Security Manager's database. When a Deep Security

Agent is first activated, it only installs protection modules that are currently enabled in the security policy. If you enable a new protection module later, Deep Security Agent will try to download its plug-in from Deep Security Manager. If that software is missing, the agent may not be able to install the protection module.

In this topic:

- "View agent software available for download" below
- "View a list of imported agent software" on the next page
- "Import agent software" on the next page
- "Export the agent installer" on page 524
- "Solaris-version-to-agent-package mapping table" on page 525
- "AIX agent package naming format" on page 525
- "Delete a software package from the Deep Security database" on page 526

## View agent software available for download

To view a complete list of software available for import into Deep Security Manager, you can start from Deep Security Manager or you can start from the Help Center.

To start from Deep Security Manager:

1. In Deep Security Manager, go to **Administration > Updates > Software > Download Center**.
2. Optionally, organize the list of software by version or platform by selecting **Version** or **Platform** from the list at the top.
3. Optionally, search the software by entering a search string in the search box in the upper right.

To start from the Help Center:

1. In the Deep Security Help Center, click **Software** on the left. The Deep Security Software page appears.
2. Click the **Major Releases (LTS)** tab for long-term support releases, and **Feature Releases (FR)** tab for feature releases. For details, see "Deep Security 20 release strategy and lifecycle policy" on page 101.

## View a list of imported agent software

To view a list of software that you have imported into Deep Security Manager:

1. In Deep Security Manager, go to **Administration > Updates > Software > Local**. All your imported software appears.
2. Optionally, organize the list of software by version or platform by selecting **Version** or **Platform** from the list at the top.

## Import agent software

Even if you do not use Deep Security Manager to deploy agent updates, you must still import the software into the Deep Security Manager. The following are the import methods:

- "Import agent software directly, from the Download Center" below
- "Import agent software indirectly, from the Help Center" on the next page
- "Import agent software updates automatically" on the next page

### Import agent software directly, from the Download Center

1. Make sure your Deep Security Manager computer has Internet access. If not, see instead "Import agent software indirectly, from the Help Center" on the next page.
2. In Deep Security Manager, go to **Administration > Updates > Software > Download Center**.
3. From the list at the top, select **Platform**.
4. Expand a platform to view the agents available for it.
5. Under the **VERSION** field, look for the version you want and click the import icon. Follow these guidelines:

   - You can select a long-term support (LTS) release or a feature release (FR). For details on LTS and FRs, see "Deep Security 20 release strategy and lifecycle policy" on page 101.
   - If you are trying to import a Solaris agent, see "Solaris-version-to-agent-package mapping table" on page 525 for information on which agent to choose.
   - If you are trying to import an AIX agent, see "AIX agent package naming format" on page 525 for the naming format, which is different depending on the agent version.

   Deep Security Manager connects to the Internet to download the software from Trend Micro Download Center. The manager then checks the digital signature on the software package.

When the manager has finished, a green check mark appears in the **IMPORTED** column for that agent. Software packages now appear on **Administration > Updates > Software > Local**.

If a package cannot be imported, you can try importing it indirectly instead.

## Import agent software indirectly, from the Help Center

If your Deep Security Manager is air-gapped (not connected to the Internet), or if a direct import did not work, you can try importing the agent software indirectly:

1. On a computer that has access to the Internet, go to the Deep Security Help Center.
2. On the left, click **Software**. The **Deep Security Software** page appears.
3. Download the software ZIP you want. For details on long-term support (LTS) releases and feature releases, see "Deep Security 20 release strategy and lifecycle policy" on page 101.
4. Move the software ZIP to the Deep Security Manager computer.
5. In Deep Security Manager, go to **Administration > Updates > Software > Local**.
6. In the main pane, click **Import** to import the ZIP file. The manager checks the digital signature on the ZIP file, and if it is valid, allows the import to proceed.

## Import agent software updates automatically

You can have Deep Security Manager look for newer software on the Download Center and import it to your local inventory automatically. Deep Security Manager only imports updates to already-imported software.

An update is a build in which only the last set of numbers changes. For example, if you already imported agent version 12.0.0.111, then the following versions would be imported automatically because they are update builds of 12.0.0.111:

12.0.0.112
12.0.0.113
12.0.0.123

However, the following versions would not be imported automatically:

12.1.0.222
11.0.0.333
10.0.0.111

To have Deep Security Manager automatically import agent update builds to your local inventory:

1. In Deep Security Manager, go to **Administration > System Settings > Updates**.
2. Select **Automatically download updates to imported software**.
3. Click **Save**.

   Note that setting imports the software to Deep Security Manager but does *not* automatically update your agent software. Continue with "Upgrade Deep Security Agent" on page 1542.

## Export the agent installer

You can download the agent installer from Deep Security Manager as follows:

1. In Deep Security Manager, go to **Administration > Updates > Software > Local**.
2. Select your agent from the list. If you have imported multiple versions of the same agent, the latest version of the software has a green check mark in the **Is Latest** column.

   If you are looking for a Solaris agent, see "Solaris-version-to-agent-package mapping table" on the next page for information on which agent to choose.

3. Click **Export > Export Installer**.

   The manager then checks the digital signature on the software package. If the signature is valid, the export proceeds.

4. Save the agent installer. If you are planning to install the agent manually, save it on the computer where you want to install Deep Security Agent.

To install Deep Security Agent, only use the exported agent installer (the `.msi`, `.rpm`, `.pkg`, `.p5p`, or `.bff` file depending on the platform) as opposed to the full agent ZIP package. If you run the agent installer from the same folder that holds the other zipped agent components, all protection modules will be installed, even if you have not enabled them on the computer. This consumes extra disk space. For comparison, if you use the `.msi`, `.rpm`, `.pkg`, `.p5p`, or `.bff` file, the agent will download and install protection modules only if your configuration requires them.

Installing an agent, activating it, and applying protection with a security policy can be done using a command-line script. For more information, see "Use deployment scripts to add and protect computers" on page 1623.

You can generate deployment scripts to automate the agent installation using the Deep Security API. For more information, see Generate an agent deployment script.

## Solaris-version-to-agent-package mapping table

If you are not sure which agent package to pick when importing and exporting the agent, review the following mapping table.

### Solaris-version-to-agent-package mapping table

| If you're installing the agent on | Choose this agent package | Help Center option |
|---|---|---|
| Solaris 10 Updates 4-6 (64-bit, SPARC or x86) | Agent-Solaris_5.10_U5-xx.x.x-xxx.<sparc\|.x86_64>.zip | Solaris_5.10_U5 |
| Solaris 10 Updates 7-11 (64-bit, SPARC or x86) | Agent-Solaris_5.10_U7-xx.x.x-xxx.<sparc\|.x86_64>.zip | Solaris_5.10_U7 |
| Solaris 11.0 (1111)-11.3 (64-bit, SPARC or x86) | Agent-Solaris_5.11-xx.x.x-xxx.<sparc\|.x86_64>.zip | Solaris_5.11 |
| Solaris 11.4 (64-bit, SPARC or x86) | Agent-Solaris_5.11_U4-xx.x.x-xxx.<sparc\|.x86_64>.zip | Solaris_5.11_U4 |

Note the following:

- The **Help Center option** column shows you which option to select from the **Agent** list on the Help Center's 'Deep Security Software' page, if that is how you have chosen to obtain the package.
- `xx.x.x.xxx` is the build number of the agent. For example, `12.0.0-682`
- `<sparc|.x86_64>` is one of `sparc` or `.x86_64`, depending on the Solaris processor.

## AIX agent package naming format

The naming format is different depending on the agent version:

- Deep Security Agent 12 for AIX: `Agent-AIX-<agent_release>-<agent_build>.powerpc.zip`. For example, `Agent-AIX-12.0.0-1234.powerpc.zip`.
- Deep Security Agent 9.0 for AIX: `Agent-AIX_<AIX_version>-<agent_release>-<build>.powerpc.bff.gz.zip`. For example, `Agent-AIX_5.3-9.0.0-5625.powerpc.bff.gz.zip`.

For details on which agent you need for the version of AIX you are using, see "Agent platform compatibility" on page 389.

## Delete a software package from the Deep Security database

To save disk space, Deep Security Manager periodically removes unused packages from the Deep Security database. To configure the maximum number of old packages kept, go to **System Settings > Storage**.

> **Note:** Deep Security Virtual Appliance uses the same protection modules as Deep Security Agent for 64-bit Red Hat Enterprise Linux. Therefore, if you have an activated Deep Security Virtual Appliance and try to delete the 64-bit Red Hat Enterprise Linux Agent software package from the database, an error message will notify you that the software is in use.

There are two types of packages that can be deleted:

- agent
- kernel support

### Deleting agent packages in single-tenancy mode

In single-tenancy mode, Deep Security automatically deletes agent packages (Agent-*platform-version*.zip) that are not currently being used by agents. Alternatively, you can manually delete unused agent packages. Only unused software packages can be deleted.

For the Windows and Linux agent packages, only the currently used package (whose version is the same as the agent installer) cannot be deleted.

### Deleting agent packages in multi-tenancy mode

In multi-tenancy mode, unused agent packages (Agent-*platform-version*.zip) are not deleted automatically. For privacy reasons, Deep Security cannot determine if software is currently in use by your tenants, even though you and your tenants share the same software repository in the Deep Security database. As the primary tenant, Deep Security does not prevent you from deleting software that is not currently running on any of your own account's computers, but before deleting a software package, ensure that no other tenants are using it.

### Deleting kernel support packages

In both single and multi-tenancy mode, Deep Security automatically deletes unused kernel support packages (KernelSupport-*platform*-*version*.zip). A kernel support package can be deleted if both of these conditions are met:

- No agent package has the same group identifier.
- Another kernel support package has the same group identifier and a later build number.

You can also manually delete unused kernel support packages. For Linux kernel support packages, only the latest one cannot be deleted.

## Configure Linux Secure Boot for agents

Some versions of Deep Security Agent for Linux are compatible with Unified Extensible Firmware Interface (UEFI) Secure Boot.

When Secure Boot is enabled, the computer's Linux kernel checks the PKI signature of each kernel module before it is loaded. It does not load unsigned kernel modules, nor modules with invalid signatures. The following Deep Security Agent features install kernel modules:

- Anti-Malware
- Web Reputation
- Firewall
- Integrity Monitoring
- Intrusion Prevention
- Application Control

To use those features with Secure Boot, you must enroll the public keys from Trend Micro into the computer's firmware to enable validating of these kernel module signatures.

Methods vary by platform:

- Enroll a Secure Boot key for AWS
- Enroll a Secure Boot key for Google Cloud Platform
- Enroll a Secure Boot key for VMware vSphere
- Enroll a Secure Boot key for physical computers

- Enroll a Secure Boot key for Oracle Linux
- Enroll a Secure Boot key for Azure

## Download the Trend Micro public keys

Before you enroll them on Secure Boot computers, you must first download the Trend Micro public keys to be used to validate kernel module signatures. If you have trouble downloading the key files, right-click and select **Save Link As**.

The public keys are encoded in DER format:

- DS2022.der

  SHA-256 certificate hash: `BB FA 4A B8 3C 61 A0 3F 1D D0 4B A7 A4 51 75 E7 D7 EF D3 C8 4B F3 D9 FE A0 CE AB B9 2A F4 8E 92`

- DS20_V2.der

  SHA-256 certificate hash: `B3 36 43 7B 12 B3 EB 6A 4E 4A 44 62 40 4F 1F BD 21 32 70 77 4C 33 7D 1C 5A 58 7C 99 83 F7 30 C7`

  When the agent is deployed on SuSE 15 with kernels 5.3.18-24.34-default or later, `DS20_v2.der` is required because verification of kernel module signatures has changed.

- DS11_2022.der

  SHA-256 certificate hash: `BB FA 4A B8 3C 61 A0 3F 1D D0 4B A7 A4 51 75 E7 D7 EF D3 C8 4B F3 D9 FE A0 CE AB B9 2A F4 8E 92`

  Note that the old public key for agent version 11 (`DS11.der` with SHA-1 hash `7D 96 56 5C 3A 77 B7 A7 24 49 D5 6A A5 0C 28 AA D7 3B 0B fB`) expired on December 5, 2022. To continue using the agent after this date, you must enroll this new public key. Otherwise an "Engine Offline" error message will appear in the console and the computer will not be protected.

You also must download the intermediate certificate authority (CA) certificates that are required to validate the signing chain on the Trend Micro public keys. The CA certificates are X.509 v3 CRT files encoded in DER format:

- MicWinProPCA2011_2011-10-19.crt

  Microsoft Windows Production PCA 2011

SHA-256 certificate hash: `E8 E9 5F 07 33 A5 5E 8B AD 7B E0 A1 41 3E E2 3C 51 FC EA 64 B3 C8 FA 6A 78 69 35 FD DC C7 19 61`

- MicCorUEFCA2011_2011-06-27.crt

  Microsoft Corporation UEFI CA 2011

  SHA-256 certificate hash: `48 E9 9B 99 1F 57 FC 52 F7 61 49 59 9B FF 0A 58 C4 71 54 22 9B 9F 8D 60 3A C4 0D 35 00 24 85 07`

- MicCorKEKCA2011_2011-06-24.crt

  Microsoft Corporation KEK CA 2011

  SHA-256 certificate hash: `A1 11 7F 51 6A 32 CE FC BA 3F 2D 1A CE 10 A8 79 72 FD 6B BE 8F E0 D0 B9 96 E0 9E 65 D8 02 A5 03`

## Update the Trend Micro public key

You need to update your enrolled public keys for signed Trend Micro kernel modules if any of the following applies:

You upgrade the agent to a later major release

> In every major release of the agent (for example, agent 12.0 and 20.0), Trend Micro refreshes the public keys for Secure Boot kernel module signatures. New kernel module signatures cannot be validated with an old public key. As a result, when you upgrade the agent, you must also enroll the new public key.

The public key has expired

| Agent version | Key | Expiry date | Comment |
|---|---|---|---|
| 20 | DS2022.der | 24-Nov-2031 | A new replacement key is expected to be released one year before the expiry date. |
| | DS20.der | 26-Nov-2024 | DS20.der was replaced by DS2022.der. DS2022.der must have been enrolled prior to the expiry date of DS20.der. |
| | DS20_V2.der | 24-Oct- | |

| Agent version | Key | Expiry date | Comment |
|---|---|---|---|
| | | 2026 | • Required for SUSE 15 kernels after 5.3.18-24.34-default.<br>• DS20_V2.der will be replaced by DS2022.der upon its expiry. Ensure that DS2022.der is enrolled prior to the expiry date of DS20_V2.der. |
| 12 | DS12.der | 26-Nov-2024 | DS12.der was replaced by DS2022.der upon its expiry. DS2022.der must have been enrolled prior to the expiry date of DS12.der. |
| 11 | DS11_2022.der | 24-Nov-2031 | |
| | DS11.der | 05-Dec-2022 | |

For Deep Security Agent 20 to use Secure Boot, it is essential to have DS2022.der and DS20_V2.der keys enrolled.

Linux kernel module signature verification has changed

When you update a Linux kernel, the method that it uses to verify kernel module signatures might change. This may require you to replace the enrolled public keys.

For example, SuSE 15 added EKU code signing verification in kernel version 5.3.18-24.34-default, which required a new public key version `DS20_v2.der`.

**Warning:** If a public key for Secure Boot becomes invalid for any of these reasons, and you do not replace it, then an "Engine Offline" error message might appear in the console and the computer can lose protection.

## Enroll a Secure Boot key for AWS

1. Download the required CA certificates and Trend Micro public keys for Secure Boot.
2. If you do not have a platform key, see the AWS documentation to generate a Secure Boot platform key .

   > **Warning:** Only replace the platform key if you can access the firmware of all devices that are loaded during boot (for example, the GPU). If you cannot update the firmware's signing chain to use your new platform key, then Secure Boot could make the instance permanently unable to boot.

3. Create an EC2 virtual machine instance from a Linux distribution AMI that supports Secure Boot.
4. In the console on that instance, install the Machine Owner Key (MOK) command `mokutil`, `uefivars`, and Python.

   For example, on Red Hat Enterprise Linux, execute the following commands:

   ```
   yum install mokutil
   ```

   ```
   yum install python3
   ```

   ```
   curl -L -o uefivars.zip https://github.com/awslabs/python-uefivars/archive/refs/heads/main.zip
   ```

   ```
   unzip uefivars.zip
   ```

   On Debian or Ubuntu, execute the following commands:

   ```
   sudo apt-get update
   ```

   ```
   sudo apt-get install efitools
   ```

   ```
   sudo apt-get install python3
   ```

   ```
   curl -L -o uefivars.zip https://github.com/awslabs/python-uefivars/archive/refs/heads/main.zip
   ```

   ```
   unzip uefivars.zip
   ```

5. Upload the CA certificates and Trend Micro public keys to the instance.

6. Put each platform key, CA certificate, and Trend Micro public key inside a UEFI signature list (`.esl`) file. Combine them into one file, and then convert it into binary (`.bin`) format.

   For example, depending on which Trend Micro public keys you use, you might enter the following commands:

   ```
   # Convert your platform key into signatures list format
   cert-to-efi-sig-list YOUR_PLATFORM_KEY.crt YOUR_PLATFORM_KEY.esl
   # Convert CA certificates
   sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --
   output MS_CA_KEK.esl MicCorKEKCA2011_2011-06-24.crt
   sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --
   output MS_CA_PROD.esl MicWinProPCA2011_2011-10-19.crt
   sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --
   output MS_CA_UEFI.esl MicCorUEFCA2011_2011-06-27.crt
   # Convert Trend Micro public keys
   sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --
   output TREND_UEFI_db_DS11.esl DS11_2022.der
   sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --
   output TREND_UEFI_db_DS20_v2.esl DS20_v2.der
   sbsiglist --owner 77fa9abd-0359-4d32-bd60-28f4e78f784b --type x509 --
   output TREND_UEFI_db_DS2022.esl DS2022.der
   # Combine CA and vendor public keys into one signatures list
   cat MS_CA_PROD.esl MS_CA_UEFI.esl TREND_UEFI_db_DS11.esl TREND_UEFI_db_
   DS12.esl TREND_UEFI_db_DS20.esl TREND_UEFI_db_DS20_v2.esl TREND_UEFI_
   db_DS2022.esl > ALL_SIGNATURES_db.esl
   cp *.esl /root/
   # Combine all and convert to binary
   ./python-uefivars-main/uefivars.py -i none -o aws -O YOUR_BINARY_
   SIGNING_CHAIN.bin -P ./YOUR_PLATFORM_KEY.esl -K ./MS_CA_KEK.esl --db
   ./ALL_SIGNATURES_db.esl
   ```

where `77fa9abd-0359-4d32-bd60-28f4e78f784b` is the GUID in the `SignatureOwner` field of the Microsoft Corporation KEK CA 2011 certificate.

7. Download the `.bin` file.

8. Create a new EC2 snapshot of the instance.

9. Go to AWS Cloudshell, select **Actions > Files > Upload file**, and then select the binary file.

10. Create a new AMI with the snapshot ID and the `.bin` file that you uploaded.

    For example, you could enter the following command:

    ```
    aws ec2 register-image --name LIFT-UBUNTU20SecureBootX64 --uefi-data
    $(cat YOUR_BINARY_SIGNING_CHAIN.bin) --block-device-mappings
    "DeviceName=/dev/sda1,Ebs= {SnapshotId={{YOUR-SNAPSHOT-
    ID}},DeleteOnTermination=true}" --architecture x86_64 --root-device-
    name /dev/sda1 --virtualization-type hvm --boot-mode uefi
    ```

11. Use the customized image to create a new instance with Secure Boot enabled.

12. Execute the following command to verify that the keys are successfully enrolled in the MOK list:

    ```
    mokutil --db | grep Trend
    ```

    and that the kernel has successfully loaded the Trend Micro public keys:

    ```
    dmesg | grep cert
    ```

## Enroll a Secure Boot key for Google Cloud Platform

1. Download the required CA certificates and Trend Micro public keys for Secure Boot.

2. If you do not have a platform key, see the Google Cloud Platform documentation to generate a platform key.

    > **Warning:** Only replace the platform key if you can access the firmware of all devices that are loaded during boot (for example, the GPU). If you cannot update the firmware's signing chain to use your new platform key, then Secure Boot could make the instance permanently unable to boot.

3. Create customized virtual machine images with the CA certificates and Trend Micro public keys that will be used by Secure Boot:

   For example, enter the following command:

   ```
   gcloud compute images create [IMAGE_NAME] \
   --source-image=[SOURCE_IMAGE] \
   --source-image-project=[SOURCE_PROJECT] \
   --platform-key-file=YOUR_PLATFORM_KEY.der \
   --signature-database-file=./MicCorUEFCA2011_2011-06-
   27.crt,./MicWinProPCA2011_2011-10-19.crt,./DS2022.der,./DS20_
   v2.der,./DS11_2022.der[,OTHER_EXISTING_KEYS] \
   --guest-os-features=UEFI_COMPATIBLE
   ```

   Public keys must be in DER or BIN format. Separate each with a comma ( `,` ). For details on command usage and the API, see the Google Cloud Platform documentation.

   You must include all existing Secure Boot keys when you enter this command, as it overwrites all existing keys. If you do not include them, they will be deleted and their kernel modules will not load.

4. Use the customized image to create new virtual machine instances with Secure Boot enabled.

5. Execute the following command to verify that the keys are successfully enrolled:

   ```
   grep 'Trend' /proc/keys
   ```

## Enroll a Secure Boot key for VMware vSphere platform

Follow these steps to enroll a Secure Boot key for the VMware vSphere virtualization platform, unless the computer uses the release earlier than the Unbreakable Enterprise Kernel Release 6 Update 3 (UEK R6U3) for Oracle Linux:

1. Download the required CA certificates and Trend Micro public keys for Secure Boot.

2. On the computer where Secure Boot will be enabled, install the Machine Owner Key (MOK) command `mokutil`.

   For example, on Red Hat Enterprise Linux, enter the following command:

```
yum install mokutil
```

On Debian or Ubuntu, enter the following command:

```
sudo apt-get update
```

```
sudo apt-get install efitools
```

3. Add the Trend Micro public keys to the MOK list, separating multiple keys with a space (if applicable). The following example shows the command to execute if Deep Security Agent version earlier than 20.0.0.7119 is used:

   ```
   mokutil --import /opt/ds_agent/DS2022.der /opt/ds_agent/DS20_v2.der
   ```

   The following example shows the command to execute if Deep Security Agent version 20.0.0.7119 or later is used:

   ```
   mokutil --import /opt/ds_agent/secureboot/DS2022.der /opt/ds_
   agent/secureboot/DS20_v2.der
   ```

   When prompted, enter a password that you will use later.

4. Reboot the computer.
5. When the Shim UEFI key management console opens, press any key to continue.
6. On the Perform MOK Management screen, select Enroll MOK.
7. Select View key X if you need to verify the details of the public keys. Press any key to return to the Enroll MOK screen.
8. Select Continue on the Enroll the key(s)? screen.
9. Select Yes, and then enter the password that you entered earlier.
10. On the The system must now be rebooted screen, select OK.
11. Verify that the keys are successfully enrolled in the MOK list:
    - For most Linux distributions, enter the following command:

      ```
      mokutil --test-key /opt/ds_agent/${certificate_file}.der
      ```

- For Debian Linux 11, 12, or 13 enter the following command:

  ```
  keyctl show %:.platform | grep 'Trend'
  ```

## Enroll a Secure Boot key for physical computers

Follow these steps to enroll a Secure Boot key for a physical computer, unless it uses the release earlier than the Unbreakable Enterprise Kernel Release 6 Update 3 (UEK R6U3) for Oracle Linux:

1. Download the required CA certificates and Trend Micro public keys for Secure Boot.
2. If you do not have a platform key, see your Linux distribution's documentation to generate a Secure Boot platform key.

   > **Warning:** Only replace the platform key if you can access the firmware of all devices that are loaded during boot (for example, the GPU). If you cannot update the firmware's signing chain to use your new platform key, then Secure Boot could make the instance permanently unable to boot.

3. On the computer where Secure Boot will be enabled, install the Machine Owner Key (MOK) command `mokutil`.

   For example, on Red Hat Enterprise Linux, enter the following command:

   ```
   yum install mokutil
   ```

   On Debian or Ubuntu, enter the following command:

   ```
   sudo apt-get update
   ```

   ```
   sudo apt-get install efitools
   ```

4. Add the Trend Micro public keys to the MOK list, separating multiple keys with a space (if applicable). The following example shows the command to execute if Deep Security Agent version earlier than 20.0.0.7119 is used:

   ```
   mokutil --import /opt/ds_agent/DS2022.der /opt/ds_agent/DS20_v2.der
   ```

   The following example shows the command to execute if Deep Security Agent version 20.0.0.7119 or later is used:

```
mokutil --import /opt/ds_agent/secureboot/DS2022.der /opt/ds_agent/secureboot/DS20_v2.der
```

When prompted, enter a password that you will use later.

5. Reboot the computer.
6. When the Shim UEFI key management console opens, press any key to continue.
7. On the Perform MOK Management screen, select Enroll MOK.
8. Select View key X if you need to verify the details of the public keys. Press any key to return to the Enroll MOK screen.
9. Select Continue on the Enroll the key(s)? screen.
10. Select Yes, and then enter the password that you entered earlier.
11. On the The system must now be rebooted screen, select OK.
12. Verify that the keys are successfully enrolled in the MOK list:
    - For most Linux distributions, enter the following command:

      ```
      mokutil --test-key /opt/ds_agent/${certificate_file}.der
      ```

    - For Debian Linux 11, 12, or 13 enter the following command:

      ```
      keyctl show %:.platform | grep 'Trend'
      ```

## Enroll a Secure Boot key for Oracle Linux

On the releases earlier than the Unbreakable Enterprise Kernel Release 6 Update 3 (UEK R6U3) for Oracle Linux, Secure Boot requires slightly different procedure. With UEK, the kernel only trusts keys that are in the built-in keyring. Therefore, the kernel must be recompiled with the Trend Micro public keys, and since that changes the kernel itself, you must also sign the new kernel boot image.

1. Download the required CA certificates and Trend Micro public keys for Secure Boot.
2. Follow the Oracle Linux documentation for Signing Kernel Images and Kernel Modules for Use With Secure Boot.

3. When you reach the step for Insert the Module Certificate in the Kernel Image, replace `pubkey.der` with the name of your Trend Micro public key. For example:

   ```
   sudo /usr/src/kernels/$(uname -r)/scripts/insert-sys-cert -s
   /boot/System.map$(uname -r) -z /boot/vmlinuz$(uname -r) -c ./DS20_
   v2.der
   ```

4. Continue with the remaining steps to sign the kernel boot image.

5. Execute the following command to verify that the key is listed in the `builtin_trusted_keys` keyring:

   ```
   sudo keyctl show %:.builtin_trusted_keys | grep 'Trend'
   ```

## Enroll a Secure Boot key for Azure

1. Download the required CA certificates and Trend Micro public keys for Secure Boot.

2. Create a generation 2 Azure VM from a Linux distribution image that supports Secure Boot, as follows:

   a. Select a VM image with generation 2 supported.
   b. Navigate to the **Create a virtual machine** page in the Azure portal.
   c. From the **Security type** list, select **Trusted launch virtual machines**.
   d. In **Configure security features**, select **Enable Secure Boot**.

   Skip the preceding procedure if you already have a generation 2 Azure VM for custom image that meets the following criteria:

   - The security type is specified as **Trusted launch virtual machines**.
   - The **Enable Secure Boot** security feature is selected.

3. Ensure that the Azure VM is stopped and note the VM disk name.

4. Execute the `az login` command locally or through the Cloud Shell on Azure.

5. Execute the following script line by line to generate a shared access signatures (SAS) URL:

   ```
   read -p 'Your Subscription ID: ' subscriptionId
   ```

   ```
   read -p 'Your Resource Group Name: ' resourceGroupName
   ```

   ```
   read -p 'Your Disk Name for Exporting: ' diskName
   ```

```
read -p 'Input the Expiry Duration for SAS URL in seconds (for example, 3600): ' sasExpiryDuration
```

```
read -p 'Your Storage Account Name to Hold this VHD file: ' storageAccountName
```

```
read -p 'Your Storage Container Name: ' storageContainerName
```

```
read -p 'Your Storage Account Key: ' storageAccountKey
```

```
read -p 'Your Destination VHD File Name: ' destinationVHDFileName
```

```
az account set --subscription $subscriptionId
```

```
sas=$(az disk grant-access --resource-group $resourceGroupName --name $diskName --duration-in-seconds $sasExpiryDuration --query [accessSas] -o tsv)
```

```
az storage blob copy start --destination-blob $destinationVHDFileName --destination-container $storageContainerName --account-name $storageAccountName --account-key $storageAccountKey --source-uri $sas
```

6. Copy the contents of the following file and save it as `CreateSIGFromOSvhdWithCustomUEFIKey.json`:

```

   {
       "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json",
       "contentVersion": "1.0.0.0",
       "parameters": {
           "galleryName": {
               "defaultValue": "{{ change to custom gallary name for the deployed template }}",
               "type": "String",
               "metadata": {
                   "description": "Name of the gallery"
               }
           },
           "imageDefinitionName": {
               "defaultValue": "{{ change to custom image definition name }}",
               "type": "String",
               "metadata": {
                   "description": "Name of the image definition"
               }
           },
           "versionName": {
               "defaultValue": "{{ change to custom image version
}}",
               "type": "String",
               "metadata": {
                   "description": "Name of the image version"
               }
           },
           "storageAccountName": {
               "defaultValue": "{{ change to custom storage account
name contains the exported OS vhd }}",
               "type": "string",
               "metadata": {
                   "description": "Storage account name containing
the OS vhd"
               }
           },
           "vhdURI": {
               "defaultValue": "{{ change to custom vhd URL of the
exported OS vhd }}",
               "type": "String",
               "metadata": {
                   "description": "OS vhd URL"
               }
           },
           "imagePublisher": {
               "defaultValue": "{{ change to custom image publisher
name }}",
               "type": "String",
               "metadata": {
                   "description": "Publisher name of the image"
               }
           },
           "offer": {
               "defaultValue": "{{ change to custom image offer name
}}",
               "type": "String",
               "metadata": {
                   "description": "Offer of the image"
               }
           },
           "sku": {
               "defaultValue": "{{ change to custom image sku name
}}",
               "type": "String",
               "metadata": {
                   "description": "Sku of the image"
               }
           },
           "osType": {
               "defaultValue": "Linux",
               "allowedValues": [
                   "Windows",
                   "Linux"
               ],
               "type": "String",
               "metadata": {
                   "description": "Operating system type"
               }
           },
           "gallerySecurityType": {
               "defaultValue": "TrustedLaunchSupported",
               "type": "String",
               "allowedValues": [
                   "TrustedLaunchSupported",
                   "TrustedLaunchAndConfidentialVMSupported"
               ],
               "metadata": {
                   "description": "Gallery Image security type"
               }
           },
           "customDBKeyDS20V2": {
```

```
           "defaultValue":
"MIIFyzCCA7OgAwIBAgIJAOqCjczOdriRMA0GCSqGSIb3DQEBCwUAMGsxGjAYBgNVBAoM
EVRyZW5kIE1pY3JvLCBJbmMuMSUwIwYDVQQDDBxUcmVuZCBNaWNybyBEZWVwIFNlY3Vya
XR5IDIwMSYwJAYJKoZIhvcNAQkBFhdjc3VwcG9ydEB0cmVuZG1pY3JvLmNvbTAeFw0yMD
ExMjQwOTIzNTFaFw0yNjEwMjQwOTIzNTFaMGsxGjAYBgNVBAoMEVRyZW5kIE1pY3JvLCB
JbmMuMSUwIwYDVQQDDBxUcmVuZCBNaWNybyBEZWVwIFNlY3VyaXR5IDIwMSYwJAYJKoZI
hvcNAQkBFhdjc3VwcG9ydEB0cmVuZG1pY3JvLmNvbTCCAiIwDQYJKoZIhvcNAQEBBQADg
gIPADCCAgoCggIBAK5e7V+I80gksQSQR74uxAZylIdKaLVqBob/J6Fbca8zt7pdxCLeeb
u6S3yT0DRiaS5UslWO21v9q09cuqd0GoDCCaImNdMpCfTB91OZf9t3gHili0cTUyzkktT
8n4g2/xw2mzoXBrm5PvX2psCFwBFh3FE7Mb5VgeA/Bh8uz7jpV9+7+TjouHQ9DXgV2dID
D2QacvtvaGyFqssNLKoKOnEm6+7o0/Cl/9eIzJT0YKzqS2BFY13ANHVTJieNVrfl9dIu1
XxU7ABQ8LOVI835CAIJGJyYtIhnu2bCei7AGZzPYP7Way7djOvmG+2t+NopIE/RMTknsn
3NQMJtrUi4oJOAwI36z8dMDBASUUCpglK12C9z6vHelNrE4z/tiUFYei2OBsLB/yNP9Hl
oVDq4CMvcrZzwWbUtxmtcbTIW/uU1LOsqV92aHIMA3ZivLvvAPvlr4/8NltTvEy5N/Csx
UxAeC21AbE9OXDyyE/9C+VB16YvrqQIEm5IW1Q0/fmmO6rBwy3Uu+4vZcUkq0QbOji/Xc
Nbu17Cfg5fMuuLKu7kwqtl0JZxhZ0XBNdmhOL+XfwrZbZvCqXIKFZo1QsXsbFIoiOWVak
XDonUTLPLJX5n5/7iIrw7hiUViPvTrkAUSjUm5OIu1p+hkKjGDHehdU4XX2bv9rrLAh3v
IKxQSCTdlAgMBAAGjcjBwMAwGA1UdEwEB/wQCMAAwCwYDVR0PBAQDAgeAMBMGA1UdJQQM
MAoGCCsGAQUFBwMDMB0GA1UdDgQWBBQ50RP6qbc9bEOp0jufVa+TgZWLlzAfBgNVHSMEG
DAWgBQ50RP6qbc9bEOp0jufVa+TgZWLlzANBgkqhkiG9w0BAQsFAAOCAgEAXBhNUgJeKl
B/ZwwsIjJsGXa9IPczWfTklg85hZILCT5Khcxl36zs6AEdtbW5pjV/hN+bV5LD84ZHoAa
76ib4iHdU5nK4Q35AhWFdXMTCjg5bm78lESkyC7vLIjj1ITy2K3k+CgZosDXSe9V77AIN
43+R4wwqbsI/FEuXmLw8UHW1DSQphjzcNGXAdbJVXhGoYLLBpyZ/OSFqhcqWwTtHZukri
vtfix8fAQZ1GvfPZA0NlseXbSh883aERqwgP/etvdkUFuby0P66YTSaGZ4Dc9Q5NB4sJ+
W/GcSz7Tnn2cF/hZor9ErjC+AUD0nvhn0IaJxzcCpz53XjFD8K/XeHVpBP8FqHFCoh7Ro
4WcYBFR+DfoCc9Xq6tovWFZlcokybM7AmYw3DDisclkfMZFmhxi+yZQ6fmN9evVp2g7X/
+w+hHrV38pnpz323186ALqSXShBPqG3HcQRvjdnS1Ve1nS8UKvy+ae+0+TKR9KTD+jQsL
9daW4NfaSaBetFmdnbuNRIlKXscgoSne+Qi3YhtI93BoOnfpxEbWB4sWnSHkDO9iekSa4
2tabtCaY1d1MHxdYtdEBb1Gx5aWl8CmsZoWB0xRrk1NG7S8Mi+ux/2LiOfECkm1mpzaUY
0w4dKfTT7/YeVAm1zgumWX+T0dsDc5Sc3t7AxiLHSmTxtYphFT4c=",
           "type": "String",
           "metadata": {
              "description": "Custom UEFI DB DS20_V2.der in
base64 format"
           }
        },
        "customDBKeyDS2022": {
           "defaultValue":
```

```
"MIIFzzCCA7egAwIBAgIJAIfzdTk2xdt2MA0GCSqGSIb3DQEBCwUAMG0xGjAYBgNVBAoM
EVRyZW5kIE1pY3JvLCBJbmMuMScwJQYDVQQDDB5UcmVuZCBNaWNybyBEZWVwIFNlY3Vya
XR5IDIwMjIxJjAkBgkqhkiG9w0BCQEWF2NzdXBwb3J0QHRyZW5kbWljcm8uY29tMB4XDT
IxMTEyNjA2MzI0OVoXDTMxMTEyNDA2MzI0OVowbTEaMBgGA1UECgwRVHJlbmQgTWljcm8
sIEluYy4xJzAlBgNVBAMMHlRyZW5kIE1pY3JvIERlZXAgU2VjdXJpdHkgMjAyMjEmMCQG
CSqGSIb3DQEJARYXY3N1cHBvcnRAdHJlbmRtaWNyby5jb20wggIiMA0GCSqGSIb3DQEBA
QUAA4ICDwAwggIKAoICAQCWb6JAyvw0PoMfHEMoBtj3hsRS8q5TPFoa6vDrAOcJZf0MTw
3NZjlbnNzVP/Ri4J5DGpOWDXLte0ngugtdAG+w3y8UY8K2agEq1ehGIB3iUz45zPqDiQW
s/huafj96q9FzNlWkLJT+M0E2l0qpNJ9NlyphbQ+cnccm1fHrNOMNtEbm31nW4DVD9VyB
7BFf4NRS2h4FiDjRqUTAREMfk84MReQNEP98kPZLXR3ajE4MTZztYF6INR68nK9Jzig/v
JjMRpMwFp+VkQaFnbiti6hbfRjS/GbCW62aJJCTHEavbyJKKY1+MRG406lYVlpH632iyv
Hfj2ni+B7lLvfi5qag+27mX+rBxlqLGuiwNu0geGv5GTlmDyx2onNWRz1akk5GJUloY2x
G9ak92o6WsnDdJCXlFHytPc0R+FleZ/nNNpyzPYr1V8pqWenk+wpVcA7BsuRHofWYzut9
8GkjGYWXXjsipaDt1V2tTKNexFgzMCUIi/tJGmUe3U6czS4zk3tXiTq2Z3kZvrV59nRWJ
+QEdax0ICNZH6AEqNNajgvcvP9WcZmOtgozNxoJuQrCETMKcPQ+JgLbSAiZU7zLIp1z7X
F358G7Azu/AGFpJ0orSpZ9f2J7f1WQ8CsHUgz9KISw6P7b8j160CCEbLBxcRnORCGSeVp
O5tdKt4a7oil5wwIDAQABo3IwcDAMBgNVHRMBAf8EAjAAMAsGA1UdDwQEAwIHgDATBgNV
HSUEDDAKBggrBgEFBQcDAzAdBgNVHQ4EFgQUnbil6RHtl1sidPNZk/35mq9EaWAwHwYDV
R0jBBgwFoAUnbil6RHtl1sidPNZk/35mq9EaWAwDQYJKoZIhvcNAQELBQADggIBADsauv
VNB9jPnlkOJY48eayLDfDN6JMriDA8Q0s0X9EZtTBMcRSNGIQjtyr4LOCOMNrUGMG2XFK
Ha8S17QYtcFM/2Y+t7aOilSTokWTkwC9jU1XBESH7fV44d/fYEO5yD3LBYw5BIEgSqJg3
9rdWWWOD6N1CGRwH3SZwT1aeDj7+YqCYXIUFR/jUm6SXyenoxIlSkn6Ymf3Pil3Gtnqqx
W1+VfkL6YOa715/3ZxqdWfvf1ArUL0spEtQEm4yHwdCuhPWbIG1RKejSFSLk92B/Rdxqv
YXiCxZ5SLziOLslvW0s48LrQ0TEr/HWhiuJ2Q//NSSCllUYy9f6CwXnW38xml+zZu/I8q
J5smI19JfO77HeRGACNSp2GC/C2mamLb1dSXSDKG6YomcrEFSO9oll/gfi6hwCw5Lx21/
dD2SBjKMnwBYGRvDsovE2BQ26GnzvKQbJZW+kN6s5Gi3L0C56kSLLZUFJUxkKFN2//Qyu
0cMC0oeecr+CYDxAHD2FMf4HGJAAScnk9mcEhxYs+B2IW/nCaRjbYvUg1LdaOR9oCXH14
rh+FJ9DZmR84ia/YArHOJXSX/ziy0ftePgAGqQBmHNIPDA0TSGUYg/P5fcfYTT2bKO6lV
/uXiqmDQuuCm1ietUpaTAJ0kWdDxhDzJem+N1qABRpuT93xbaapiX3199",
               "type": "String",
               "metadata": {
                   "description": "Custom UEFI DB DS2022.der in
base64 format"
               }
           }
       },
       "variables": {
           "linuxSignatureTemplate":
```

```
"MicrosoftUefiCertificateAuthorityTemplate",
            "windowsSignatureTemplate": "MicrosoftWindowsTemplate"
        },
        "resources": [
            {
                "type": "Microsoft.Compute/galleries",
                "apiVersion": "2022-01-03",
                "name": "[parameters('galleryName')]",
                "location": "[resourceGroup().location]",
                "tags": {
                    "AzSecPackAutoConfigReady": "true"
                },
                "properties": {
                    "identifier": {}
                }
            },
            {
                "type": "Microsoft.Compute/galleries/images",
                "apiVersion": "2022-08-03",
                "name": "[concat(parameters('galleryName'), '/',
parameters('imageDefinitionName'))]",
                "location": "[resourceGroup().location]",
                "dependsOn": [
                    "[resourceId('Microsoft.Compute/galleries',
parameters('galleryName'))]"
                ],
                "tags": {
                    "AzSecPackAutoConfigReady": "true"
                },
                "properties": {
                    "hyperVGeneration": "V2",
                    "architecture": "x64",
                    "osType": "[parameters('osType')]",
                    "osState": "Generalized",
                    "identifier": {
                        "publisher": "[parameters('imagePublisher')]",
                        "offer": "[parameters('offer')]",
                        "sku": "[parameters('sku')]"
```

```
                   },
                   "features": [
                       {
                           "name": "SecurityType",
                           "value": "TrustedLaunchSupported"
                       }
                   ],
                   "recommended": {
                       "vCPUs": {
                           "min": 1,
                           "max": 16
                       },
                       "memory": {
                           "min": 1,
                           "max": 32
                       }
                   }
               }
           },
           {
               "type": "Microsoft.Compute/galleries/images/versions",
               "apiVersion": "2022-08-03",
               "name": "[concat(parameters('galleryName'),
'/',parameters('imageDefinitionName'),'/', parameters
('versionName'))]",
               "location": "[resourceGroup().location]",
               "dependsOn": [
                   "[resourceId('Microsoft.Compute/galleries/images',
parameters('galleryName'), parameters('imageDefinitionName'))]",
                   "[resourceId('Microsoft.Compute/galleries',
parameters('galleryName'))]"
               ],
               "properties": {
                   "publishingProfile": {
                       "targetRegions": [
                           {
                               "name": "[resourceGroup().location]",
                               "regionalReplicaCount": 1
                           }
                       ]
                   },
                   "storageProfile": {
                       "osDiskImage": {
                           "hostCaching": "ReadOnly",
                           "source": {
                               "uri": "[parameters('vhdURI')]",
                               "storageAccountId": "[resourceId
('Microsoft.Storage/storageAccounts', parameters
('storageAccountName'))]"
                           }
                       }
                   },
                   "securityProfile": {
                       "uefiSettings": {
                           "signatureTemplateNames": [
                               "[if(equals(parameters
('osType'),'Linux'), variables('linuxSignatureTemplate'), variables
('windowsSignatureTemplate'))]"
                           ],
                           "additionalSignatures": {
                               "db": [
                                   {
                                       "type": "x509",
                                       "value": [
                                           "[parameters
('customDBKeyDS20')]"
                                       ]
                                   },
                                   {
                                       "type": "x509",
                                       "value": [
                                           "[parameters
('customDBKeyDS20V2')]"
                                       ]
                                   },
                                   {
                                       "type": "x509",
                                       "value": [
                                           "[parameters
('customDBKeyDS2022')]"
                                       ]
                                   }
                               ]
                           }
                       }
                   }
               }
           }
       ]
   }

```

7. Replace the values inside `{{ }}` in the `"parameters"` section of the `CreateSIGFromOSvhdWithCustomUEFIKey.json` file, keeping in mind the following:

   - The preceding `CreateSIGFromOSvhdWithCustomUEFIKey.json` file is an example for custom deployment. DS20_v2.der and DS2022.der have already been filled in by Base64 format.

   - To enroll another public key into the template, use the following command to convert the key to Base64 format, and then add the key to the JSON file:

     ```
     openssl base64 -in <Trend_Micro_public_key> -A
     ```

8. Create a Shared Image Gallery (SIG) image using template deployment by Azure CLI, as follows:

   ```
   az deployment group create --resource-group <resource-group-name> --
   template-file CreateSIGFromOSvhdWithCustomUEFIKey.json
   ```

9. Create an Azure VM by the custom deployment image.

10. Execute the following command to verify that the keys are successfully enrolled in the Machine Owner Key (MOK) list:

    ```
    mokutil --db | grep Trend
    ```

11. Execute the following command to verify that the kernel has loaded the Trend Micro public keys:

```
dmesg | grep cert
```

For more information, see Secure Boot UEFI keys.

# Install the agent

Topics:

- "Install the agent manually" below
- "Install the agent using other methods" on page 554
- "Post-installation tasks" on page 554

## Install the agent manually

Before you begin, make sure you have:

1. Reviewed the agent's system requirements. See "Deep Security Agent requirements" on page 386.
2. Windows only: "Coexistence of Deep Security Agent with Microsoft Defender Antivirus" on page 766
3. Allowed inbound and outbound communication to and from the agent on the appropriate port numbers. See "Deep Security port numbers" on page 478.
4. Imported the agent software into the manager. See "Import agent software" on page 522.
5. Exported the agent software from the manager. See "Export the agent installer" on page 524.

Next, install the agent. Follow the instructions for your platform.

### Install the agent on Windows

1. Copy the agent ZIP to the computer and extract it.
2. Double-click the installation file (.MSI file) to run the installer package.

> **Note:** On Windows Server 2012 R2 Server Core, launch the installer using this command instead: `msiexec /i Agent-Core-Windows-12.x-xxxx.x86_64.msi`

3. At the Welcome screen, click **Next** to begin the installation.
4. **End-User License Agreement:** If you agree to the terms of the license agreement, select **I accept the terms of the license agreement** and click **Next**.
5. **Destination Folder:** Select the location where you would like Deep Security Agent to be installed and click **Next**.
6. **Ready to install Trend Micro Deep Security Agent:** Click **Install** to proceed with the installation.
7. **Completed:** when the installation has completed successfully, click **Finish**.

The Deep Security Agent is now installed and running on this computer, and will start every time the machine boots.

> **Note:** When installing the agent on Windows 2012 Server Core, the notifier will not be included.

> **Note:** During an install, network interfaces will be suspended for a few seconds before being restored. If you are using DHCP, a new request will be generated, potentially resulting in a new IP address for the restored connection.

### Installation on Amazon WorkSpaces

- If you are unable to install Deep Security Agent .msi file due to error code ‘2503’ then you must do one of the following:
  - Edit your C:\Windows\Temp folder and allow the write permission for your user OR
  - Open the command prompt as an administrator and run the .msi file

> **Note:** Amazon has fixed this issue for newly-deployed Amazon WorkSpaces.

### Installation on Windows 2012 Server Core

- Deep Security does not support switching the Windows 2012 server mode between Server Core and Full (GUI) modes after the Deep Security Agent is installed.

- If you are using Server Core mode in a Hyper-V environment, you will need to use Hyper-V Manager to remotely manage the Server Core computer from another computer. When the Server Core computer has the Deep Security Agent installed and Firewall enabled, the Firewall will block the remote management connection. To manage the Server Core computer remotely, turn off the Firewall module.
- Hyper-V provides a migration function used to move a guest VM from one Hyper-V server to another. The Deep Security Firewall module will block the connection between Hyper-V servers, so you will need to turn off the Firewall module to use the migration function.

### Install the agent on Red Hat, Amazon, SUSE, Oracle, Alma, Rocky, Miracle, or Cloud Linux

1. Copy the agent ZIP to the computer and extract it.
2. Install the agent.

```
# sudo rpm -i <package name>
```

```
Preparing... ########################################## [100%]
```

```
1:ds_agent ########################################## [100%]
```

```
Loading ds_filter_im module version ELx.x [ OK ]
```

```
Starting ds_agent: [ OK ]
```

The Deep Security Agent will start automatically upon installation.

### Install the agent on Ubuntu or Debian

1. Copy the agent ZIP to the computer and extract it.

2. Install the agent.

```
sudo dpkg -i <installer deb file>
```

To start, stop, or reset the agent:

Using SysV init scripts:

- Start: : `/etc/init.d/ds_agent start`
- Stop: `/etc/init.d/ds_agent stop`
- Reset: `/etc/init.d/ds_agent reset`
- Restart: `/etc/init.d/ds_agent restart`
- Display status: `svcs -a | grep ds_agent`

Using systemd commands:

- Start: `systemctl start ds_agent`
- Stop: `systemctl stop ds_agent`
- Restart: `systemctl restart ds_agent`
- Display status: `systemctl status ds_agent`

---

## Install the agent on Solaris

> **Note:** The Deep Security Agent installation is only supported in the global zone.

Solaris requires the following libraries to be installed to support Deep Security Agent:

**Solaris 10:** SUNWgccruntime

**Solaris 11.0 - 11.3:** gcc-45-runtime

**Solaris 11.4:** none; gcc-c-runtime version 7.3 is installed by default

1. Copy the agent installer package to the computer where you want to install the agent.
2. Unzip the ZIP file.
3. Unzip the GZ file.

   ```
   gunzip <agent_GZ_file>
   ```

   The agent installer file (P5P or PKG) is now available.

4. Install the agent. Some examples of installation commands are provided below. Alter the commands to suit your Solaris version, Solaris zone, Solaris processor, and Deep Security agent package name.

- On Solaris 11, with one zone, run the following command in the global zone:

  x86: `pkg install -g file:///mnt/Agent-Solaris_5.11-xx.x.x-xxxx.x86_64/Agent-Core-Solaris_5.11-xx.x.x-xxxx.x86_64.p5p pkg:/security/ds-agent`

  SPARC: `pkg install -g file:///mnt/Agent-Solaris_5.11-xx.x.x-xxxx.sparc/Agent-Core-Solaris_5.11-xx.x.x-xxxx.sparc.p5p pkg:/security/ds-agent`

- On Solaris 11, with multiple zones, run the following command in the global zone:

  ```
  mkdir <path>
  ```

  ```
  pkgrepo create <path>
  ```

  ```
  pkgrecv -s file://<path_to_agent_p5p_file> -d <path> '*'
  ```

  ```
  pkg set-publisher -g <path> trendmicro
  ```

  ```
  pkg install pkg://trendmicro/security/ds-agent
  ```

  ```
  pkg unset-publisher trendmicro
  ```

  ```
  rm -rf <path>
  ```

- On Solaris 10, run one of these commands:

  x86: `pkgadd -G -d Agent-Core-Solaris_5.10_Ux-xx.x.x-xxx.x86_64.pkg`

  SPARC: `pkgadd -G -d Agent-Core-Solaris_5.10_Ux-xx.x.x-xxx.sparc.pkg`

To start, stop, or reset the agent:

- Start: `svcadm enable ds_agent`
- Stop: `svcadm disable ds_agent`
- Reset: `/opt/ds_agent/dsa_control -r`
- Restart: `svcadm restart ds_agent`
- Display status: `svcs -a | grep ds_agent`

To uninstall the agent on Solaris 11:

```
pkg uninstall pkg:/security/ds-agent
```

To uninstall the agent on Solaris 10:

```
pkgrm -v ds-agent
```

### Install the agent on AIX

1. Copy the agent ZIP to the computer and extract it. A GZ file becomes available.
2. Move the GZ file to another location.
3. Extract the GZ file using gunzip. A BFF file becomes available. This is the installer file.
4. Copy the BFF file to the AIX computer.
5. Place the BFF file in a temporary folder such as `/tmp`.
6. Install the agent.

   ```
   /tmp> installp -a -d /tmp/<agent_BFF_file_name> ds_agent
   ```

   where `<agent_BFF_file_name>` is replaced with the name of the BFF installer file you extracted.

To start, stop, load, or unload the driver for the agent:

- Start: `startsrc -s ds_agent`
- Stop: `stopsrc -s ds_agent`
- Load the driver: `/opt/ds_agent/ds_fctrl load`
- Unload the driver: `/opt/ds_agent/ds_fctrl unload`

### Install the agent on Red Hat OpenShift

Before you begin:

1. Ensure that you have helm v3 or newer installed.
2. Make sure you have imported the agent software to Deep Security Manager. See "Get Deep Security Agent software" on page 520 for details.
3. Ensure that you have enabled agent-initiated activation (AIA). AIA is required if you want your deployment script to activate the agent after installation. See "Activate and protect agents using agent-initiated activation and communication" on page 1386 for details.

Installing the agent:

1. From the Deep Security console, in the upper right corner, click **Support** > **Deployment Scripts**.
2. Select **OpenShift Agent Deployment**.
3. *(optional)* Select the options for **Security Policy**, **Computer Group**, **Relay Group**, **Proxy to contact Deep Security Manager**, and **Proxy to contact Relay(s)**.
   The deployment script generator displays the script.
4. Do one of the following:
   - Click **Copy to Clipboard** and paste the deployment script in your preferred deployment tool
   - Click **Save to File**.

## Install the agent using other methods

If you don't want to install the agent manually, you can use one of the methods described below.

- **Deployment scripts:** Generate deployment scripts within the manager and use them to install the agent. For details, see "Use deployment scripts to add and protect computers" on page 1623
- **Deep Security API**: Use the API to generate deployment scripts to automate the installation of the agent on a computer. See Use Scripts to Deploy Deep Security Manager and Agent on the Deep Security Automation Center.
- **SCCM:** Use Microsoft System Center Configuration Manager (SCCM) to install an agent, activate it, and apply a policy. To use SCCM, go to **Administration > System Settings > Agents** and enable agent-initiated activation.
- **Template:** Include the agent in your VM template. See "Install the agent on an AMI or WorkSpace bundle" on page 560 and "Install the agent on Azure VMs" on page 564.

## Post-installation tasks

After you install the agent, you must perform the following post-installation tasks, if they were not already completed as part of the installation process:

- "Activate the agent" on page 566
- "Assign a policy to a computer" on page 633

# Install the agent on Amazon EC2 and WorkSpaces

Deep Security Agent only supports Amazon WorkSpaces Windows desktops. There is no support for Linux desktops.

You can protect your existing Amazon EC2 instances and Amazon WorkSpaces with Deep Security as follows:

1. "Add your AWS accounts to Deep Security Manager" below
2. "Set the communication direction" on the next page
3. "Configure the activation type" on the next page
4. "Open ports" on page 557
5. "Deploy agents to your Amazon EC2 instances and WorkSpaces" on page 558
6. "Verify the agent installation and activation" on page 559
7. "Assign a policy" on page 559

If instead you want to launch new Amazon EC2 instances and Amazon WorkSpaces with the agent baked-in, see "Install the agent on an AMI or WorkSpace bundle" on page 560.

To protect Amazon WorkSpaces after already protecting your Amazon EC2 instances, see "Protect Amazon WorkSpaces if you already added your AWS account" on page 591.

## Add your AWS accounts to Deep Security Manager

You need to add your AWS account or accounts to Deep Security Manager. These AWS accounts contain the Amazon EC2 instances and Amazon WorkSpaces that you want to protect with Deep Security.

See "About adding AWS accounts" on page 582 for details.

After adding your AWS accounts:

- Your existing Amazon EC2 instances and Amazon WorkSpaces appear in Deep Security Manager. If no agent is installed on them, they appear with a **Status** of **Unmanaged (Unknown)** and a grey dot next to them. If an agent was already installed, they appear with a **Status** of **Managed (Online)** and green dot next to them.
- Any new Amazon EC2 instances or Amazon WorkSpaces that you launch through AWS under this AWS account are auto-detected by Deep Security Manager and displayed in the list of computers.

## Set the communication direction

You are required to set the communication direction as either agent-initiated, manager-initiated, or bi-directional:

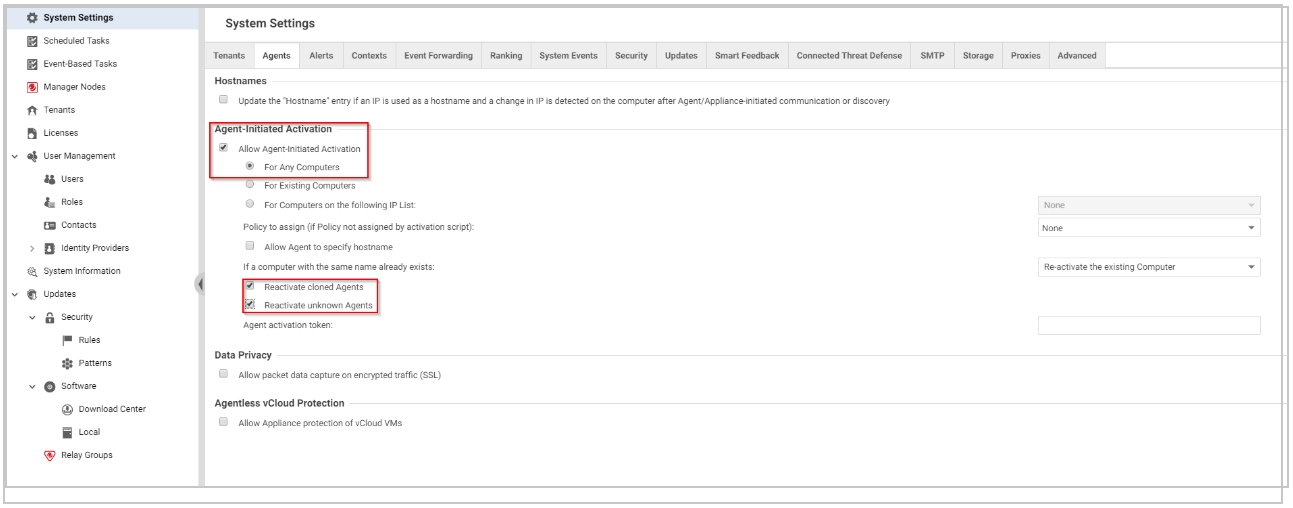
1. Log in to Deep Security Manager.
2. Set the communication direction by following instructions provided in "Configure communication directionality" on page 1375 and considering these guidelines:
   - **Agent/Appliance Initiated** does not require you to open inbound ports on the Amazon EC2 instance or Amazon WorkSpace, while **Bidirectional** and **Manager-Initiated** do.
   - **Agent/Appliance Initiated** is the safest option since no inbound ports need to be opened on the Amazon EC2 instance or Amazon WorkSpace.
3. If you are using Amazon WorkSpaces, and you chose to set the communication direction to **Bidirectional** or **Manager-Initiated**, manually assign an elastic IP address to each WorkSpace before proceeding with further configurations. This gives the WorkSpace a public IP that can be contacted by Deep Security Manager. This is not required for EC2 instances because they already use public IP addresses. WorkSpaces use private IP addresses.

## Configure the activation type

Activation is the process of registering an agent with a manager. You need to indicate whether or not to allow agent-initiated activation. If not, only manager-initiated activation is allowed.

1. Log in to Deep Security Manager.
2. Click **Administration** at the top.
3. On the left, click **System Settings**.
4. Ensure that the **Agents** tab is selected.
5. Select or deselect **Allow Agent-Initiated Activation**, keeping in mind the following:
   - Agent-initiated activation does not require you to open up inbound ports to your Amazon EC2 instances or Amazon WorkSpaces, while manager-initiated activation does.
   - If agent-initiated activation is enabled, manager-initiated activation continues to work.
   - Agent-initiated activation works even if you set the communication direction to **Manager-Initiated**.
6. If you selected **Allow Agent-Initiated Activation**, also select **Reactivate cloned Agents** and **Enable Reactivate unknown Agents**. See "Agent settings" on page 1399 for more information.

7. Click **Save**.
8. If you are using Amazon WorkSpaces, and you did not allow agent-initiated activation, manually assign an elastic IP address to each WorkSpace now, before proceeding with further configurations. This gives each Amazon WorkSpace a public IP that can be contacted by other computers. This is not required for EC2 instances because they already use public IP addresses.



System Settings

Hostnames

□ Update the "Hostname" entry if an IP is used as a hostname and a change in IP is detected on the computer after Agent/Appliance-initiated communication or discovery

Agent-Initiated Activation

☑ Allow Agent-Initiated Activation

● For Any Computers

○ For Existing Computers

○ For Computers on the following IP List: None

Policy to assign (if Policy not assigned by activation script): None

□ Allow Agent to specify hostname

If a computer with the same name already exists: Re-activate the existing Computer

☑ Reactivate cloned Agents

☑ Reactivate unknown Agents

Agent activation token:

Data Privacy

□ Allow packet data capture on encrypted traffic (SSL)

Agentless vCloud Protection

□ Allow Appliance protection of vCloud VMs

# Open ports

You are required to make sure that the necessary ports are open to your Amazon EC2 instances or Amazon WorkSpaces.

1. Open ports to your Amazon EC2 instances, as follows:
   a. Log in to your Amazon Web Services Console.
   b. Go to **EC2 > Network & Security > Security Groups**.
   c. Select the security group that is associated with your EC2 instances, then select **Actions > Edit outbound rules**.
   d. Open the necessary ports. For details, see "Ports to open" below.
2. Open ports to your Amazon WorkSpaces, as follows:
   a. Go to the firewall software that is protecting your Amazon WorkSpaces, and open the ports.

You have now opened the necessary ports so that Deep Security Agent and Deep Security Manager can communicate.

## Ports to open

Typically:

- Agent-to-manager communication requires you to open the outbound TCP port (443 or 80, by default)
- Manager-to-agent communication requires you to open an inbound TCP port (4118).

Specifically:

- If you set the communication direction to **Agent/Appliance-Initiated**, open the outbound TCP port 443 or 80.
- If you set the communication direction to **Manager-Initiated**, open the inbound TCP port 4118.
- If you set the communication direction to **Bidirectional**, open both the outbound TCP port 443 or 80, as well as the inbound TCP port 4118.
- If you enabled **Allow Agent-Initiated Activation**, open the outbound TCP port 443 or 80 regardless of the communication direction.
- If you disabled **Allow Agent-Initiated Activation**, open the inbound TCP port 4118 regardless of the communication direction.

## Deploy agents to your Amazon EC2 instances and WorkSpaces

You are required to deploy agents onto your Amazon EC2 instances and Amazon WorkSpaces by using one of the following options:

1. Use a deployment script to install, activate, and assign a policy.

   This is the best option if you need to deploy agents to many Amazon EC2 instances and Amazon WorkSpaces.

   With this option, you must run a deployment script on the Amazon EC2 instances or Amazon WorkSpaces. The script installs and activates the agent and then assigns a policy. See "Use deployment scripts to add and protect computers" on page 1623 for details.

2. Manually install and activate.

   This is the best option if you only need to deploy agents to a few EC2 instances and Amazon WorkSpaces. You would need to perform the following:

   a. Get the Deep Security Agent software, copy it to the Amazon EC2 instance or Amazon WorkSpace, and then install it. For details, see "Get Deep Security Agent software" on page 520, and "Install the agent" on page 548.

b. Activate the agent. You can do so on the agent (if the agent-initiated activation was enabled) or on Deep Security Manager. For details, see "Activate the agent" on page 566

You have now installed and activated Deep Security Agent on an Amazon EC2 instance or Amazon WorkSpace. A policy may or may not have been assigned, depending on the option you chose. If you chose to use a deployment script, a policy was assigned to the agent during activation. If you chose to manually install and activat the agent, then no policy has been assigned, and you need to assign one.

## Verify the agent installation and activation

You should verify that your agent was installed and activated properly:

1. Log in to Deep Security Manager.
2. Click **Computers** at the top.
3. On the left, make sure your Amazon EC2 instance or Amazon WorkSpace appears under **Computers** > *your_AWS_account* > *your_region* . Look for WorkSpaces in a **WorkSpaces** sub-node.
4. In the main pane, make sure your Amazon EC2 instances or Amazon WorkSpaces appear with a **Status** of **Managed (Online)** and a green dot next to them.

## Assign a policy

Skip this step if you ran a deployment script to install and activate the agent, as the script already assigned a policy so no further action is required.

If you installed and activated the agent manually, you must assign a policy to the agent. Assigning the policy sends the necessary protection modules to the agent so that your computer is protected.

To assign a policy, see "Assign a policy to a computer" on page 633.

After assigning a policy, your Amazon EC2 instance or Amazon WorkSpace is now protected.

# Install the agent on an AMI or WorkSpace bundle

Read this page if you want to launch *new* Amazon EC2 instances and Amazon WorkSpaces with the agent 'baked in'.

If instead you want to:

- protect *existing* Amazon EC2 instances and Amazon WorkSpaces with Deep Security, see "Install the agent on Amazon EC2 and WorkSpaces" on page 555.
- protect Amazon WorkSpaces after already protecting your Amazon EC2 instances, see instead "Protect Amazon WorkSpaces if you already added your AWS account" on page 591.

'Baking the agent' is the process of launching an EC2 instance based on a public AMI, installing the agent on it, and then saving this custom EC2 image as an AMI. This AMI (with the agent 'baked in') can then be selected when launching new Amazon EC2 instances.

Similarly, if you want to deploy the Deep Security Agent on multiple Amazon WorkSpaces, you can create a custom 'WorkSpace bundle' that includes the agent. The custom bundle can then be selected when launching new Amazon WorkSpaces.

To bake an AMI and create a custom WorkSpace bundle with a pre-installed and pre-activated agent, follow these steps:

1. "Add your AWS account to Deep Security Manager" below
2. "Set the communication direction" on the next page
3. "Configure the activation type" on the next page
4. "Launch a 'master' Amazon EC2 instance or Amazon WorkSpace" on the next page
5. "Deploy an agent on the master" on the next page
6. "Verify that the agent was installed and activated properly" on page 562
7. "(Recommended) Set up policy auto-assignment" on page 562
8. "Create an AMI or custom WorkSpace bundle based on the master" on page 563
9. "Use the AMI" on page 563

## Add your AWS account to Deep Security Manager

You'll need to add your AWS accounts to Deep Security Manager. These are the AWS accounts that will contain the Amazon EC2 instances and Amazon WorkSpaces that you want to protect.

See "About adding AWS accounts" on page 582 for details.

## Set the communication direction

You'll need to set the communication direction: either agent-initiated, manager-initiated, or bidirectional.

See "Install the agent on Amazon EC2 and WorkSpaces" on page 555 > "Set the communication direction" on page 556 for instructions.

## Configure the activation type

You'll need to indicate whether you'll allow agent-initiated activation.

See "Install the agent on Amazon EC2 and WorkSpaces" on page 555 > "Configure the activation type" on page 556 for instructions.

## Launch a 'master' Amazon EC2 instance or Amazon WorkSpace

You'll need to launch a 'master' Amazon EC2 instance or Amazon WorkSpace. The master instance is the basis for the EC2 AMI or WorkSpace bundle that you will create later.

1. In AWS, launch an Amazon EC2 instance or Amazon WorkSpace. See the Amazon EC2 documentation and Amazon WorkSpaces documentation for details.
2. Call the instance 'master'.

## Deploy an agent on the master

You'll need to install and activate the agent on the master. During this process, you can optionally install a policy.

See "Install the agent on Amazon EC2 and WorkSpaces" on page 555 > "Deploy agents to your Amazon EC2 instances and WorkSpaces" on page 558 for instructions.

Tip: Ideally, if you bake the agent into your AMI or workspace bundle and then want to use a newer agent later on, you should update the bundle to include the new agent. However, if that's not possible, you can use the **Automatically upgrade agents on activation** setting so when the agent in the AMI or bundle activates itself, Deep Security Manager can automatically upgrade the agent to the latest version. For details, see "Automatically upgrade agents on activation" on page 1388.

## Verify that the agent was installed and activated properly

You should verify that the agent was installed and activated properly on the master before proceeding.

See "Install the agent on Amazon EC2 and WorkSpaces" on page 555 > "Verify the agent installation and activation" on page 559 for instructions.

## (Recommended) Set up policy auto-assignment

You may need to set up policy auto-assignment depending on how you deployed the agent on the master:

- If you used a deployment script, then a policy has already been assigned, and no further action is required.
- If you manually installed and activated the agent, no policy was assigned to the agent, and one should be assigned now so that the master is protected. The Amazon EC2 instances and Amazon WorkSpaces that are launched based on the master will also be protected.

If you want to assign a policy to the master, as well as auto-assign a policy to future EC2 instances and WorkSpaces that are launched using the master, follow these instructions:

1. In Deep Security Manager, create an event-based task with these parameters:
   - Set the **Event** to **Agent-Initiated Activation**.
   - Set **Assign Policy** to the policy you want to assign.
   - (Optional) Set a condition to **Cloud Instance Metadata**, with
     - a **tagKey** of **EC2** and a **tagValue.*** of **True** (for an EC2 instance)
       OR
     - a **tagKey** of **WorkSpaces** and a **tagValue.*** of **True** (for WorkSpaces)

   The above event-based task says:
   *When an agent is activated, assign the specified policy, on condition that* `EC2=true` *or* `WorkSpaces=true` *exists in the Amazon EC2 instance or WorkSpace.*
   If that key/value pair does not exist in the EC2 instance or WorkSpace, then the policy is not assigned (but the agent is still activated). If you do not specify a condition, then the policy is assigned on activation unconditionally.

For details on creating event-based tasks, see "Automatically assign policies using cloud provider tags/labels" on page 1635.

2. If you added a key/value pair in Deep Security Manager in the previous step, do the following:
   a. Go to AWS.
   b. Find your master EC2 instance or WorkSpace.
   c. Add tags to the master with a **Key** of **EC2** or **WorkSpaces** and a **Value** of **True**.
      For details, see this Amazon EC2 documentation on tagging, and this Amazon WorkSpace documentation on tagging.
      You have now set up policy auto-assignment. New Amazon EC2 instances and Amazon WorkSpaces that are launched using the master are activated automatically (since the agent is pre-activated on the master), and then auto-assigned a policy through the event-based task.
3. On the master EC2 instance or WorkSpace, reactivate the agent by re-running the activation command on the agent, or by clicking the **Reactivate** button in Deep Security Manager. For details, see "Activate the agent" on page 566
   The re-activation causes the event-based task to assign the policy to the master. The master is now protected.

You are now ready to bake your AMI or create a custom WorkSpace bundle.

## Create an AMI or custom WorkSpace bundle based on the master

> **Note:** When creating an AMI from AWS, do not select the AWS option **No reboot**. Images created with the **No reboot** option will not be protected by the agent.

- To create an AMI on Linux, see this Amazon documentation.
- To create an AMI on Windows, see this Amazon documentation.
- To create a custom WorkSpace bundle, see this Amazon documentation.

You now have an AMI or WorkSpace bundle that includes a pre-installed and pre-activated agent.

## Use the AMI

Now that you have a custom AMI or WorkSpace bundle, you can use it as the basis for future Amazon EC2 instances and Amazon WorkSpaces. With the custom AMI or bundle, Deep

Security Agent starts up automatically, activates itself, and applies the protection policy assigned to it. It appears in Deep Security Manager with a **Status** of **Managed** and a green dot next to it.

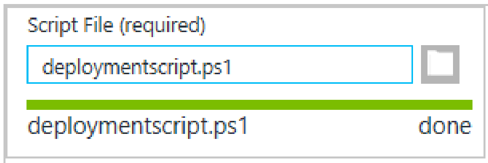
## Install the agent on Azure VMs

To install the agent on VM instances running in the Microsoft Azure cloud, you need to deploy Deep Security Agents to them. You can do this in multiple ways:

- You can generate Deep Security deployment scripts for automatically deploying agents using deployment tools such as RightScale, Chef, Puppet, and SSH. For more information on how to do so, see "Use deployment scripts to add and protect computers" on page 1623.
- You can add a custom script extension to an existing virtual machine to deploy and activate the Deep Security Agent. To do this, navigate to your existing virtual machine in the Azure management portal and follow the steps below to upload and execute the deployment script on your Azure VM.

To add a custom script extension to an existing virtual machine:

1. Log in to the Azure portal.
2. Switch to the preview portal, and then click the virtual machine that you want to add the custom script to.
3. In the **Settings** blade, click **Extensions**, in the **Extensions** blade, click **Add extension**, in the **New Resource** blade, select **Custom Script**, and then click **Create**.
4. In the **Add Extension** blade under **Script File (required)**, click **upload**, select the saved .ps1 deployment script, and then click **OK**.


Script File (required)

deploymentscript.ps1

deploymentscript.ps1 done

## Install the agent on Google Cloud Platform VMs

Read this page if you want to protect existing Google Cloud Platform (GCP) VM instances with Deep Security.

To protect your existing GCP VMs:

1. Add a GCP service account to Deep Security Manager. For instructions, see "Add a Google Cloud Platform account" on page 614.

2. Set the communication direction to **Agent Initiated**. For instructions, see "Configure communication directionality" on page 1375.
3. Configure agent-initiated activation (AIA). For instructions, see "Activate and protect agents using agent-initiated activation and communication" on page 1386.
4. Open ports so that Deep Security components can access your GCP VMs and the GCP API. For information on which ports to open, see "Port numbers, URLs, and IP addresses" on page 478. For instructions on how to open ports, see this GCP webpage.
5. Deploy agents to your GCP VMs. You must use Deep Security Agent *12 or later*.

   To deploy agents, you have two options:

| Option | Use if... | Instructions |
|---|---|---|
| Option 1:<br>Use a deployment script to install, activate, and assign a policy to the agent | You need to deploy many agents to your GCP VMs. | See "Use deployment scripts to add and protect computers" on page 1623 for instructions. |
| Option 2:<br>Manually install and activate the agent | You only need to deploy a few agents. | a. Obtain the Deep Security Agent software, copy it to the GCP VM, and then install it. For details, see "Get Deep Security Agent software" on page 520<br>b. Activate the agent. You can do so on |

| Option | Use if... | Instructions |
|---|---|---|
| | | the agent or on the Deep Security Manager. For details, see "Activate the agent" below |

6. Verify that the agent was installed and activated properly:
   a. Log in to Deep Security Manager.
   b. Click **Computers** at the top.
   c. On the navigation pane on the left, make sure your GCP VM appears under **Computers** > *your_GCP_service_account* > *your_GCP_project* .
   d. In the main pane, make sure your GCP VMs appear with a **Status** of **Managed (Online)** and a green dot next to them.
7. Assign a policy if you installed and activated the agent manually. For instructions, see "Assign a policy to a computer" on page 633. Assigning the policy sends the necessary protection modules to the agent so that your computer is protected.

   **Note:** Skip the policy assignment step if you ran a deployment script to install and activate the agent. The script already assigned a policy so no further action is required.

   After assigning a policy, your GCP VM is now protected.

## Activate the agent

**Tip:** If you haven't already installed the agent, see "Use deployment scripts to add and protect computers" on page 1623 or "Install the agent" on page 548 for instructions.

Before the installed agent can protect its computer or be converted to a relay, you must activate the agent with Deep Security Manager. Activation registers the agent with the manager during an initial communication.

To do this, you can either:

- Activate the agent from the manager. Go to **Computers**, right-click the computer whose agent you want to activate or reactivate and select **Actions > Activate/Reactivate**. (Alternatively, click **Activate** or **Reactivate** in the computer's **Details** window.)
- Activate the agent through a deployment script. See "Use deployment scripts to add and protect computers" on page 1623 for details.
- Activate the agent from the computer where the agent is installed. Run this command:
  `dsa_control -a dsm://<dsm_host_or_IP>:<port>/`
  where:
  `<dsm_host_or_IP>` is replaced with the Deep Security Manager hostname or IP address, and
  `<port>` is replaced with the Deep Security Manager heartbeat port, which is 4120, by default.
  For details on this command, including additional parameters, see "Command-line basics" on page 1565.
- Activate the agent through an event-based task ("Computer Created (by System)" event) to automatically activate computers when they connect to the manager or when the manager syncs with an LDAP directory, cloud account, or vCenter. For more information, see "Automatically perform tasks when a computer is added or changed (event-based tasks)" on page 1603.

Before activation, the agent will have one of these statuses:

- **No Agent:** Indicates one of the following situations:
  - No agent is running or listening on the default port.
  - An agent is installed and running but is working with another manager and communications are configured as agent-initiated. In this case, the agent is not listening for this manager. To correct this situation, deactivate the agent from the computer.
- **Activation Required:** The agent is installed and listening, and is ready to be activated by the manager.
- **Reactivation Required:** The agent is installed and listening and is waiting to be reactivated by the manager.
- **Deactivation Required:** The agent is installed and listening, but has already been activated by another manager.
- **Unknown:** The computer has been imported (as part of an imported Computers list) without state information, or has been added by way of an LDAP directory discovery process.

After a successful activation, the agent state is Online. If the activation failed, the computer status is Activation Failed with the reason for the failure in brackets. Click this link to display the system event for more details on the reason for the activation failure.

> **Note:** Although IPv6 traffic is supported by Deep Security 8.0 and earlier agents, it is blocked by default. To allow IPv6 traffic on Deep Security 8.0 Agents, open a **Computer or Policy editor**[1] and go to **Settings > Advanced > Advanced Network Engine Settings**. Set the **Block IPv6 for 8.0 and Above Agents** option to **No**.

## Deactivate the agent

If you want to transfer control of a computer from one Deep Security Manager installation to another, you must deactivate the agent with its current manager, and then re-activate it with the new manager.

You can normally deactivate the agent from the Deep Security Manager that is currently managing the agent. If the Deep Security Manager cannot communicate with the agent, you may have to perform the deactivation manually. To run the commands below, you must have administrator privileges on the local machine.

**To deactivate the agent on Windows:**

1. From a command line, change to the agent directory (Default is C:\Program Files\Trend Micro\Deep Security Agent)
2. Run the following: **dsa_control -r**

**To deactivate the agent on Linux:**

1. Run the following: **/opt/ds_agent/dsa_control -r**

## Start or stop the agent

**To start or stop the agent on Windows:**

- Start: `sc start ds_agent`
- Stop: `sc stop ds_agent`

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

**To start or stop the agent on Linux:**

Using SysV init scripts:

- Start: `/etc/init.d/ds_agent start`
- Stop: `/etc/init.d/ds_agent stop`

Using systemd commands:

- Start: `systemctl start ds_agent`
- Stop: `systemctl stop ds_agent`

# Common issues when installing or updating the agent

This article looks at three of the most common issues that can occur when installing or updating agents.

**General helpful links**

https://help.deepsecurity.trendmicro.com/aws/welcome.html

https://success.trendmicro.com/product-support/deep-security-20-0

## 1. Anti-Malware engine offline (Windows)

This problem typically occurs on Windows machines, where the Anti-Malware module has either not installed properly, or a driver/service is not running. From the Agent side, the Deep Security notifier app in the taskbar will show a status of “Driver Offline/Not Installed.” If the server reporting this error has not had the initial root certificate updates installed from Microsoft’s Updates, then the server must be patched, the Agent must be uninstalled, the server rebooted, and the Agent re-installed/re-activated.

Most of the time this problem is resolved by uninstalling, restarting, and re-installing/re-activating the Agent, as the troubleshooting steps in the first article referenced below states.

For a full walkthrough of cleaning up the Deep Security Agent from a Windows machine, refer to the third article linked below, which includes instructions for manually uninstalling the Deep Security Agent. It’s not always necessary to manually uninstall the Agent, but the instructions include file locations, registry entries, and services to clean up, after a normal uninstall and reboot has been completed.

**Helpful links:**

Updating the VeriSign, DigiCert, USERTrust RSA certificate on Deep Security and Trend Cloud One - Endpoint & Workload Security

Error: Anti-Malware Engine Offline

Manually uninstalling Deep Security Agent, Relay, and Notifier from Windows

## 2. Security update failed

If a Deep Security Agent is unable to communicate with the designated Deep Security Relay in the environment, the server has a risk of not running the latest Anti-Malware patterns, so this can be a higher priority issue.

When troubleshooting security update failures, the most common reason for the failure is due to network connectivity between the Deep Security Agent and the Deep Security Relay. The article linked below gives a few steps for checking that connectivity and confirming TCP communication is functioning between the two components.

Using a utility like Test-NetConnection in Powershell, or telnet/curl from a Linux server can help with confirming TCP communication between the Agent and Manager are open. If TCP connectivity is open, then there could potentially be a device between the two that is performing SSL Inspection, or interfering with the encrypted connection between the two points.

The ds_agent.log file on the Agent will normally provide a reason for why it cannot perform a security update and will be identified at the start of the line with the word Error or Warning. Correlate the update attempt time with the time in the log file to identify the underlying reason why updates are failing.

Log file location:

- Windows - `C:\ProgramData\Trend Micro\Deep Security Agent\diag`
- Linux - `/var/opt/ds_agent/diag`

**Helpful links:**

https://help.deepsecurity.trendmicro.com/aws/security-update-connectivity.html

https://www.trendmicro.com/en_us/business/products/downloads.html

## 3. Performance/Application issues introduced after installing the Deep Security Agent (Anti-Malware and Module Isolation)

Prior to deploying a Deep Security Agent, the appropriate security configuration will need to be applied to a server; this is common with any Anti-Malware/Security software, and ensures the server or applications installed are not negatively impacted by increased review of their activity.

Although this section does not refer directly to a status in the Deep Security console, this is one of the more common configuration adjustments that will require troubleshooting after deploying the Deep Security Agent to a new server. If a server's performance is impacted, or an application's functionality is impacted, you should first identify which Deep Security module could be contributing to the problem.

Performance issues can be identified first by which processes on a server may be utilizing more CPU/RAM than others. In Windows machines, there are two services that could typically be the culprit; dsa.exe or coreServiceShell.exe. dsa.exe is the core Agent process running on the machine, and coreServiceShell.exe is part of the Anti-Malware module. In a Linux server, these processes are named ds_agent and ds_am, respectively.

Regardless of which process is consuming resources, you'll want to narrow down which protection module(s) are contributing to the increased use of resources. By turning off individual modules, one-by-one, from the Deep Security Manager console, you can watch the resource utilization for any decrease in use, then likely attribute that behavior to the most recent module disabled.

When coreServiceShell.exe or ds_am processes are utilizing a high amount of CPU, this is usually indicative of the Real-Time Anti-Malware engine scanning a high number of read/write transactions on the server, requiring a higher amount of resources to complete its job.

This high amount of activity can be reduced by adding exclusions for data/applications we know are safe. The most common method for reducing resource utilization, or resolving other Application issues introduced from the Anti-Malware module, is by identifying safe applications running on the server, and implementing Process Image exclusions. A Process Image exclusion is a pointer to the full path of a process running on the server that you know to be safe, such as sqlsvr.exe for Microsoft SQL Server. By excluding this process, any files accessed by the sqlsvr.exe process would not be scanned by the Real-Time engine. To make these adjustments, the Scan Configuration for the machine/policy must be edited in the Deep Security Manager, to include the appropriate processes to be excluded.

Applications that are impacted by the Anti-Malware module may require additional troubleshooting after applying exclusions, including collecting additional information from the server. On the server encountering Anti-Malware related application issues, additional debug logging can be enabled by editing the C:\Program Files\Trend Micro\AMSP\AmspConfig.ini file; change the line DebugLevel=0 to DebugLevel=1 or 2 (2 logs further information). Restart the Trend Micro Deep Security Agent and Solution Platform services for those changes to take effect. To revert these logging options, adjust the DebugLevel back to 0, and perform the same service restarts.

On Linux servers, Identify the PID for ds_am process:

```
$ ps aux | grep ds_am
```

Increase debug level (run command multiple times to increase level by 1):

```
kill -USR1 $(PID_for_ds_am)
```

To decrease the debug level (run command multiple times to decrease level by 1):

```
kill -USR2 $(PID_for_ds_am)
```

Reproduce the problem, and then collect a diagnostic package from the command line (link), which will include the additional information from the logging level that was adjusted (note: collecting the Diagnostic Package from the Deep Security Manager will include additional information not collected via command line). This diagnostic package can be provided to the support team to review and help identify the underlying problem.

**Helpful links:**

https://help.deepsecurity.trendmicro.com/aws/high-cpu-usage.html

# User Guide

## Add computers

### About adding computers

The **Computers** page in Deep Security Manager enables you to manage and monitor the computers you are protecting with Deep Security.

This page regularly refreshes itself to display the most current information. (You can modify the refresh rate on a per-user basis. Go to **Administration > User Management > Users** and then double-click on a user account to open its **Properties** window. On the **Settings** tab, in the **Refresh Rate** section, modify the page refresh rate.)

## Add computers to the manager

**Note:** After being installed on a computer, an agent must be activated by the Deep Security Manager. During activation, the Deep Security Manager sends a fingerprint to the agent, after which the agent accepts instructions only from a manager with that unique fingerprint.

You can add computers through the **Computers** page.

## Group computers

Creating computer groups is useful from an organizational point of view and it speeds up the process of applying and managing policies. Groups are displayed in the tree structure on the left side of the Computers page. To create a new group, select the computer group under which you want to create the new computer group and then click **Add > Create Group(s)**.

To move a computer to a group, select the computer and click **Actions > Move to Group**. Keep in mind that policies are applied at the computer level, not the computer group level. Moving a computer from one computer group to another has no effect on the policy assigned to that computer.

To remove a group, right-click it and click **Remove Group**. You can only remove a computer group if it contains no computers and has no sub-groups.

You can also "Group computers dynamically with smart folders" on page 1467.

## Export your computers list

You can click **Export** on the Computers page to export your computers list to an XML or CSV file. Exporting is useful when you want to back up your computer information, integrate it with other reporting systems, or to migrate computers to another Deep Security Manager. (If you export, you do not have to re-discover and scan computers from the new manager.)

**Note:** The exported computers file does **not** include any assigned policies, firewall rules, firewall stateful configurations or intrusion prevention rules. To export this configuration information use the Policy export option in the **Policies** page.

### Delete a computer

If you delete a computer (by selecting it and clicking **Delete**), all information pertaining to that computer is deleted along with it. If you re-discover the computer, you will have to re-assign a policy and whatever rules were assigned previously.

## Add local network computers

### Agent-initiated activation

If the Deep Security Manager cannot initiate communication with computers that you want to protect (for example, if computers are on a different local network or are protected by a firewall), then computers must initiate connections to the manager instead. This includes the connection for agent activation. To use agent-initiated activation, you must install the Deep Security Agent on the computer and then run a set of command-line instructions which tell the agent to communicate with the Deep Security Manager. During the communication, the Deep Security Manager activates the agent and can be further instructed to perform a number of other actions such as assigning a security policy, making the computer a member of a computer group, and so on.

If you are going to add a large number of computers to the Deep Security Manager at one time, you can use the command-line instructions to create scripts to automate the process. For more information on agent-initiated activation, scripting, and command line options, see "Command-line basics" on page 1565.

### Manually add a computer

You can manually add an individual computer by specifying its IP address or hostname.

1. Go to the **Computers** page and click **Add > Add Computer** in the toolbar to display the **New Computer** wizard.
2. Enter the new computer's IP address or hostname.
3. Select a policy to assign to it from the list.

4. Select a relay group from which the new computer will download security updates.
5. Click **Next** to begin the search for the computer.

If the computer is detected and an agent is installed and running on that computer, the computer will be added to your computers list and the agent will be activated.

> **Note:** "Activating" an agent means that the manager communicates with the agent sending it a unique "fingerprint". The agent will then use this fingerprint to uniquely identify the Deep Security Manager and will not accept instructions from any other managers that might try to contact it.

If a policy has been assigned to the computer, the policy will be deployed to the agent and the computer will be protected with all the rules and configurations that make up the policy.

By default, the security updates delivered by relay groups include new malware patterns. If you have enabled the **Support 9.0 (and earlier) agents** option (on the **Administration > System Settings > Updates** page), updates to the engines will also be included.

If the computer is detected but no Deep Security Agent is present, you will be told that the computer can still be added to your computers list but that you still have to install an agent on the computer. Once you install an agent on the computer, you will have to find the computer in your computers list, right-click it, and choose **Activate/Reactivate** from the context menu.

If the computer is not detected (not visible to the manager), you will be told that you can still add the computer but that when it becomes visible to the manager you will have to activate it as above.

## Discover computers

A discovery operation scans the network for visible computers. To initiate a discovery operation, go to the **Computers** page, click **Add > Discover**. The Discover Computers dialog will appear.

You are provided several options to restrict the scope of the scan. You can choose to perform a port scan of each discovered computer.

> **Note:** If you are discovering or scanning a large number of computers, a port scan can take time and reduce performance until it is complete.

When discovering computers, you can specify a computer group to which they should be added. Depending on how you have chosen to organize your computer groups, it may be convenient to create a computer group called "Newly Discovered Computers", or "Newly Discovered Computers on Network Segment X" if you will be scanning multiple network segments. You can then move your discovered computers to other computer groups based on their properties and activate them.

During discovery, the manager searches the network for any visible computers that are not already listed. When a computer is found, the manager attempts to detect whether an agent is present. When discovery is complete, the manager displays all the computers it has detected and displays their status in the **Status** column.

**Note:** The Discovery operation only checks the status of newly-discovered computers. To update the status of already-listed computers, right-click the selected computer(s) and click **Actions > Check Status**.

After discovery operations, a computer can be in one of the following states:

- **Discovered (No Agent):** The computer has been detected but no agent is present. The computer may also be in this state if an agent is installed but has been previously activated and is configured for agent initiated communications. In this case, you will have to deactivate and then reactivate the agent. ("No Agent" will also be reported if the agent is installed but not running.)
- **Discovered (Activation Required):** The agent is installed and listening, and has been activated, but is not yet being managed by the manager. This state indicates that this manager was at one point managing the agent, but the agent's public certificate is no longer in the manager's database. This may be the case if the if the computer was removed from the manager and then discovered again. To begin managing the agent on this computer, right-click the computer and select **Activate/Reactivate**. Once reactivated, the **Status** will change to "Online".
- **Discovered (Deactivation Required):** The agent is installed and listening, but it has already been activated by another manager. In this case, the agent must be deactivated (reset) prior to activation by this manager. Deactivating an agent can be done using the manager that originally activated it or it can be reset through the command line. To deactivate the agent from the manager, right-click the computer and choose **Actions > Deactivate**. To deactivate the agent from the command line, see "Reset the agent" on page 1580.
- **Discovered (Activated):** The agent is installed and activated by the current manager. In this case, the status will change to "Online" on the next heartbeat. To begin managing the

agent, right-click the computer and select **Activate/Reactivate**. Once reactivated, the **Status** will change to "Online".

> **Note:** The discovery operation does not discover computers running as virtual machines in a vCenter, computers in a Microsoft Active Directory or in other LDAP directories.

## Add Active Directory computers

Deep Security can use an LDAP server such as Microsoft Active Directory for computer discovery and to create user accounts and their contacts. Deep Security Manager queries the server, and then displays computer groups according to the structure in the directory.

If you are using Deep Security in FIPS mode, you must import the Active Directory's SSL certificate into Deep Security Manager before connecting the manager with the directory. See "Manage trusted certificates" on page 1525.

1. In Deep Security Manager, click **Computers**.
2. In the main pane, click **Add > Add Active Directory**.
3. Type the host name or IP address, name, description, and port number of your Active Directory server. Also enter your access method and credentials. Follow these guidelines:

   - The **Server Address** must be the same as the Common Name (CN) in the Active Directory's SSL certificate if the access method is LDAPS.
   - The **Name** doesn't have to match the directory's name in Active Directory.
   - The **Server Port** is Active Directory's LDAP or LDAPS port. The defaults are 389 (LDAP and StartTLS) and 636 (LDAPS).
   - The **Username** must include your domain name. For example, `EXAMPLE/Administrator`.
   - If you are using Deep Security in FIPS mode, click **Test Connection** in the Trusted Certificate section to check whether the Active Directory's SSL certificate has been imported successfully into Deep Security Manager.

   Click **Next** to continue.

4. Specify your directory's schema. If you have not customized the schema, you can use the default values for a Microsoft Active Directory server.

The **Details** window of each computer in Deep Security Manager has a **Description** field. To use an attribute of the "Computer" object class from your Active Directory to populate the "Description" field, type the attribute name in the **Computer Description Attribute** text box.

Select **Create a Scheduled Task to Synchronize this Directory** if you want to automatically keep this structure in the Deep Security Manager synchronized with your Active Directory server. A **Scheduled Task** wizard will appear when you are finished adding the directory. You can set this up later using the **Scheduled Tasks** wizard: **Administration > Scheduled Tasks**.

5. Click **Next** to continue.
6. When the Manager has imported your directory, it will display a list of computers that it added. Click **Finish**.

   The directory structure will appear on the **Computers** page.

## Additional Active Directory options

Right-clicking an Active Directory structure gives you options that are not available for non-directory computer groups:

- **Remove Directory**
- **Synchronize Now**

### Remove Directory

When you remove a directory from the Deep Security Manager, you have these options:

- **Remove directory and all subordinate computers/groups from DSM:** Remove all traces of the directory.
- **Remove directory but retain computer data and computer group hierarchy:** Turn the imported directory structure into identically organized regular computer groups, no longer linked with the Active Directory server.
- **Remove directory, retain computer data, but flatten hierarchy:** Remove links to the Active Directory server, discards directory structure, and places all the computers into the same computer group.

### Synchronize Now

You can manually trigger Deep Security Manager to synchronize with the Active Directory server to refresh information on computer groups.

Tip: You can automate this procedure by creating a scheduled task.

## Server certificate usage

If it is not already enabled, enable SSL on your Active Directory server.

Computer discovery can use either SSL or TLS or unencrypted clear text, but importing user accounts (including passwords and contacts) requires authentication and SSL or TLS.

SSL or TLS connections require a server certificate on your Active Directory server. During the SSL or TLS handshake, the server will present this certificate to clients to prove its identity. This certificate can be either self-signed or signed by a certificate authority (CA). If you don't know if your server has a certificate, on the Active Directory server, open the Internet Information Services (IIS) Manager, and then select **Server Certificates**. If the server doesn't have a signed server certificate, you must install it.

## Import users and contacts

Deep Security can import user account information from Active Directory and create corresponding Deep Security users or contacts. This offers the following advantages:

- Users can use their network passwords as defined in Active Directory.
- Administrators can centrally delete accounts from within Active Directory.
- Maintenance of contact information is simplified (e.g., email, phone numbers, etc.) by leveraging information already in Active Directory.

Both users and contacts can be imported from Active Directory. Users have configuration rights on the Deep Security Manager. Contacts can only receive Deep Security Manager notifications. The synchronization wizard allows you to choose which Active Directory objects to import as users and which to import as contacts.

To successfully import an Active Directory user account into Deep Security as a Deep Security user or contact, the Active Directory user account must have a **userPrincipalName** attribute value. The **userPrincipalName** attribute corresponds to an Active Directory account holder's "User logon name".

1. Click **Administration > User Management** and then click either **Users** or **Contacts**.
2. Click **Synchronize with Directory**.
   If this is the first time user or contact information is imported, the server information page is displayed. Otherwise, the Synchronize with Directory wizard is displayed.
3. Select the appropriate access options, provide logon credentials, and click **Next**.
4. Select the groups you want to synchronize by selecting them from the left column and clicking **>>** to add them to the right column and then click **Next**.

   > Tip: You can select multiple groups by holding down shift or control while clicking on them.

5. Select whether to assign the same Deep Security role to all Directory group members or to assign Deep Security roles based on Directory Group membership and then select a default role from the list and click **Next**.
6. If you assigned Deep Security roles based on Directory Group membership, specify the synchronization options for each group and click **Next**.

   After synchronization, the wizard generates a report showing the number of objects imported.

   Before you finish the synchronization, you can choose to create a scheduled task to regularly synchronize users and contacts.

7. Click **Finish**.

Once imported, you will be able to tell the difference between organic (non-imported) Deep Security accounts and imported accounts because you will not be able to change any general information for these accounts.

## Keep Active Directory objects synchronized

Once imported, Active Directory objects must be continually synchronized with their Active Directory servers to reflect the latest updates for these objects. This ensures, for example, that computers that have been deleted in Active Directory are also deleted in Deep Security Manager. To keep the Active Directory objects that have been imported to the Deep Security Manager synchronized with Active Directory, it is essential to set up a scheduled task that synchronizes directory data. The wizard to import computers includes the option to create these scheduled tasks.

Alternatively, you can create this task using the Scheduled Task wizard. On-demand synchronization can be performed using the **Synchronize Now** option for computers and **Synchronize with Directory** button for users and contacts.

You do not need to create a scheduled task to keep users and contacts synchronized. At login, Deep Security Manager checks whether the user exists in Active Directory. If the username and password are valid, and the user belongs to a group that has synchronization enabled, the user will be added to Deep Security Manager and allowed to log in.

If you disable an account in Active Directory but do not delete it, the user remains visible and active in Deep Security Manager.

## Disable Active Directory synchronization

You can stop Deep Security Manager from synchronizing with Active Directory for both computer groups and user accounts.

### Remove computer groups from Active Directory synchronization

1. Go to **Computers**.
2. Right-click the directory, and select **Remove Directory**.
3. Select what to do with the list of computers from this directory when Deep Security Manager stops synchronizing with it:
   - **Remove directory and all subordinate computers/groups from Deep Security Manager**: Remove this directory's structure.
   - **Remove directory but retain computer data and group hierarchy**: Keep the existing structure, including its user and role access to folders and computers.
   - **Remove directory, retain computer data, but flatten hierarchy**: Convert the directory's structure to a flat list of computers inside a group that is named after the directory. The new computer group has the same user and role access as the old structure.
4. Confirm the action.

### Delete Active Directory users and contacts

Unlike when you remove directory queries for computer groups, if you delete the query for users and contacts, all those accounts will be deleted from Deep Security Manager. As a result, you cannot delete while logged into Deep Security Manager with a user account that was imported from the directory server. Doing so will result in an error.

1. On either **Users** or **Contacts**, click **Synchronize with Directory**.
2. Select **Discontinue Synchronization** and then click **OK**.
3. Click **Finish**.

# Add AWS instances

## About adding AWS accounts

Topics:

- "Overview of methods for adding AWS accounts" below
- "What happens when you add an AWS account?" below
- "Benefits of adding an AWS account" on the next page
- "Supported AWS regions" on the next page

### Overview of methods for adding AWS accounts

There are several ways to add AWS accounts to Deep Security Manager:

- "Add an AWS account using an access key" on the next page. Use this method if Deep Security Manager is outside AWS.
- "Add an AWS account using a cross-account role" on page 587. Use this method if you want to add multiple AWS accounts.

### What happens when you add an AWS account?

When you add an AWS account to Deep Security, all the Amazon EC2 and Amazon WorkSpace instances under that account are imported into Deep Security Manager and become visible in one of these locations:

- EC2 instances appear on the left under **Computers** > *your_AWS_account* > *your_region* > *your_VPC* > *your_subnet*
- Amazon WorkSpaces appear on the left under **Computers** > *your_AWS_account* > *your_region* >**WorkSpaces**

Once imported, the EC2 and WorkSpace instances can be managed like any other computer. These instances are tree structures and are treated as computer groups.

If you previously added Amazon EC2 instances or Amazon WorkSpaces as individual computers, and they are part of your AWS account, after importing the account, the instances are moved into the treestructure described above.

### Benefits of adding an AWS account

The following are benefits of adding an AWS account through Deep Security Manager > **Computers > Add AWS Account** instead of adding individual EC2 instances and WorkSpaces through Deep Security Manager > **Computers > Add Computer**:

- Changes in your EC2 and WorkSpaces inventory are automatically reflected in Deep Security Manager. For example, if you delete a number of EC2 or WorkSpace instances in AWS, those instances disappear automatically from the manager. By contrast, if you use **Computers > Add Computer**, EC2 and WorkSpace instances that are deleted from AWS remain visible in the manager until they are manually deleted.
- Your EC2 and WorkSpace instances are organized into AWS region > VPC > subnet in the manager, which lets you easily see which instances are protected and which are not. Without the AWS account, all your EC2 and WorkSpace instances appear at the same root level under **Computers**.
- You get AWS metadata, which can be used in event-based tasks (EBTs) to simplify policy assignment. You can also use metadata with smart folders to organize your AWS instances.

### Supported AWS regions

Deep Security Manager's **Computers > Add > Add AWS Account** option only supports AWS regions that use the global AWS Identity Access Management (IAM) service at `iam.amazonaws.com`. To determine if your region uses the global service, see AWS service endpoints.

At the time or writing, the following regions did not use the global IAM service:

- China (Beijing) - See Beijing region endpoints.
- China (Ningxia) - See Ningxia region endpoints.

## Add an AWS account using an access key

Follow the instructions below to add an AWS account to Deep Security Manager using an access key. Use an access key if your Deep Security Manager is on a server outside of AWS, or if you have tried another method and it doesn't work. For all other scenarios, we recommend you use another method for adding AWS accounts. (Access keys are discouraged because the keys need to be updated periodically (for security reasons), which creates management overhead.)

**Note:** The term 'AWS Primary Account' will be used throughout this topic to describe the AWS account that contains the EC2 and WorkSpace instances that you want to add to the manager.

First, log in to the AWS Primary Account

1. Go to Amazon Web Services at https://aws.amazon.com/.
2. Sign in using the AWS Primary Account.

Next, configure an IAM policy

1. In the Amazon Web Services Console, go to the **IAM** service.
2. In the left navigation pane, click **Policies**.

   **Note:** If this is your first time on this page, you'll need to click **Get Started**.

3. Click **Create policy**.
4. Select the **JSON** tab.
5. Copy the following JSON code into the text box:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "cloudconnector",
            "Action": [
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeRegions",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVpcs",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeSecurityGroups",
                "workspaces:DescribeWorkspaces",
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:DescribeTags",
                "iam:ListAccountAliases",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "sts:AssumeRole"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

> **Note:** The `"sts:AssumeRole"` permission is required only if you plan on adding more AWS accounts to the manager (using cross account roles).

> **Note:** The `"iam:GetRole"` and `"iam:GetRolePolicy"` permissions are optional, but recommended because they allow Deep Security to determine whether you have the correct policy when an update to the manager occurs that requires additional AWS permissions.

6. Click **Review policy**.
7. Give the policy a name and description. Example name: `Deep_Security_Policy`.
8. Click **Create policy**. Your policy is now ready to use.

---

Next, create an IAM user with an access key ID and secret

1. Go to the **IAM** service.
2. Click **Users**.
3. Click **Add user**.
4. Enter a user name. Example: Deep_Security_IAM_User.
5. For **Access type**, select **Programmatic access**.
6. Click **Next: Permissions**.
7. Click the **Attach existing policies directly** box.
8. Find the IAM policy you just created and select the check box next to it.
9. Click **Next: Review**.

---

10. Click **Create user**. Your access key ID and secret access key are shown in the table.
11. Copy the access key ID and secret access key to a safe location. You'll need them later.

---

Next, add the access key to the manager

1. Log in to Deep Security Manager.
2. Click **Administration** at the top.
3. Click **System Setting** on the left.
4. Click the **Advanced** tab in the main pane.
5. Scroll to the bottom and look for the **Manager AWS Identity** heading.
6. Next to **Access Key - The Access Key of an AWS User used for the manager identity**, enter the access key of the IAM user you created previously.
7. Next to **Secret Key - The Secret Access Key of an AWS User used for the manager identity**, enter the secret key of the IAM user that you created previously.
8. Click **Save**.

---

Finally, add your AWS Primary Account and its access key to the manager

1. Click **Computers** at the top.
2. Click **Add > Add AWS Account**.
3. Select **Use AWS Access Keys**.
4. Enter your AWS Primary Account's IAM user **Access Key ID** and **Secret Access Key** that you created previously.
5. If your AWS Primary Account includes Amazon WorkSpaces, select **Include Amazon WorkSpaces** to include them with your Amazon EC2 instances. By enabling the check box, you ensure that your Amazon WorkSpaces appear in the correct location in the tree structure in Deep Security Manager and are billed at the correct rate.

   Your AWS Primary Account's Amazon EC2 instances and Amazon WorkSpaces are loaded.

---

After completing the above tasks, proceed to Install the agent on your Amazon EC2 and WorkSpace instances if you have not done so already.

## Add an AWS account using a cross-account role

Follow the instructions below to add an AWS account using a cross-account role. Use a cross-account role if you want to add multiple AWS accounts.

The instructions below assume you want to add AWS accounts with these names:

- AWS Primary Account
- AWS Account A

**Tip:** You can also add a cross-account role through the Deep Security API. See "Add the account through the API" on page 590 for details.

First, add the AWS Primary Account

- Complete all tasks in "Add an AWS account using an access key" on page 583 to add the AWS Primary Account.

Next, find the AWS Primary Account identifier

1. Make sure you're logged in to the AWS Primary Account.
2. At the top-right of AWS, click **Support > Support Center**.
3. Note the **Account Number** shown at the top-right (`1111111111`, in this example). You'll need it later to create the cross-account role.

Next, retrieve the external ID

1. Log in to Deep Security Manager.
2. Click **Computers** at the top.
3. Click **Add > Add AWS Account**. A wizard appears.
4. Click the eye icon next to the obscured external ID to reveal it. For more on this ID, see "What is the external ID?" on page 594
5. Copy the external ID to a secure place. You will need it in the next step to configure AWS Account A and any other AWS accounts you want to add.
6. (Optional.) Close the wizard and the manager.

Next, configure an IAM policy for AWS Account A

> **Note:** This IAM policy is the same as the policy for the AWS Primary Account, except it does not require the `sts:AssumeRole` permission.

1. Make sure you're logged in to AWS Account A.
2. In the Amazon Web Services Console, go to the **IAM** service.
3. In the left navigation pane, click **Policies**.

   > **Note:** If this is your first time on this page, you'll need to click **Get Started**.

4. Click **Create policy**.
5. Select the **JSON** tab.
6. Copy the following JSON code into the text box:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "cloudconnector",
            "Action": [
                "ec2:DescribeImages",
                "ec2:DescribeInstances",
                "ec2:DescribeRegions",
                "ec2:DescribeSubnets",
                "ec2:DescribeTags",
                "ec2:DescribeVpcs",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeSecurityGroups",
                "workspaces:DescribeWorkspaces",
                "workspaces:DescribeWorkspaceDirectories",
                "workspaces:DescribeWorkspaceBundles",
                "workspaces:DescribeTags",
                "iam:ListAccountAliases",
                "iam:GetRole",
                "iam:GetRolePolicy"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

> **Note:** The `"iam:GetRole"` and `"iam:GetRolePolicy"` permissions are optional, but recommended because they allow Deep Security to determine whether you have the correct policy when an update to the manager occurs that requires additional AWS permissions.

7. Click **Review policy**.
8. Give the policy a name and description. Example name: `Deep_Security_Policy_Cross`.
9. Click **Create policy**. Your policy is now ready to use.

Next, create a cross-account role for AWS Account A

1. Make sure you're logged in to AWS Account A.
2. Go to the **IAM** service.
3. In the left navigation pane, click **Roles**.
4. In the main pane, click **Create role**.
5. Click the **Another AWS account** box.
6. In the **Account ID** field:
    - Enter the account ID of AWS Primary Account that you noted in a previous step. For example: `1111111111`
7. Next to **Options**, enable **Require external ID**. In the **External ID** field, enter the external ID you retrieved from the manager earlier.
8. Click **Next: Permissions**.
9. Select the IAM policy that you just created (the example name was `Deep_Security_Policy_Cross`) and then click **Next: Review**.
10. On the **Review** page, enter a role name and description. Example role name: `Deep_Security_Role_Cross`.
11. On the main role page, search for the role you just created (`Deep_Security_Role_Cross`).
12. Click it.
13. Find the **Role ARN** field at the top. It looks similar to: `arn:aws:iam::2222222222:role/Deep_Security_Role_Cross`
14. Note the **Role ARN** value. You'll need it later.

You now have a cross-account role under AWS Account A that includes the correct policy and references the account ID of the AWS Primary Account.

Next, add AWS Account A to the manager

1. Log in to Deep Security Manager.
2. Click **Computers** at the top.
3. Click **Add > Add AWS Account**.
4. Select **Use Cross Account Role**.
5. Enter AWS Account A's **Cross Account Role ARN**. You noted this earlier, when you created the cross-account role. In this example, it is `arn:aws:iam::2222222222:role/Deep_Security_Role_Cross`
6. If AWS Account A includes Amazon WorkSpaces, select **Include Amazon WorkSpaces** to include them with your Amazon EC2 instances. By enabling the check box, you ensure that your Amazon WorkSpaces appear in the correct location in the tree structure in Deep Security Manager and are billed at the correct rate.
7. Click **Next**.
   AWS Account A's Amazon EC2 instances and Amazon WorkSpaces are loaded.

You have now added AWS Account A to the manager.

After completing the above tasks, proceed to Install the agent on your Amazon EC2 and WorkSpace instances if you have not done so already.

## Add the account through the API

1. If you don’t yet have the external ID, call the Deep Security `/api/awsconnectorsettings` endpoint to retrieve it (the `ExternalId` parameter). For more on this ID, see "What is the external ID?" on page 594
2. In AWS, specify the external ID in your cross-account role's IAM trust policy.
3. Use the `/api/awsconnectors` API endpoint to add AWS accounts to Deep Security. Do not use the `/rest/cloudaccounts/aws` API because it has been deprecated. See Action required if you are using cross account roles with the API /rest/cloudaccounts/aws for details on how long the `/rest/cloudaccounts/aws` API will continue to be supported and tips on how to move to the new endpoint.

# Add Amazon WorkSpaces

Amazon WorkSpaces are virtual cloud desktops that run in Amazon Web Services (AWS). You can protect them with Deep Security following the instructions in one of these sections:

- "Protect Amazon WorkSpaces if you already added your AWS account" below
- "Protect Amazon WorkSpaces if you have not yet added your AWS account" on the next page

**Note:** The Deep Security Agent only supports Amazon WorkSpaces Windows desktops–it does not support Linux desktops.

After completing the steps in one of the above-mentioned sections:

- your Amazon WorkSpaces are displayed in Deep Security Manager on the left under **Computers** > *your_AWS_account* > *your_region* > **WorkSpaces**
- your Amazon WorkSpaces are protected by the Deep Security Agent

## Protect Amazon WorkSpaces if you already added your AWS account

If you already added your AWS account to Deep Security Manager (to protect your Amazon EC2 instances), complete the steps in this section to configure Deep Security to work with Amazon WorkSpaces.

1. Upgrade Deep Security Manager VM for Azure Marketplace to version 10.3 or later. See "Upgrade Deep Security Manager VM for Azure Marketplace" on page 1549.
2. Launch an Amazon WorkSpace, and then install and activate Deep Security Agent 10.2 or later on it. See "Install the agent on Amazon EC2 and WorkSpaces" on page 555 for details. Optionally, create a custom WorkSpace bundle so that you can deploy it to many people. See "Install the agent on an AMI or WorkSpace bundle" on page 560 for details on installation, activation, and bundle creation.
3. Modify your IAM policy to include Amazon WorkSpaces permissions:
   a. Log in to AWS with the account that was added to Deep Security Manager.
   b. Go to the **IAM** service.
   c. Find the Deep Security IAM policy. You can find it under **Policies** on the left, or you can look for the Deep Security IAM role or IAM user that references the policy and then click the policy within it.
   d. Modify the Deep Security IAM policy to look like the one shown in "Add an AWS account using a cross-account role" on page 587. The policy includes Amazon

WorkSpaces permissions. If you added more than one AWS account to Deep Security, the IAM policy must be updated under all the AWS accounts.

4. In Deep Security Manager, edit your AWS account:
   a. On the left, right-click your AWS account and select **Properties**.
   b. Enable **Include Amazon WorkSpaces**.
   c. Click **Save**.

You have now added Amazon WorkSpaces to Deep Security.

### Protect Amazon WorkSpaces if you have not yet added your AWS account

If you have not yet added your AWS account to Deep Security Manager, complete the steps in one of the following sections:

- If you want to protect existing Amazon WorkSpaces, read "Install the agent on Amazon EC2 and WorkSpaces" on page 555
- If you want to be able to launch new Amazon WorkSpaces with the agent 'baked in', read "Install the agent on an AMI or WorkSpace bundle" on page 560.

## Manage an AWS account

Topics:

- "Edit an AWS account" below
- "Remove an AWS account" on the next page
- "Synchronize an AWS account" on the next page

### Edit an AWS account

You can edit an AWS account's settings in Deep Security Manager. You might need to do this if, for example, your AWS account needs to be configured to include Amazon WorkSpaces. To edit an AWS account:

1. Log in to Deep Security Manager.
2. Click **Computers** at the top.
3. On the left, right-click your AWS account name and select **Properties**.
4. Edit the settings and click **OK**.

### Remove an AWS account

Removing an AWS account from Deep Security Manager permanently removes the account from the Deep Security database as well as its underlying computers. Your account with AWS is unaffected and any Deep Security Agents that were installed on the instances are still installed, running, and providing protection (although they will no longer receive security updates). If you decide to re-import computers from the AWS account, the Deep Security Agents download the latest security updates at the next scheduled opportunity.

1. In Deep Security Manager, click **Computers**  at the top.
2. In the navigation panel, right-click the AWS account and select **Remove AWS Account**.
3. Confirm that you want to remove the account.
   The account is removed from the Deep Security Manager.

### Synchronize an AWS account

When you synchronize (sync) an AWS account, Deep Security Manager connects to the AWS API to obtain and display the latest set of AWS EC2 and WorkSpace instances.

To force a sync immediately:

1. In Deep Security Manager, click **Computers**.
2. On the left, right-click your AWS account and select **Synchronize Now**.

There is also a background sync that occurs every 10 minutes, and this interval is not configurable. If you force a sync, the background sync is unaffected and continues to occur according to its original schedule.

## Manage an AWS account external ID

**Note:** The AWS account external ID is only used when adding an AWS account using a cross-account role.

Topics:

- "What is the external ID?" on the next page
- "Configure the external ID" on the next page
- "Update the external ID" on the next page
- "Retrieve the external ID" on page 596
- "Disable retrieval of the external ID" on page 596

## What is the external ID?

Along with the cross-account role ARN, the external ID is used to grant access from one AWS role to another. The external ID is provided by a third-party service that wants to assume the role of your account. If you trust that service to act on your behalf, you add that external ID to your cross-account role. In this case, Deep Security is the third-party service that is providing an external ID to you, in order to act on behalf of your AWS account. Deep Security uses this access to synchronize information from your AWS account and maintain an up-to-date record of your resources. For details, see this AWS document: How to Use External ID When Granting Access to Your AWS Resources.

Notes:

- The external ID is only used when adding an AWS account using a cross-account role.
- The same external ID is used for all AWS accounts added using cross-account roles.

## Configure the external ID

Configuring the external ID is one step in a larger process of adding a cross-account role. See "Add an AWS account using a cross-account role" on page 587 for details.

## Update the external ID

If you previously added an AWS account using cross-account role, you might have specified a user-defined external ID. To better align with AWS best-practices, Trend Micro recommends switching to the manager-defined external ID.

> **Note:** AWS accounts that were previously added with a user-defined external ID will continue to function as normal.

Determine whether you're using a user- or manager-defined external ID

If you're not sure whether you're currently using a user- or manager-defined external ID, follow the procedure below to find out.

1. Log in to Deep Security Manager.
2. Click **Computers**.
3. Right-click the AWS account that was added using a cross-account role and select **Properties**.

4. If an **Update** link appears next to the external ID, it means that a user-defined external ID is currently in use and should be updated. If an **Update** link does not appear, it's because the manager-defined external ID is currently in use, and no action is necessary.
5. Repeat this procedure for each account that has been added to the manager using a cross-account role.

---

Update the external ID through the manager

1. If you have not already done so, log in to Deep Security Manager, right-click the AWS account you want to update, and select **Properties**.
2. Click the **Update** link that appears next to the external ID. The **Update** link disappears.
3. Note the external ID. You'll need it in the next step to configure the cross-account role.
4. Log in to the AWS account whose external ID you just updated. Update the cross-account role's IAM policy by replacing the old external ID with the new one.
5. Back on the properties window, click **Apply** to apply changes.

   Your account's user-defined external ID has now been updated to the manager-defined one.

6. Repeat this procedure for each account that has been added to the manager using a cross-account role.

---

Update the external ID through the Deep Security API

1. If you don't already have the new manager-defined external ID, call the `/api/awsconnectorsettings` endpoint to retrieve it (the `ExternalId` parameter).
2. Log in to the AWS account where the cross-account role was configured. Update the cross-account role's IAM policy by replacing the old external ID with the new one. Repeat this step for each account that has been added to the manager using a cross-account role.
3. Using the `/api/awsconnectors` endpoint, perform an `Update` action on the account you are updating, with its `CrossAccountRoleARN` parameter set to the same role ARN as it is currently. Do not provide an external ID in the request object.

---

Your account's user-defined external ID has now been updated to the manager-defined one.

## Retrieve the external ID

There are a few ways to retrieve the external ID for use with cross-accounts.

Through the 'add account' wizard

- See "Add an AWS account using a cross-account role" on page 587 which includes a sub-section on how to retrieve the external ID through the wizard.

Through the Deep Security API

- Call the `/api/awsconnectorsettings` endpoint to retrieve it (the `ExternalId` parameter).

## Disable retrieval of the external ID

You might want to disable the ability to view and retrieve the external ID in the manager to prevent unauthorized access to it. You can retrieve the ID once, store it in a safe place like your secrets manager, and then disable the retrieval for everyone else.

**Note:** Retrieval can be enabled again at any time.

To disable retrieval:

1. Log in to Deep Security Manager.
2. Click **Administration** at the top.
3. In the main pane, click the **Security** tab.
4. Deselect **Enable retrieval and viewing of AWS external ID**.
5. Click **Save**.

**Tip:** You can also use roles to prevent access to the external ID. For details, see "Define roles for users" on page 1415.

# Manage AWS regions

## Add an Amazon Web Services region

If the Amazon Web Services (AWS) region hosting your EC2 resources does not appear when you try to add a cloud account using the **Add AWS Cloud Account** wizard, manually add the region.

1. On the server that is hosting Deep Security Manager, enter the command:
   `dsm_c -action addregion -region REGION -display DISPLAY -endpoint ENDPOINT`

   where the parameters are:

   | Parameter | Description | Example |
   |---|---|---|
   | REGION | The Amazon Web Services identifier for the region. | `ca-east-1` |
   | DISPLAY | The display string to use for the region in the **Add AWS Cloud Account** wizard. | Canada East (Ottawa) |
   | ENDPOINT | The fully-qualified domain name of the Amazon Elastic Compute Cloud (EC2) endpoint to use for the region. | `ec2.ca-east-1.amazonaws.com` |

   **Note:** If Deep Security Manager is running on a Linux server, you must run the command with `sudo` or use a superuser account such as root.

2. If the specific AWS region requires that you import a trusted certificate (most don't), see "Manage trusted certificates" on page 1525.

## Viewing your Amazon Web Services regions

You can view any AWS regions that you have added using the CLI.

On the server that is hosting Deep Security Manager, enter the command:

```
dsm_c -action listregions
```

**Note:** If Deep Security Manager is running on a Linux server, you must run the command with `sudo` or use a superuser account such as root.

### Removing an Amazon Web Services region

You can delete any AWS regions that you have added using the CLI. Any existing cloud accounts for the region will continue to work unless you remove them, but administrators won't be able to create new cloud accounts for the region.

1. On the server that is hosting Deep Security Manager, enter the command:

   ```
   dsm_c -action listregions
   ```

2. Find the identifier for the that you want to remove.
3. Enter the command:

   ```
   dsm_c -action removeregion -region REGION
   ```

   The `REGION` parameter is required.

| Parameter | Description | Example |
|---|---|---|
| REGION | The Amazon Web Services identifier for the region. | `ca-east-1` |

**Note:** If Deep Security Manager is running on a Linux server, you must run the command with `sudo` or use a superuser account such as root.

## Protect an account running in AWS Outposts

Deep Security supports AWS accounts running on AWS Outposts.

To protect your AWS accounts in Outposts:

1. . .

   **Note:** Once you've added your AWS account to Deep Security Manager, the **Computers** page will display the resource as part of the AWS region the Outpost is connected to. For EC2 instances, the ARN of the Outpost rack is added to the instance metadata.

2. "Install the agent on Amazon EC2 and WorkSpaces" on page 555.
3. "Activate the agent" on page 566.
4. "Create policies" on page 630.

**Note:** High availability is supported. For more information, see "Install Deep Security Manager on multiple nodes" on page 511.

# Add Azure instances

## Create an Azure application for Deep Security

In your operating environment, it may not be desirable to allow the Deep Security Manager to access Azure resources with an account that has both the Global Administrator role for Microsoft Entra ID and the Subscription Owner role for the Azure subscription. As an alternative, you can create an Azure application for Deep Security Manager that provides read-only access to Azure resources.

If you have multiple Azure subscriptions, you can create a single Deep Security Azure application for all of them, as long as the subscriptions all connect to the same Active Directory.

To create an Azure application, you need to do the following:

1. "Assign the correct roles" below
2. "Create the Azure application" below
3. "Record the Azure app ID and Active Directory ID" below
4. "Record the Subscription ID" on page 601
5. "Assign the Azure application a role and connector" on page 601

### Assign the correct roles

To create an Azure application, your account must have the User Administrator role for Microsoft Entra ID and the User Access Administrator role for the Azure subscription. Assign these roles to your Azure account before proceeding.

### Create the Azure application

1. In the **Microsoft Entra ID** blade, click **App registrations**.
2. Click **New registration**.
3. Enter a **Name** (for example, Deep Security Azure Connector).
4. For the **Supported account types**, select **Accounts in this organizational directory only**.
5. Click **Register**.

   The Azure application appears in the **App registrations** list with the **Name** you provided.

### Record the Azure app ID and Active Directory ID

1. In the **App registrations** list, click the Azure application.
2. Record the **Application (client) ID**.
3. Record the **Directory (tenant) ID**

## Create an application secret or upload the application certificate

1. On the **Certificates & secrets** tab, select the type of the application credential to use:
   - Option 1: Client secrets (application password)
   - Option 2: Certificate

   You can create multiple application credentials in Azure, but Deep Security Manager only required one credential (either the application secret or application certificate) for the Azure account.

2. Follow the procedure for either Option 1 or Option 2 (below) depending on the type of credential you want to use.

### Option 1: Create client secrets (application password)

1. Click **New client secret**.
2. Enter a **Description** for the client secret.
3. Select an appropriate **Duration**. The client secret expires after this time.
4. Click **Add**.

   The client secret **Value** appears.

5. Record the client secret **Value**. You need to use it as the Application Password when registering the Azure application with Deep Security.

   The client secret **Value** only appears once, so record it now. If you do not, you must regenerate it to obtain a new **Value**.

   If the client secret **Value** expires, you must regenerate it and update it in the associated Azure accounts.

### Option 2: Upload an application certificate

1. Prepare a certificate in X.509 PEM text format.

   The certificate can be either public-signed or self-signed and should not expire. If the private key is protected with a secret, you need the certificate private key and optional passphrase or secret when setting up the Azure account in Deep Security Manager. The RSA key size must be at least 2048 bits.

   Deep Security Manager currently does not support certificates in binary format.

2. Click the **Upload certificate** button.

3. Select certificate file to upload.
4. Click **Add**.

If you provide invalid credentials or configurations (for example, the RSA key is too short), the Azure connector displays an error message "Unable to authenticate to Azure Entra ID. Credential or configuration is invalid".

## Record the Subscription ID

1. On the left, go to **All Services** and click **Subscriptions**.

   A list of subscriptions appears.

   If **Subscriptions** does not appear on the left, use the search box at the top of the screen to find it.

2. Record the **Subscription ID** of each subscription you want to associate with the Azure application. You need the ID later, when adding the Azure accounts to Deep Security.

## Assign the Azure application a role and connector

1. Under **All Services > Subscriptions**, click a subscription that you want to associate with the Azure application.

   You can associate another subscription with the Azure application later if you want to.

2. Click **Access Control (IAM)**.
3. In the main pane, click **Add**, and then select **Add Role Assignment** from the menu.
4. Under **Role**, enter `Reader` and then click the **Reader** role that appears.
5. Under **Assign access to**, select **User, user group, or service principal**.
6. Under **Select members**, enter the Azure application **Name** (for example, `Deep Security Azure Connector`).

   The Azure application appears with the **Name** you chose for it in Step 3 of the "Create the Azure application" on page 599 procedure.

7. Click **Save**.
8. If you want to associate the Azure application to another subscription, repeat this procedure ("Assign the Azure application a role and connector" above) for that subscription.

You can now configure Deep Security to add Azure virtual machines by following the instructions in "Add a Microsoft Azure account to Deep Security" on the next page.

# Add a Microsoft Azure account to Deep Security

Once you've installed Deep Security Manager, you can add and protect Microsoft Azure virtual machines by connecting a Microsoft Azure account to the Deep Security Manager. Virtual machines appear on the Computers page, where you can manage them like any other computer.

Topics in this section:

- "What are the benefits of adding an Azure account?" below
- "Configure a proxy setting for the Azure account" below
- "Add virtual machines from a Microsoft Azure account to Deep Security" below
- "Manage Azure classic virtual machines with the Azure Resource Manager connector" on page 604
- "Remove an Azure account" on page 604
- "Synchronize an Azure account" on page 605

## What are the benefits of adding an Azure account?

The benefits of adding an Azure account (through Deep Security Manager > **Computers > Add Azure Account**) instead of adding individual Azure virtual machines (through Deep Security Manager > **Computers > Add Computer**), are:

- Changes in your Azure virtual machine inventory are automatically reflected in Deep Security Manager. For example, if you delete a number of instances in Azure, those instances disappear automatically from the manager. By contrast, if you use **Computers > Add Computer**, Azure instances that are deleted from Azure remain visible in the manager until they are manually deleted.
- Virtual machines are organized into their own branch in the manager, which lets you easily see which Azure instances are protected and which are not. Without the Azure account, all your virtual machines appear at the same root level under **Computers**.

## Configure a proxy setting for the Azure account

You can configure the Deep Security Manager to use a proxy server to access resources in Azure accounts. For details, see "Connect to cloud accounts via proxy" on page 1340.

## Add virtual machines from a Microsoft Azure account to Deep Security

Add your Microsoft Azure account to Deep Security following the instructions below.

1. Before you begin, create an Azure app for Deep Security.
2. In Deep Security Manager, go to **Computers > Add > Add Azure Account**.

   > **Note:** As of Deep Security Manager 12.0, 'Quick' mode is no longer available. If you used Quick mode in prior releases, there is no impact to your deployment. All new Azure Cloud accounts must use the advanced method.

3. Enter a **Display name**, and then enter the following Azure access information you recorded in step 1:
   - **Directory ID**
   - **Subscription ID**
   - **Application ID**

   > **Note:** If you are upgrading from the Azure classic connector to the Azure Resource Manager connector, the Display name and the Subscription ID of the existing connector will be used.

   > **Note:** If you have multiple Azure subscriptions, specify only one in the **Subscription ID** field. You can add the rest later.

4. Select the type of application credential that you want to use (**Password** or **Certificate**) and then provide the credential information:
   - For Password:
     - In the **Application Password** field, enter the client secret.
   - For Certificate:
     - Next to **Certificate**, click **Choose File** and upload the certificate.
     - Next to **Private Key**, click **Choose File** and upload the private key.
     - If the private key is protected by a password, enter it in **Private Key Password (optional)**.

     > **Note:** The certificate must be in X.509 PEM text format and must be within its validity period. Binary format is not supported.

5. Click **Next**.
6. Review the summary information, and then click **Finish**.
7. Repeat this procedure for each Azure subscription, specifying a different **Subscription ID** each time.

The Azure virtual machines will appear in the Deep Security Manager under their own branch on the **Computers** page.

**Tip:** You can right-click your Azure account name and select **Synchronize Now** to see the latest set of Azure VMs.

**Tip:** You will see all the virtual machines in the account. If you'd like to only see certain virtual machines, use smart folders to limit your results. See "Group computers dynamically with smart folders" on page 1467 for more information.

**Note:** If you have previously added virtual machines from this Azure account, they will be moved under this account in the Computers tree.

## Manage Azure classic virtual machines with the Azure Resource Manager connector

You can also manage virtual machines that were added with the Azure classic connector with the Azure Resource Manager connector, allowing you to manage both your Azure classic and Azure Resource Manager virtual machines with a single connector.

For more information, see "Why should I upgrade to the new Azure Resource Manager connection functionality?" on the next page

1. On the **Computers** page, in the **Computers tree**, right-click the **Azure classic portal** and then click **Properties**.
2. Click **Enable Resource Manager connection**.
3. Click **Next**. Follow the corresponding procedure above.

## Remove an Azure account

Removing an Azure account from the Deep Security Manager will permanently remove the account from the Deep Security database. This will not affect the Azure account. Virtual machines with Deep Security Agents will continue to be protected, but will not receive security updates. If you later import these virtual machines from the same Azure account, the Deep Security Agents will download the latest security updates at the next scheduled update.

1. Go to the **Computers** page, right-click on the Microsoft Azure account in the navigation panel, and select **Remove Cloud Account**.
2. Confirm that you want to remove the account.
3. The account is removed from the Deep Security Manager.

### Synchronize an Azure account

When you synchronize (sync) an Azure account, Deep Security Manager connects to the Azure API to obtain and display the latest set of Azure VMs.

To force a sync immediately:

1. In Deep Security Manager, click **Computers**.
2. On the left, right-click your Azure account and select **Synchronize Now**.

There is also a background sync that occurs every 10 minutes, and this interval is not configurable. If you force a sync, the background sync is unaffected and continues to occur according to its original schedule.

## Why should I upgrade to the new Azure Resource Manager connection functionality?

The next time you try to add an Azure cloud account to Deep Security Manager you will be shown a message suggesting that you upgrade to the new Resource Manager connection functionality. Basically, this new functionality allows Deep Security to connect to Azure virtual machines using the Resource Manager interface. As an Azure user, you are probably aware that the new Azure deployment model Resource Manager is now the default deployment model, replacing the classic model. Since new resources are deployed using this model by default, Deep Security is only able to display these VM resources on the Computers page if it is able to communicate with the Resource Manager interface. So, if you allow Deep Security to upgrade to this new functionality then VM resources deployed with either the Resource Manager deployment model or the classic deployment model will be visible on the Computers page.

Two things to note:

- You can upgrade to this new functionality in Deep Security 10. It is already available in the new Deep Security Manager VM for Azure Marketplace console and no upgrade is needed.
- Until you perform this upgrade VMs deployed using Resource Manager are still being fully protected by Deep Security but for you to see them on the Computers page they have to be added as a computer object. For more information, see "Why can't I view all of the VMs in an Azure subscription in Deep Security?" on page 1693

# Add GCP instances

## Create a Google Cloud Platform service account

Below is all the information you need to create a Google Cloud Platform (GCP) service account for use with Deep Security.

> Tip: For information on why you might want to create a GCP service account to use with Deep Security Manager, see "What are the benefits of adding a GCP account?" on page 615.

Topics:

- "Prerequisite: Enable the Google APIs" below
- "Create a GCP service account" on the next page
- "Add more projects to the GCP service account" on page 611
- "Create multiple GCP service accounts" on page 614

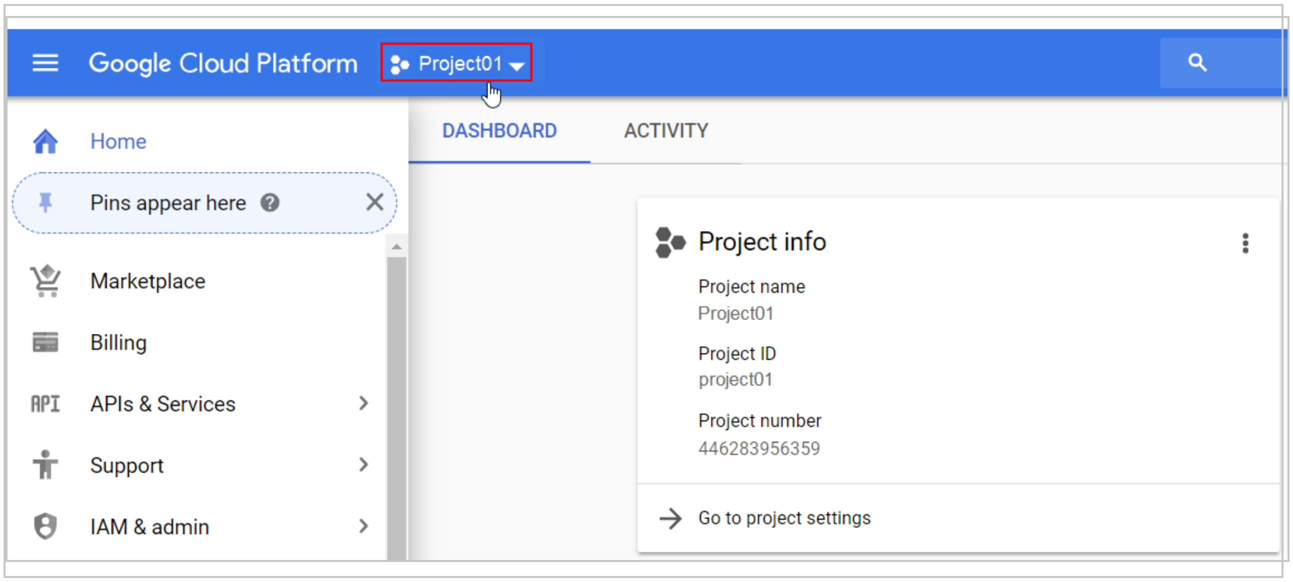
### Prerequisite: Enable the Google APIs

Before you can create a GCP service account for Deep Security Manager, you'll need to enable a few Google APIs under your existing GCP account.

Follow the procedure below to enable these APIs inside each of your projects:

1. Log in to Google Cloud Platform using your existing GCP account. This account must have access to all the GCP projects that contain VMs that you want to protect with Deep Security.
2. At the top, select a project that includes VMs that you want to add to Deep Security Manager. If you have multiple projects, you can select them later.

   For example: `Project01`



Project info

Project name
Project01

Project ID
project01

Project number
446283956359

3. Click **Google Cloud Platform** at the top to make sure you're on the Home screen.
4. From the tree view on the left, select **APIs & Services > Dashboard**.
5. Click **+ ENABLE APIS AND SERVICES**.
6. In the search box, enter `cloud resource manager API` and then click the **Cloud Resource Manager API** box.
7. Click **ENABLE**.
8. Repeat steps 5 - 7 of this procedure, entering `compute engine API` and clicking the **Compute Engine API** box.
9. Repeat steps 1 - 9 of this procedure for any other projects that include VMs that you want to add to Deep Security Manager.

For more information on how to enable or disable APIs in GCP, refer to this page from Google:

https://cloud.google.com/apis/docs/getting-started

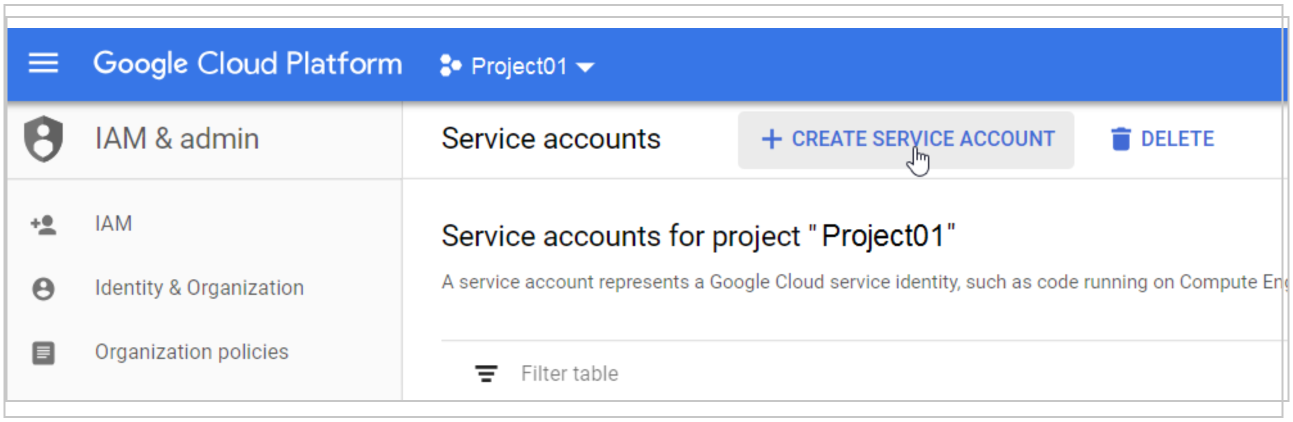
## Create a GCP service account

**Note:** A service account is a special type of Google account that is associated with an application or VM, instead of an individual end user. Deep Security Manager assumes the identity of the service account to call Google APIs, so that users aren't directly involved.

Follow the procedure below to create a service account for Deep Security Manager:

1. Before you begin, make sure you've enabled the GCP APIs. See "Prerequisite: Enable the Google APIs" on the previous page.
2. Log in to Google Cloud Platform using your existing GCP account.

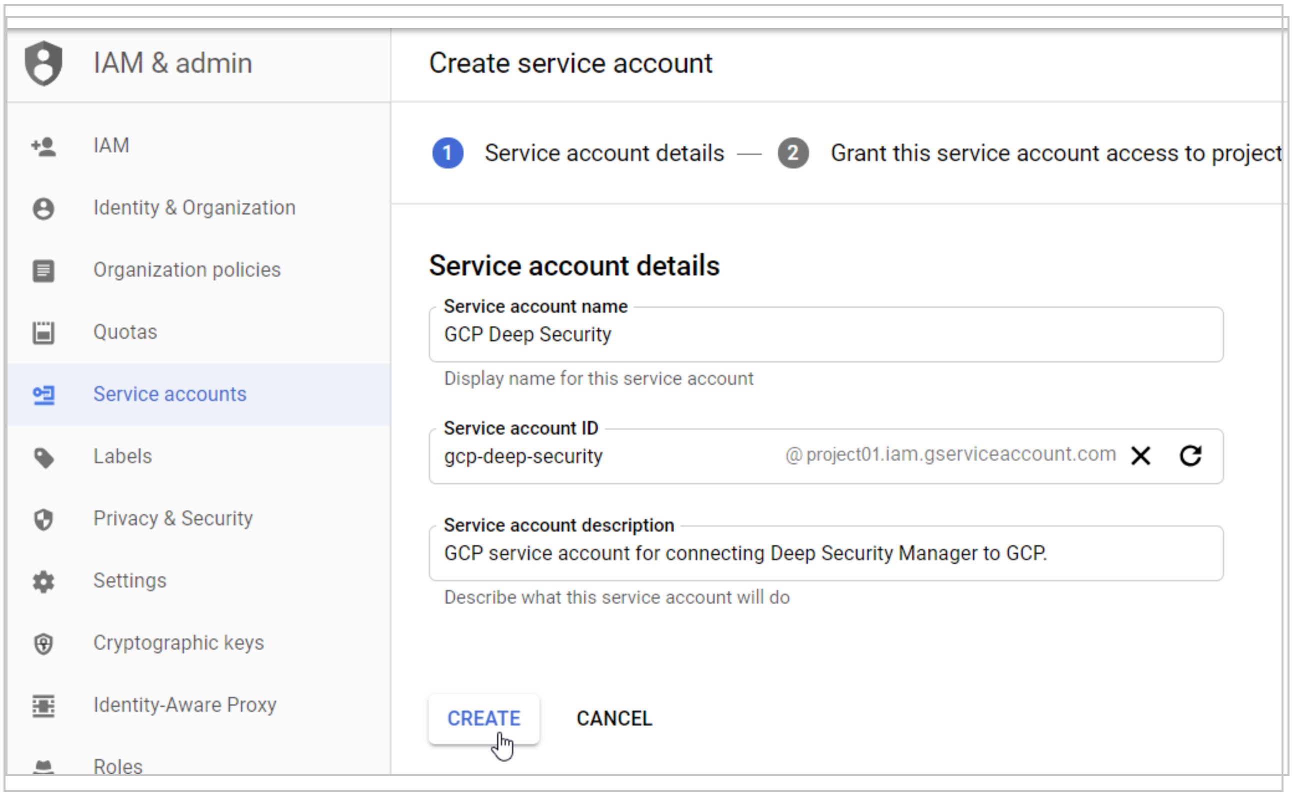
3. At the top, select a project. If you have multiple projects, you can select any one. For example: `Project01`.
4. Click **Google Cloud Platform** at the top to make sure you're on the Home screen.
5. From the tree view on the left, select **IAM & admin > Service accounts**.
6. Click **+ CREATE SERVICE ACCOUNT**.



Service accounts for project "Project01"

A service account represents a Google Cloud service identity, such as code running on Compute En

7. Enter a service account name, ID and description.



Service account details

Service account name: GCP Deep Security

Display name for this service account

Service account ID: gcp-deep-security @project01.iam.gserviceaccount.com

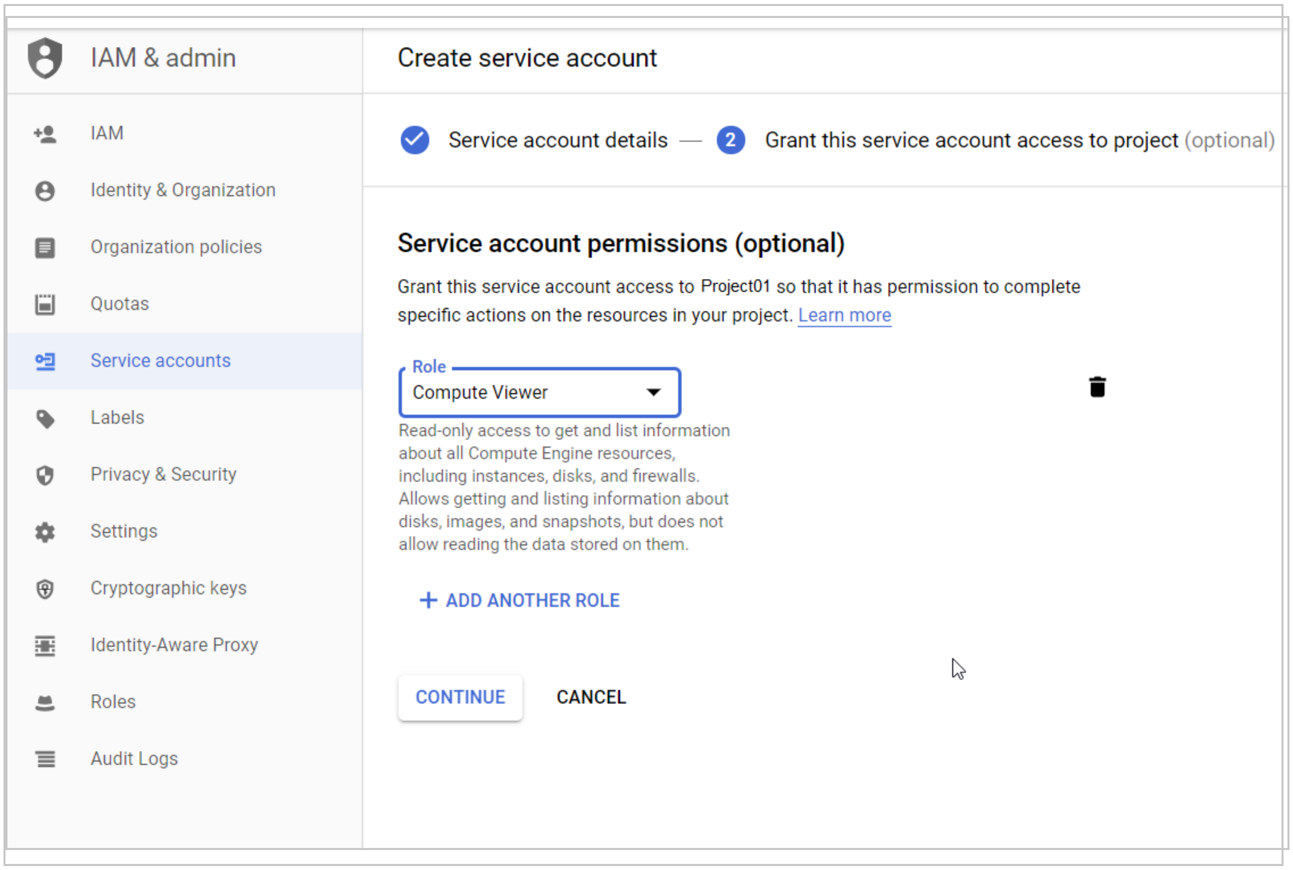
Service account description: GCP service account for connecting Deep Security Manager to GCP.

Describe what this service account will do

For example:

- Service account name: `GCP Deep Security`
- Service account ID: `gcp-deep-security@<your_project_ID>.iam.gserviceaccount.com`
- Service account description: `GCP service account for connecting Deep Security Manager to GCP.`

8. Click **Create**.
9. In the **Select a role** drop-down list, select the **Compute Engine > Compute Viewer** role, or click inside the **Type to filter** area and enter `compute viewer` to find it.
10. Click **CONTINUE**.



Service account permissions (optional)

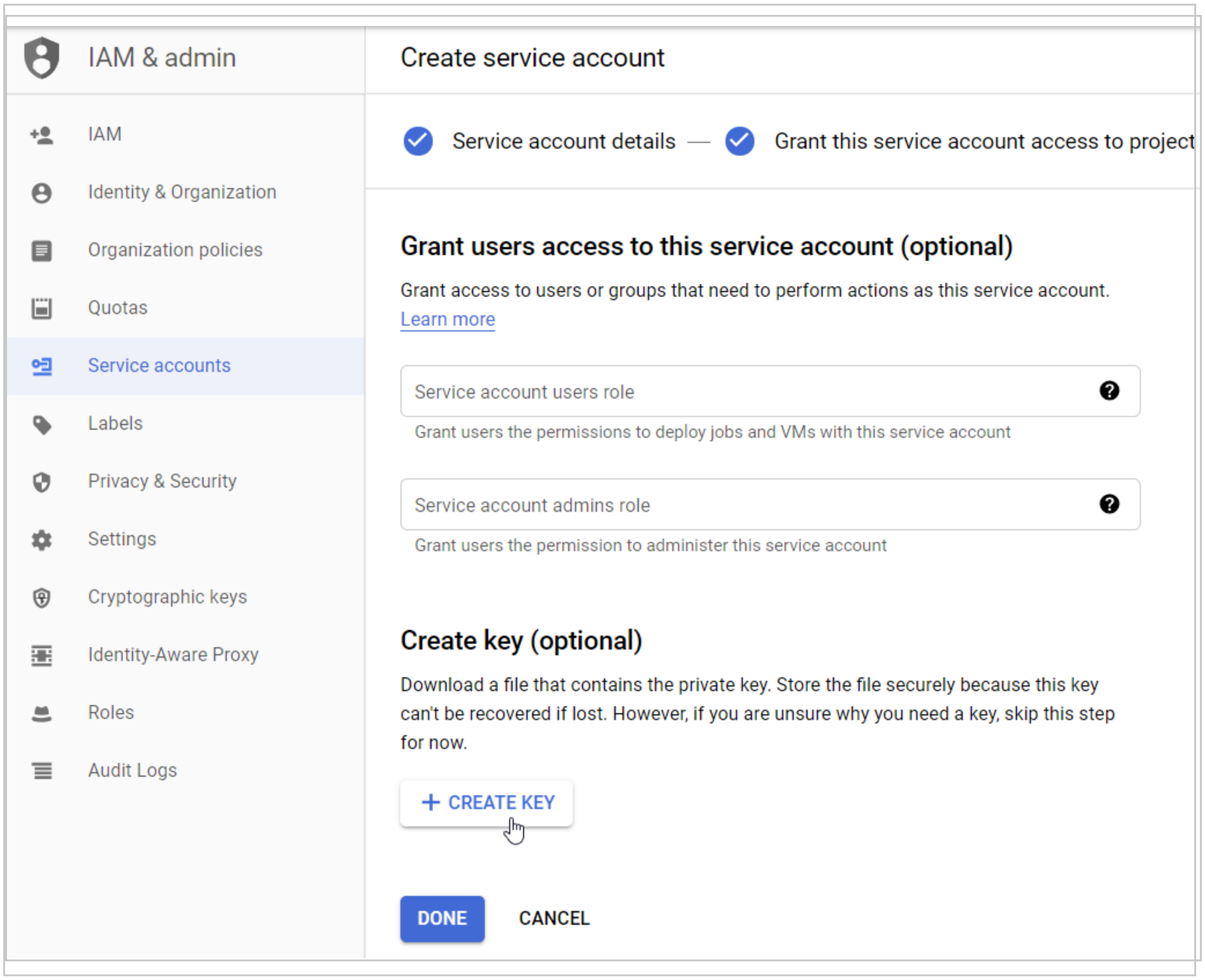
Grant this service account access to Project01 so that it has permission to complete specific actions on the resources in your project. Learn more

Role: Compute Viewer

Read-only access to get and list information about all Compute Engine resources, including instances, disks, and firewalls. Allows getting and listing information about disks, images, and snapshots, but does not allow reading the data stored on them.

You have now assigned the Compute Viewer role.

11. Click **+ CREATE KEY**.



Create service account

✓ Service account details — ✓ Grant this service account access to project

Grant users access to this service account (optional)

Grant access to users or groups that need to perform actions as this service account. Learn more

Service account users role

Grant users the permissions to deploy jobs and VMs with this service account

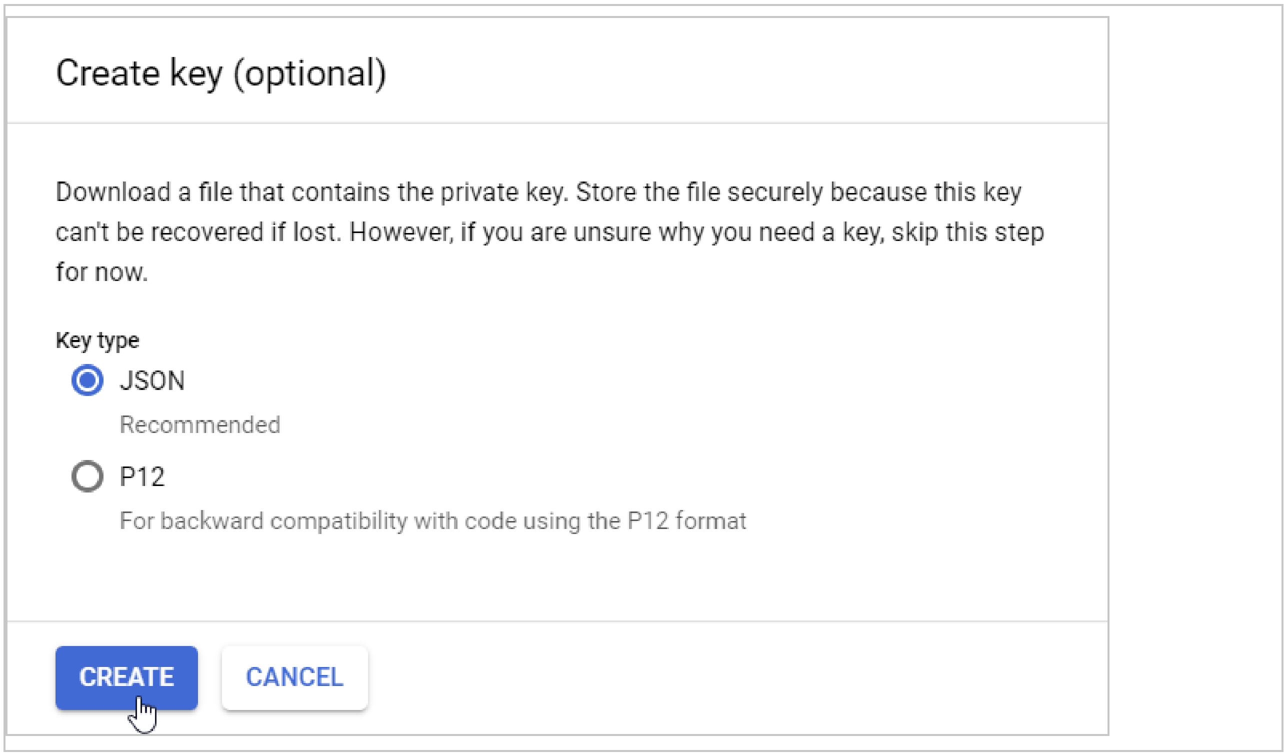
Service account admins role

Grant users the permission to administer this service account

Create key (optional)

Download a file that contains the private key. Store the file securely because this key can't be recovered if lost. However, if you are unsure why you need a key, skip this step for now.

12. Select **JSON** and click **CREATE**.



Create key (optional)

Download a file that contains the private key. Store the file securely because this key can't be recovered if lost. However, if you are unsure why you need a key, skip this step for now.

Key type

● JSON
Recommended

○ P12
For backward compatibility with code using the P12 format

The key is generated and placed in a JSON file.

13. Save the key (JSON file) to a safe place.
14. Place the JSON file in a location that is accessible to Deep Security Manager for later upload. If you need to move or distribute the file, make sure you do so using secure methods.
15. Click **DONE**.

    You have now created a GCP service account with necessary roles, as well as a service account key in JSON format. The service account is created under the selected project (`Project01`), but can be associated with additional projects. For details, see the following section.

    **Note:** It will take 60 seconds - 7 minutes for the IAM permissions to propagate through the system. See this Google article for details.

## Add more projects to the GCP service account

If you have multiple projects in GCP, you must associate them with the service account you just created. All your projects (and underlying VMs) will then become visible in Deep Security

Manager when you later add the service account to Deep Security Manager.

> **Note:** If you have many projects, you might find it easier to divide them up across multiple GCP accounts instead of adding them all to just 1, as described below. For details on a multi-GCP account setup, see "Create multiple GCP service accounts" on page 614.

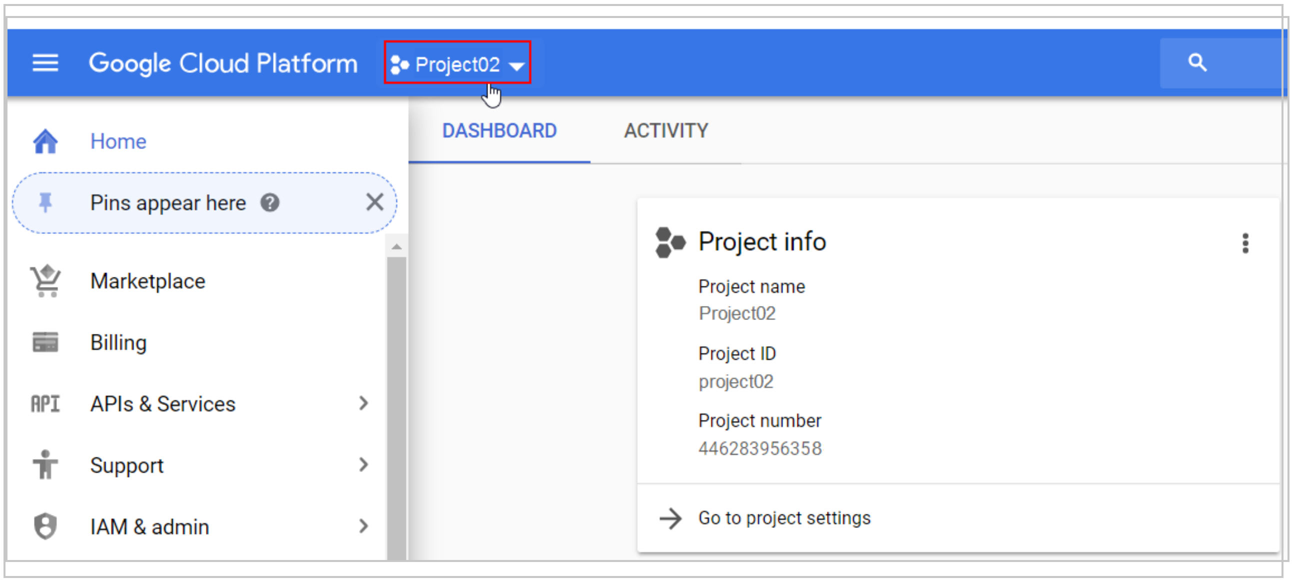
Follow this procedure to associate additional projects with 1 service account:

1. Before you begin, make sure you have completed the procedures in "Prerequisite: Enable the Google APIs" on page 606 and "Create a GCP service account" on page 607.
2. Determine the email of the GCP service account you just created, as follows:
   a. In Google Cloud Platform, from the drop-down list at the top, select the project under which you created the GCP service account (in our example, **Project01**).
   b. On the left, expand **IAM & Admin > Service accounts**.
   c. In the main pane, look under the **Email** column to find the GCP service account email. For example:

      ```
      gcp-deep-security@project01.iam.gserviceaccount.com
      ```

      The service account email includes the name of the project under which it was created.

   d. Note this address or copy it to the clipboard.
3. Still in Google Cloud Platform, go to *another* project by selecting it from the drop-down list at the top. For example: `Project02`.



Project name
Project02
Project ID
project02
Project number
446283956358

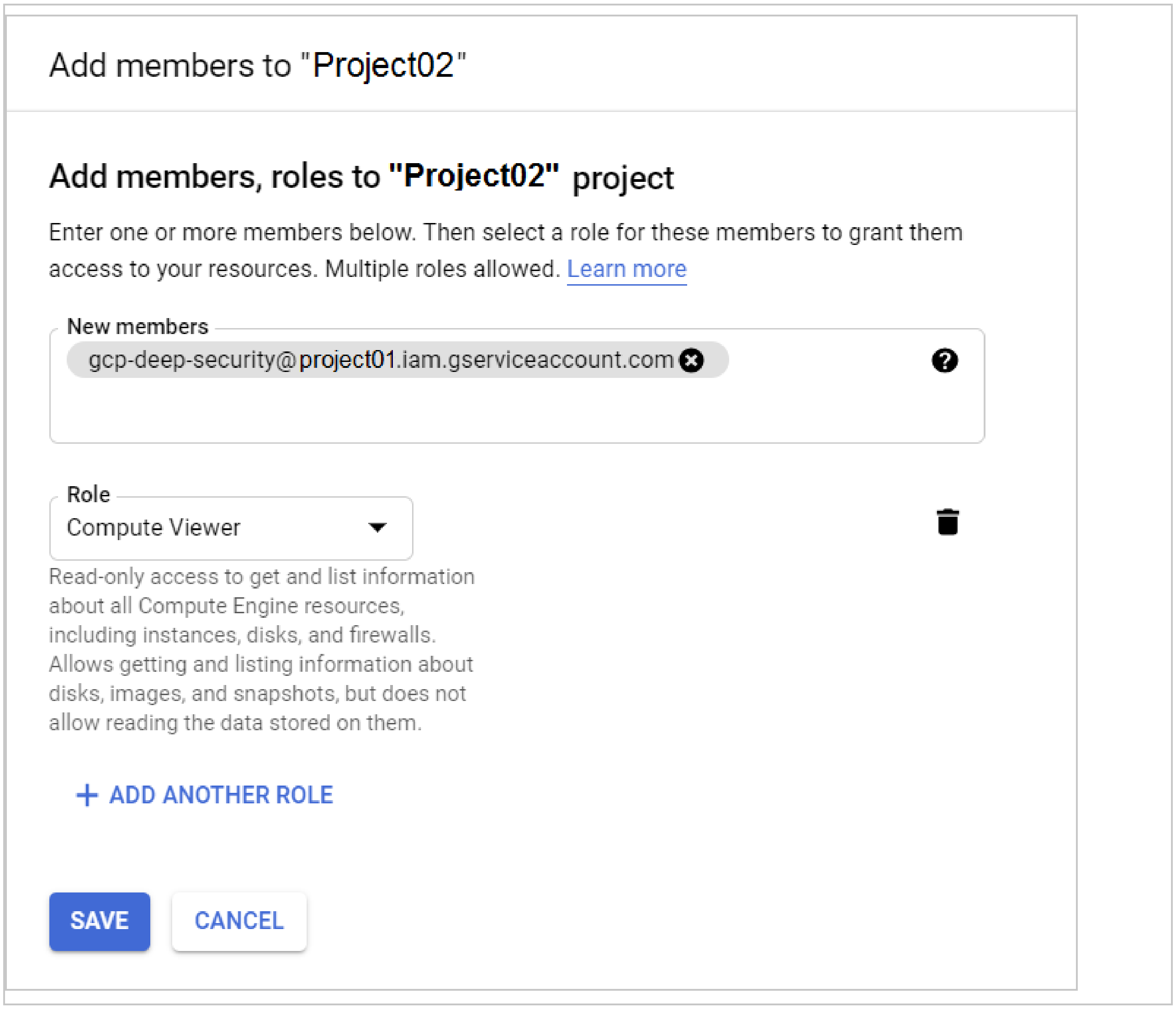
4. Click **Google Cloud Platform** at the top to make sure you're on the Home screen.
5. From the tree view on the left, click **IAM & admin > IAM**.

6. Click **ADD** at the top of the main pane.
7. In the **New members** field, paste the `Project01` GCP service account email address. For example:

   `gcp-deep-security@project01.iam.gserviceaccount.com`

   **Tip:** You can also start typing the email address to auto-fill the field.

8. In the **Select a role** drop-down list, select the **Compute Engine > Compute Viewer** role, or click inside the **Type to filter** area and enter `compute viewer` to find it.



Add members to "Project02"

Add members, roles to "Project02" project

Enter one or more members below. Then select a role for these members to grant them access to your resources. Multiple roles allowed. Learn more

New members: gcp-deep-security@project01.iam.gserviceaccount.com

Role: Compute Viewer

Read-only access to get and list information about all Compute Engine resources, including instances, disks, and firewalls. Allows getting and listing information about disks, images, and snapshots, but does not allow reading the data stored on them.

You have now added the service account with the Compute Viewer role to `Project02`.

9. Click **SAVE**.

10. Repeat steps 1 - 9 in this procedure for each project that you want to associate with the GCP service account.

For more information on how to create a service account, refer to the following page from Google:

https://cloud.google.com/compute/docs/access/create-enable-service-accounts-for-instances

You are now ready to add the GCP account you just created to Deep Security Manager. Proceed to "Add a Google Cloud Platform account" below.

### Create multiple GCP service accounts

Normally, you would create a single GCP service account for Deep Security Manager and associate all your projects to it. This configuration is straightforward and works well for smaller organizations with fewer projects. If, however, you have a large number of projects, having them all under the same GCP service account might make them difficult to manage. In this scenario, you can divide your projects across multiple GCP service accounts. Here's how you would set this up, assuming your projects were spread across your organization's Finance and Marketing departments:

1. Create a `Finance GCP Deep Security` GCP service account for Deep Security Manager.
2. Add finance-related projects to `Finance GCP Deep Security`.
3. Create a `Marketing GCP Deep Security` GCP service account for Deep Security Manager.
4. Add marketing-related projects to `Marketing GCP Deep Security`.

   For detailed instructions, see "Create a GCP service account" on page 607 and "Add more projects to the GCP service account" on page 611

5. After creating the GCP service accounts, add them to Deep Security Manager one by one, following the instructions "Add a Google Cloud Platform account" below.

## Add a Google Cloud Platform account

When you add a Google Cloud Platform (GCP) account to Deep Security, all GCP VM instances associated with that account are imported into Deep Security Manager and become visible in:

- Deep Security Manager > **Computers** > *your_GCP_service_account* > *your_GCP_project*

Once imported, the GCP VM instances can be managed like any other computer.

**Note:** Adding a GCP account to Deep Security Manager is equivalent to adding a GCP connector through the Deep Security API.

Topics:

- "What are the benefits of adding a GCP account?" below
- "Configure a proxy setting for the GCP account" below
- "Add a GCP account to Deep Security" below
- "Remove a GCP account" on page 617
- "Synchronize a GCP account" on page 618

## What are the benefits of adding a GCP account?

The benefits of adding a GCP account (through Deep Security Manager > **Computers > Add GCP Account**) instead of adding individual GCP VMs (through Deep Security Manager > **Computers > Add Computer**), are:

- Changes in your GCP VM inventory are automatically reflected in Deep Security Manager. For example, if you delete a number of VM instances in GCP, those instances disappear automatically from the manager. By contrast, if you use **Computers > Add Computer**, GCP instances that you've deleted remain visible in the manager until you manually delete them.
- VMs are organized into projects in the manager, which lets you easily see which GCP VMs are protected and which are not. Without the GCP account, all your GCP VMs appear at the same root level under **Computers**.

## Configure a proxy setting for the GCP account

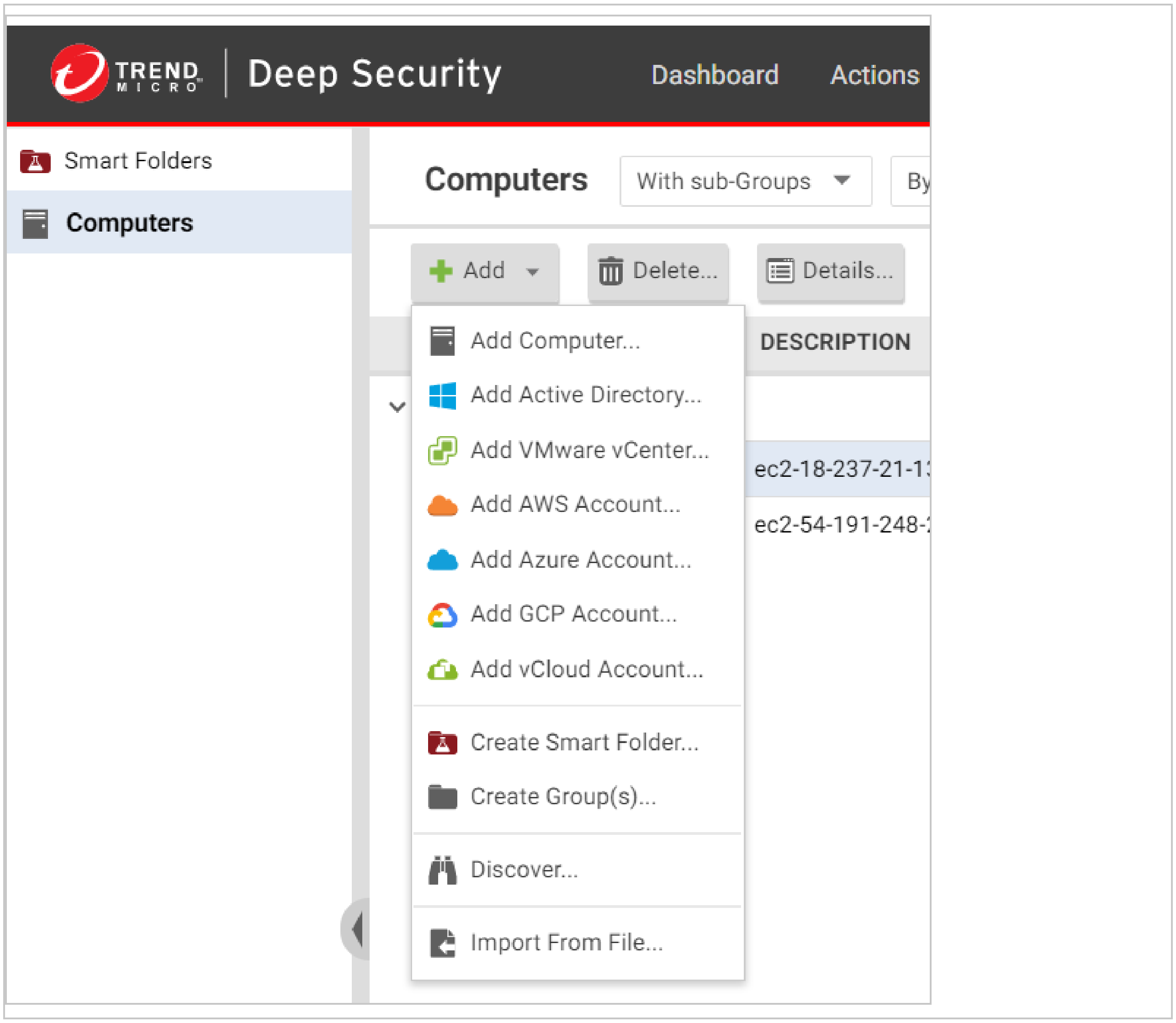
Optionally, you can configure the Deep Security Manager to use a proxy server to access resources in GCP service accounts. For details, see "Connect to cloud accounts via proxy" on page 1340.

## Add a GCP account to Deep Security

To add a GCP account to Deep Security Manager:

1. If you have not done so already, "Create a Google Cloud Platform service account" on page 606 for Deep Security.

2. In Deep Security Manager, go to **Computers > Add > Add GCP Account**.

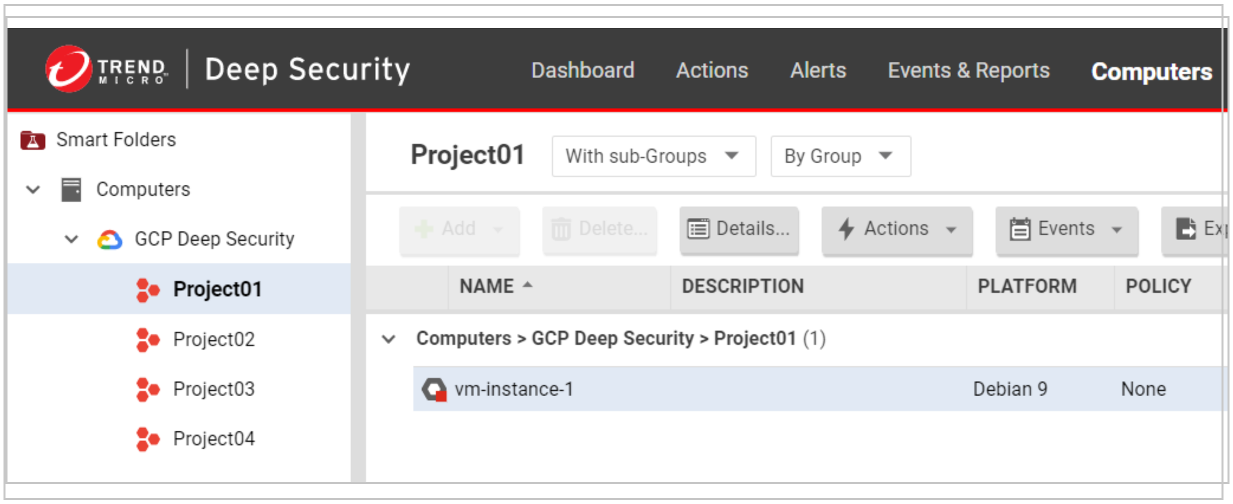


3. Enter a **Display Name**. We recommend using the GCP service account name. Examples: `GCP Deep Security`, `Finance GCP Deep Security`, `Marketing GCP Deep Security`.
4. Choose the **Service Account Key**. The key is a JSON file that you saved earlier, when creating the GCP service account. See "Create a Google Cloud Platform service account" on page 606 for details.
5. Click **Next**.
6. Review the summary information, and then click **Close**.

   The following occurs:

- Deep Security Manager displays your GCP service account and its associated projects in their own branch on the left side of the **Computers** page (see image below). Associated VMs are displayed in the main pane. You can right-click your GCP service account name and select **Synchronize Now** to see the latest set of GCP VMs.
- If you previously added VM instances from this service account through the **Computers > Add Computers** option (instead of the **Computers > Add GCP Account** option described here), these VMs are moved to the correct project under the service account you just added. This move occurs only for VMs that have *Deep Security Agent 12.0 or later installed*. VMs with pre-12.0 agents remain listed under the root **Computers** folder.

  The following image shows the imported GCP service account, projects, and a VM.



| NAME | DESCRIPTION | PLATFORM | POLICY |
|---|---|---|---|
| Computers > GCP Deep Security > Project01 (1) | | | |
| vm-instance-1 | | Debian 9 | None |

7. Repeat the steps in this procedure for each GCP service account you want to add.

   You have now added a GCP service account to Deep Security Manager. Proceed to "Install the agent on Google Cloud Platform VMs" on page 564 if you have not done so already.

## Remove a GCP account

Removing a GCP account from the Deep Security Manager permanently removes the account from the Deep Security database. This does not affect the GCP account. VM instances with Deep Security Agents continue to be protected, but do not receive security updates. If you later reactivate Deep Security Agents on these VM instances, the Deep Security Agents will download the latest security updates at the next scheduled update.

To remove a GCP account:

1. In Deep Security Manager, click **Computers** at the top.
2. Right-click the GCP account in the tree view on the left, and select **Remove Cloud Account**.
3. Confirm that you want to remove the account.

   The account is removed from the Deep Security Manager.

### Synchronize a GCP account

When you synchronize (sync) a GCP account, Deep Security Manager connects to the GCP API to obtain and display the latest set of GCP VMs.

To force a sync immediately:

1. In Deep Security Manager, click **Computers**.
2. On the left, right-click your GCP account and select **Synchronize Now**.

There is also a background sync that occurs every 10 minutes, and this interval is not configurable. If you force a sync, the background sync is unaffected and continues to occur according to its original schedule.

# Add VMWare VMs

## Add a VMware vCenter

You can import a VMware vCenter into Deep Security Manager and then protect its virtual machines with an agent.

**Note:** You cannot import a vCenter that is using vShield Manager.

You have the following options for adding a vCenter:

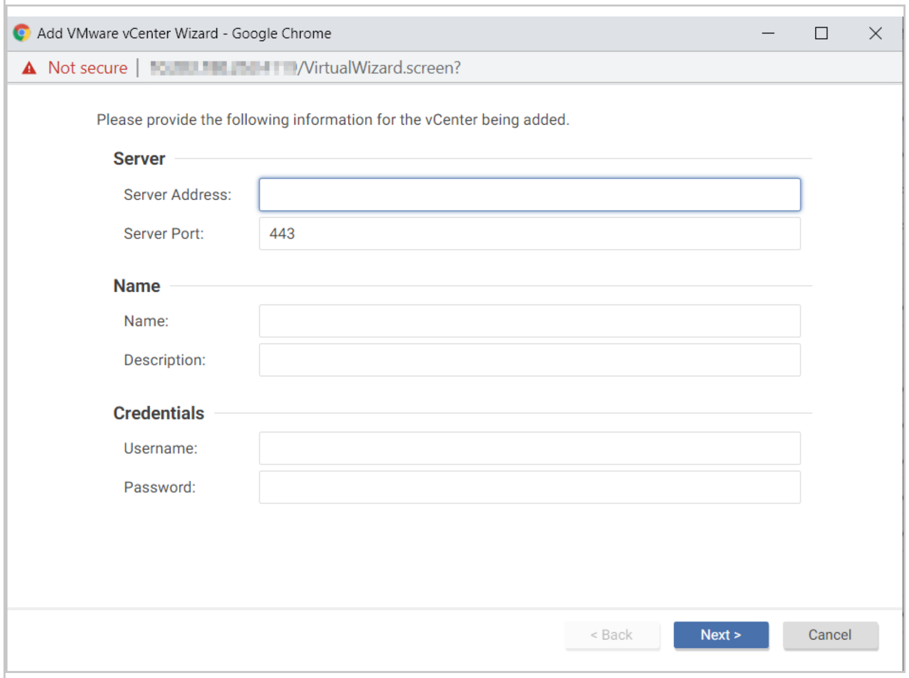
- "Add a vCenter" on the next page
- "Add a vCenter - FIPS mode" on page 621

**Note:** Deep Security Manager supports vCenter High Availability environments in Active or Passive mode.

## Add a vCenter

1. In Deep Security Manager, go to **Computers > Add > Add VMware vCenter**.

   The following page appears:



Add VMware vCenter Wizard - Google Chrome
Not secure | [redacted]/VirtualWizard.screen?

Please provide the following information for the vCenter being added.

Server

Server Address:

Server Port: 443

Name

Name:

Description:

Credentials

Username:

Password:

2. Enter vCenter information:
   - **Server Address**: The vCenter server's IP address (or host name if DNS is configured and able to resolve FQDNs to IP addresses).
   - **Server Port**: The port number to connect to the vCenter (443 by default).
   - **Name**: The name of the vCenter that will appear in the manager.
   - **Description**: A description for the vCenter.
   - **Username** and **Password**: Enter the user name and password of a vCenter user account. This account must conform to the specifications in the tables below, and is required to synchronize the VM inventory between vCenter and Deep Security Manager.

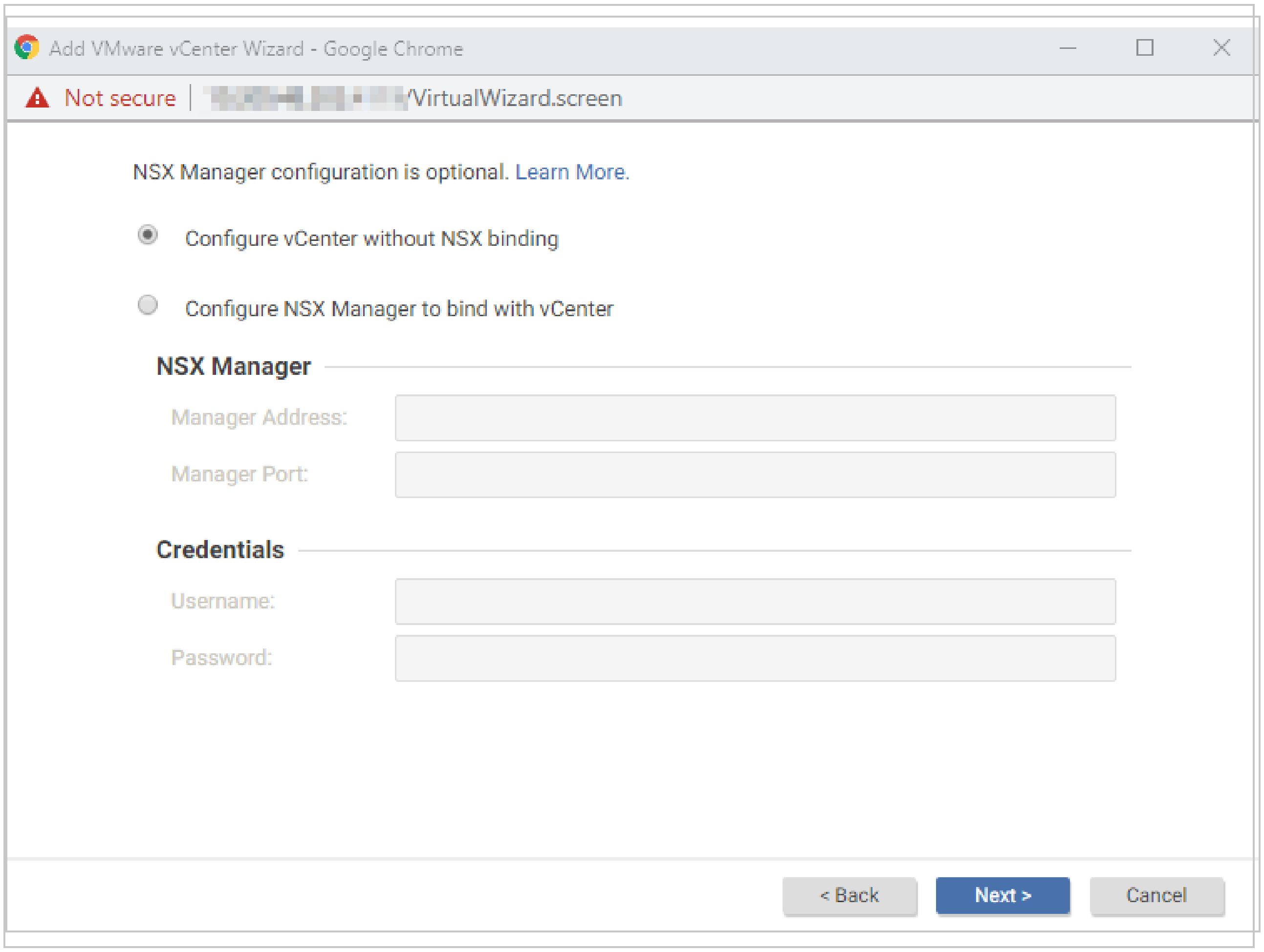
> **Note:** Applying the **Read Only** role at the **Hosts and Clusters** or **Virtual Machine** level in vCenter causes synchronization problems.

**vCenter user account specifications**

| Protection method | NSX Type | vCenter user account specifications |
|---|---|---|
| agent only | No NSX-V or NSX-T integration | The vCenter user account must have the vCenter **Read Only** role (or another role that has equal or greater privileges) at the data center level. |

3. Accept the vCenter TLS (SSL) certificate.
4. Click **Next**.

   The following page appears:



Add VMware vCenter Wizard - Google Chrome

Not secure | [redacted]/VirtualWizard.screen

NSX Manager configuration is optional. Learn More.

● Configure vCenter without NSX binding

○ Configure NSX Manager to bind with vCenter

NSX Manager

Manager Address:

Manager Port:

Credentials

Username:

Password:

**Note:** If you don't see the NSX binding options at the top of the page, it's because you're using an older version of the manager. Upgrade your manager to FR 2019-12-12 to see the options.

5. Fill out the page as follows:
   - Make sure **Configure vCenter without NSX binding** is selected and click **Next**. NSX is not supported with the Deep Security Manager VM from Azure Marketplace.
6. Click **Next**.
7. Review the vCenter information and click **Finish**.
8. The **VMware vCenter has been successfully added** message is displayed. Click **Close**.The vCenter will appear on the **Computers** page.

In a large environment with more than 3000 machines reporting to a vCenter Server, this process may take 20 to 30 minutes to complete. You can check the vCenter's Recent Task section to verify if there are activities running.

Deep Security Manager will maintain real-time synchronization with this VMware vCenter to keep the information displayed in Deep Security Manager (number of VMs, their status, etc.) up to date.

### Add a vCenter - FIPS mode

To add a vCenter when Deep Security Manager is in FIPS mode:

1. Import the vCenter and NSX Manager TLS (SSL) certificates into Deep Security Manager before adding the vCenter to the manager. See "Manage trusted certificates" on page 1525.
2. Add a vCenter following the steps in "Add a vCenter" on page 619. The steps are exactly the same, except that in FIPS mode you will see a Trusted Certificate section on the vCenter page. Click **Test Connection** to check whether the vCenter's SSL certificate has been imported successfully into Deep Security Manager. If there are no errors, click **Next** and continue on through the wizard.

## Add virtual machines hosted on VMware vCloud

To import cloud resources into Deep Security Manager, Deep Security users must first have a account with which to access the cloud provider service resources. For each Deep Security user who will import a cloud account into the Deep Security Manager, Trend Micro recommends creating a dedicated account for that Deep Security Manager to access the cloud resources. That is, users should have one account to access and control the virtual machines themselves, and a separate account for their Deep Security Manager to connect to those resources.

**Note:** Having a dedicated account for Deep Security ensures that you can refine the rights and revoke this account at any time. It is recommended to give Deep Security an access key or secret key with read-only rights at all times.

**Note:** The Deep Security Manager only requires read-only access to import the cloud resources and mange their security.

**Note:** When FIPS mode is enabled, you cannot add virtual machines hosted on VMware vCloud. See "FIPS 140 support" on page 1639.What are the benefits of adding an Azure account?

Topics in this section:

## What are the benefits of adding a vCloud account?

The benefits of adding a vCloud account (through Deep Security Manager > **Computers > Add vCloud Account**) instead of adding individual vCloud resources (through Deep Security Manager > **Computers > Add Computer**), are:

- Changes in your cloud resource inventory are automatically reflected in Deep Security Manager. For example, if you delete a number of instances from vSphere, those instances disappear automatically from the manager. By contrast, if you use **Computers > Add Computer**, cloud instances that are deleted from vCenter remain visible in the manager until they are manually deleted.
- Cloud resources are organized into their own branch in the manager, which lets you easily see which resources are protected and which are not. Without the vCloud account, all your cloud resources appear at the same root level under **Computers**.

## Proxy setting for cloud accounts

You can configure Deep Security Manager to use a proxy server specifically for connecting to instances being protected in cloud accounts. The proxy setting can be found in **Administration > System Settings > Proxies > Proxy Server Use > Deep Security Manager (Cloud Accounts - HTTP Protocol Only)**.

## Create a VMware vCloud Organization account for the manager

1. Log in to VMware vCloud Director.
2. On the **System** tab, go to **Manage And Monitor**.
3. In the left navigation pane, click **Organizations**.
4. Double-click the Organization you wish to give the Deep Security user access to.
5. On the **Organizations** tab, click **Administration**.
6. In the left navigation pane, go to **Members > Users**.
7. Click the " plus " sign to create a new user.
8. Enter the new user's credentials and other information, and select **Organization Administrator** as the user's **Role**.

   **Note:** **Organization Administrator** is a simple pre-defined Role you can assign to the new user account, but the only privilege required by the account is **All Rights > General > Administrator View** and you should consider creating a new vCloud role with just this permission.

9. Click **OK** to close the new user's properties window.

The vCloud account is now ready for access by a Deep Security Manager.

**Note:**
To import the VMware vCloud resources into the Deep Security Manager, users will be prompted for the **Address** of the vCloud, their **User name** , and their **Password** .

The **User name** must include "@orgName". For example if the vCloud account's username is **kevin** and the vCloud Organization you've given the account access to is called **CloudOrgOne**, then the Deep Security user must enter **kevin@CloudOrgOne** as their username when importing the vCloud resources.

(For a vCloud administrator view, use **@system**.)

## Import computers from a VMware vCloud Organization Account

1. In the Deep Security Manager, go to **Computers**.
2. Right-click **Computers** in the navigation panel and select **Add vCloud Account** to display the **Add vCloud Cloud Account** wizard.
3. In **Name** and **Description**, enter the resources you are adding. (These are only used for display purposes in the Deep Security Manager.)
4. In **Address**, enter the hostname or address of vCloud Director.

5. In **User Name** and **Password**, enter vCloud authentication credentials. User names should have the format **username@vcloudorganization**.
6. Click **Next**.
7. Deep Security Manager will verify the connection to the cloud resources and display a summary of the import action. Click **Finish**.

The VMware vCloud resources now appear in the Deep Security Manager under their own branch on **Computers**.

## Import computers from a VMware vCloud Air data center

1. In the Deep Security Manager, go to the **Computers** section, right-click **Computers** in the navigation panel and select **Add vCloud Account** to display the **Add vCloud Account** wizard.
2. Enter a **Name** and **Description** of the vCloud Air data center you are adding. (These are only used for display purposes in the Deep Security Manager.)

3. Enter the **Address** of the vCloud Air data center.

   To determine the address of the vCloud Air data center:

   a. Log in to your vCloud Air portal.
   b. On the **Dashboard** tab, click on the data center you want to import into Deep Security. This will display the **Virtual Data Center Details** information page.
   c. In the Related Links section of the **Virtual Data Center Details** page, click on **vCloud Director API URL**. This will display the full URL of the vCloud Director API.
   d. Use the hostname only (not the full URL) as the Address of the vCloud Air data center that you are importing into Deep Security.
4. In **User Name** and **Password**, enter virtual data center credentials. User names should have the format **username@virtualdatacenterid**.
5. Click **Next**.
6. Deep Security Manager will verify the connection to the vCloud Air data center and display a summary of the import action. Click **Finish**.

The VMware vCloud Air data center now appears in the Deep Security Manager under its own branch on **Computers**.

## Configure software updates for cloud accounts

Relays are modules within Deep Security Agents that are responsible for the download and distribution of Security and Software updates. Normally, the Deep Security Manager informs the relays when new updates are available, the relays get the updates and then the agents get their updates from the relays.

However, if your Deep Security Manager is in an enterprise environment and you are managing computers in a cloud environment, relays in the cloud may not be able to communicate with Deep Security Manager. You can solve this problem by allowing the relays to obtain software updates directly from the Trend Micro Download Center when they cannot connect to the Deep Security Manager. To enable this option, go to **Administration > System Settings > Updates** and under **Software Updates**, select **Allow Relays to download software updates from Trend Micro Download Center when Deep Security Manager is not accessible**.

### Remove a cloud account

Removing a cloud provider account from Deep Security Manager permanently removes the account from the Deep Security database. Your account with your cloud provider is unaffected and any Deep Security agents that were installed on the instances will still be installed, running, and providing protection (although they will no longer receive security updates.) If you decide to re-import computers from the Cloud Provider Account, the Deep Security Agents will download the latest Security Updates at the next scheduled opportunity.

1. Go to the **Computers** page, right-click on the Cloud Provider account in the navigation panel, and select **Remove Cloud Account**.
2. Confirm that you want to remove the account.
3. The account is removed from the Deep Security Manager.

## Control CPU usage

The Deep Security Agent CPU usage control is available for agents with Anti-Malware enabled on Linux.

You can use the Deep Security console to configure the CPU usage, as follows:

1. Open the computer where you want to enable the agent CPU usage control.
2. Click **Settings > General**.
3. Under **CPU Usage Control**, select one of the following CPU protection modes:
    - **Extremely Low**: Asynchronous deferred real-time scan for newly created and modified files. Cannot be enabled or disabled for Predictive Machine Learning and Behavior Monitoring via **Anti-Malware > General > Real-Time Scan > Malware Scan Configuration > Edit**.

- **Low**: Synchronous real-time scan for newly created and modified files within a certain time period, as well as executable files.
- **Unlimited**: Full protection via a real-time scan (default).

## Migrate to the new cloud connector functionality

If you previously used **Add Cloud Account** to import Amazon Web Services resources into Deep Security Manager, those resources are organized by AWS region on **Computers**. You may have run the wizard more than once if you have multiple AWS regions.

The latest versions of Deep Security enable you to display your AWS instances under your AWS account name, organized in a hierarchy that includes the AWS region, VPC, and subnet.

Before migrating your AWS resources, edit the policy that allows Deep Security to access your AWS account:

1. Log in to your Amazon Web Services console and go to **Identity and Access Management (IAM)**.
2. Click **Policies** on the left.
3. In the list of policies, select the policy that permits Deep Security to access your AWS account.
4. Go to the **Policy Document** tab and click **Edit**.
5. Edit the policy document to include the following JSON code:

```
{
        "Version": "2012-10-17",
        "Statement": [
                {
                        "Sid": "cloudconnector",
                        "Effect": "Allow",
                        "Action": [
                                "ec2:DescribeImages",
                                "ec2:DescribeInstances",
                                "ec2:DescribeRegions",
                                "ec2:DescribeSubnets",
                                "ec2:DescribeTags",
                                "ec2:DescribeVpcs",
                                "iam:ListAccountAliases",
                                "sts:AssumeRole"
                        ],
                        "Resource": [
                                "*"
                        ]
                }
        ]
}
```

The `"sts:AssumeRole"` permission is required only if you are using cross-account role access. For more information on IAM roles, see [Delegate access across AWS accounts using IAM roles](#).

6. Select **Save as default version**.

To migrate your AWS resources in Deep Security Manager:

1. Go to **Computers**.
2. On the left, right-click an AWS region and select **Upgrade to Amazon Account**.
3. Click **Finish**.
4. Click **Close**.

Your AWS instances appear under your AWS account name, organized in a hierarchy that includes the AWS region, VPC, and subnet.

# Protect Docker containers

The benefits of a Docker deployment are real, but so is the concern about the significant attack surface of the Docker host's operating system (OS) itself. Like any well-designed software deployment, OS hardening and the use of best practices for your deployment, such as the Center for Internet Security (CIS) Docker Benchmark, provide a solid foundation as a starting point. Once you have a secure foundation in place, adding Deep Security to your deployment gives you access to Trend Micro’s extensive experience protecting physical, virtual, and cloud workloads as well as to real-time threat information from the Trend Micro Smart Protection Network. Deep Security both protects your deployment as well as helps meet and maintain continuous compliance requirements. See "Docker compatibility" on page 401 for information on supported Docker editions and releases.

Deep Security protects your Docker hosts and containers running on Linux distributions. Deep Security can do the following:

- Identify, find, and protect Docker hosts within your deployment through the use of badges and smart folders.

- Protect Docker hosts and containers from vulnerabilities to guard them against known and zero-day exploits by virtually patching new found vulnerabilities.
- Provide anti-malware detection in real time, as well as via manual and scheduled scans, for the file systems used on Docker hosts.
- Provide real-time anti-malware detection for the file systems used within the containers.

- Assert the integrity of the Docker host for continuous compliance and to protect your deployment using the following techniques:
  - Prevent the unauthorized execution of applications on Docker hosts by helping you control which applications are allowed to run in addition to the Docker daemon.
  - Monitor Docker hosts for unexpected changes to system files.
  - Notify you of suspicious events in your OS logs.

Deep Security Docker protection works at the OS level. This means that Deep Security Agent must be installed on the Docker host's OS, not inside a container.

**Note:** Communication between containers in the pod is not supported.

Beginning with Deep Security 10.1, Deep Security supports Docker in swarm mode while using an overlay network.

## Deep Security protection for Docker hosts

The following Deep Security modules can be used to protect the Docker host:

- Intrusion Prevention (IPS)
- Anti-Malware
- Integrity Monitoring
- Log Inspection
- Application Control
- Firewall
- Web Reputation

## Deep Security protection for Docker containers

The following Deep Security modules can be used to protect Docker containers:

- Intrusion Prevention
- Anti-Malware (real-time scans only; scheduled and manual scans are not supported)

## Limitation on Intrusion Prevention recommendation scans

Although Deep Security Intrusion Prevention controls work at the host level, it also protects container traffic on the exposed container port numbers. Since Docker allows multiple applications to run on the same Docker host, a single Intrusion Prevention policy is applied to all Docker applications. This means that recommendation scans should not be relied upon for Docker deployments.

# Protect OpenShift containers

Red Hat OpenShift enables applications inside and outside Kubernetes clusters to run applications where it makes the most sense. OpenShift's basic security includes security hardening and FIPS (Federal Information Processing Standard) compliant encryption (FIPS 140-2 Level 1).

Once you have a secure foundation in place, adding Deep Security to your OpenShift deployment gives you access to Trend Micro’s extensive experience protecting physical, virtual, and cloud workloads as well as to real-time threat information from the Trend Micro Smart Protection Network. Deep Security both protects your deployment as well as helps meet and maintain continuous compliance requirements.

Deep Security protects your OpenShift hosts and containers running on Red Hat Linux distributions. Deep Security can do the following:

- Identify, find, and protect OpenShift hosts within your deployment
- Provide "Enable and configure Anti-Malware" on page 742 for the file systems used on OpenShift hosts and within the containers

**Note:** Communication between containers in the pod is not supported.

## Deep Security protection for the OpenShift host

The following Deep Security modules can be used to protect the OpenShift host:

- Anti-Malware (excluding On-demand scan)

## Deep Security protection for OpenShift containers

The following Deep Security modules can be used to protect OpenShift containers:

- Anti-Malware (excluding On-demand scan)

# Configure policies

## Create policies

Policies allow collections of rules and configuration settings to be saved for easier assignment to multiple computers. You can use the **Policy editor**[1] to create and edit policies that you can then apply to one or more computers. You can also use the **Computer editor**[2] (which is very similar to the Policy editor) to apply settings to a specific computer, but the recommended method is to create specialized policies rather then edit the settings in the Computer editor.

> **Tip:** You can automate policy creation and configuration using the Deep Security API. For examples, see the Create and Configure Policies guide in the Deep Security Automation Center.

In this article:

- "Create a new policy" on the next page
- "Other ways to create a policy" on the next page
- "Edit the settings for a policy or individual computer" on page 632
- "Assign a policy to a computer" on page 633
- "Disable automatic policy updates" on page 633
- "Send policy changes manually" on page 633
- "Export a policy" on page 634

[1] To open the Policy editor, go to the Policies page and double-click the policy that you want to edit (or select the policy and click Details).

[2] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

## Create a new policy

1. Click **Policies > New > New Policy**.
2. Enter a name for the policy. If you want the new policy to inherit its settings from an existing policy, select a policy from the **Inherit from** list. Click **Next**.

   Tip: For information on inheritance, see "Policies, inheritance, and overrides" on page 634.

3. Select whether you want to base this policy on an existing computer's configuration and then click **Next**.
4. If you selected **Yes** in step 3:
   a. Select a computer to use as the basis for the new policy and click **Next**.
   b. Specify which protection modules will be enabled for the new policy. If this policy is inheriting its settings from an existing policy, those settings will be reflected here. Click **Next**.
   c. On the next screen, select the properties that you want to carry into the new policy and click **Next**. Review the configuration and click **Finish**.
5. If you selected **No** in step 3, specify which protection modules will be enabled for the new policy. If this policy is inheriting its settings from an existing policy, those settings will be reflected here. Click **Finish**.
6. Click **Close**. Next, you can edit the settings for the policy, as described in "Edit the settings for a policy or individual computer" on the next page.

## Other ways to create a policy

There are several ways to create a policies on the **Policies** page:

- Create a new policy as described above.
- Click **New > Import From File** to import policies from an XML file.
- Note: When importing policies, ensure that the system where you created the policies and the system that will receive them both have the latest security updates. If the system that is receiving the policies is running an older security update, it may not have some of the rules referenced in the policies from the up-to-date system.
- Duplicate (and then modify and rename) an existing policy. To do so, right-click an existing policy you want to duplicate and then click **Duplicate**.

- Create a new policy based on a recommendation scan of a computer. To do so, go to the **Computers** page, right-click a computer and select **Actions > Scan for Recommendations**. When the scan is complete, return to the **Policies** page and click **New** to display the **New Policy** wizard. When prompted, choose to base the new policy on "an existing computer's current configuration". Then select "Recommended Application Types and Intrusion Prevention Rules", "Recommended Integrity Monitoring Rules", and "Recommended Log Inspection Rules" from among the computer's properties.
- **Note:** The Policy will consist only of recommended elements on the computer, regardless of what Rules are currently assigned to that computer.

## Edit the settings for a policy or individual computer

The **Policies** page shows your existing policies in their hierarchical tree structure. To edit the settings for a policy, select it and click **Details** to open the policy editor.

These sections are available in the **Computer or Policy editor**[1]:

- Overview (the "Overview section of the policy editor" on page 657 and "Overview section of the computer editor" on page 651 are different)
- Anti-Malware
- Web Reputation
- Device Control
- Firewall
- Intrusion Prevention
- Integrity Monitoring
- Log Inspection
- Application Control
- Interface Types
- Settings
- Overrides

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

## Assign a policy to a computer

1. Go to **Computers**.
2. Select your computer from the Computers list, right click and choose **Actions > Assign Policy**.
3. Select the policy from the hierarchy tree and click **OK**.

One of the following occurs:

- If you set the communication direction to **Manager Initiated** or **Bidirectional**, the policy is sent immediately to the agent computer.
- If you set the communication direction to **Agent/Appliance Initiated**, then the policy is sent when the next agent heartbeat occurs.

For more information on how child policies in a hierarchy tree can inherit or override the settings and rules of parent policies, see "Policies, inheritance, and overrides" on the next page.

After assigning a policy to a computer, you should still run periodic recommendation scans on your computer to make sure that all vulnerabilities on the computer are protected. See "Manage and run recommendation scans" on page 639 for more information.

## Disable automatic policy updates

By default, any changes to a security policy are automatically sent to the computers that use the policy. You can change this so automatic sending is disabled, and you must manually send the policy.

1. Open the **Policy editor**[1] for the policy to configure.
2. Go to **Settings > General > Send Policy Changes Immediately.**
3. Next to **Automatically send Policy changes to computers**, select **Yes** to allow automatic sending of policy changes. To disable automatic sending, and only allow manually sending, select **No**.
4. Click **Save** to apply the changes.

## Send policy changes manually

If you make a policy change and want to send the policy changes manually to a particular computer, follow the instructions below.

[1] To open the Policy editor, go to the Policies page and double-click the policy that you want to edit (or select the policy and click Details).

1. Go to **Computers** .
2. Double-click your computer from the Computers list.
3. In the navigation pane, make sure **Overview** is selected.
4. In the main pane, click the **Actions** tab.
5. Under **Policy**, click **Send Policy**.

One of the following occurs:

- If you set the communication direction to **Manager Initiated** or **Bidirectional**, the policy is sent immediately to the agent computer.
- If you set the communication direction to **Agent/Appliance Initiated**, then the policy is sent when the next agent heartbeat occurs.

## Export a policy

To export a policy to an XML file, select a policy from the policies tree and click **Export > Export Selected to XML (For Import)**.

Exported policies can only be imported by another Deep Security Manager within the same multi-node cluster. If the goal is to migrate to Workload Security, see the article on how to Migrate policies to Workload Security

**Note:** Deep Security Manager does not support exporting and importing policies with custom rules.

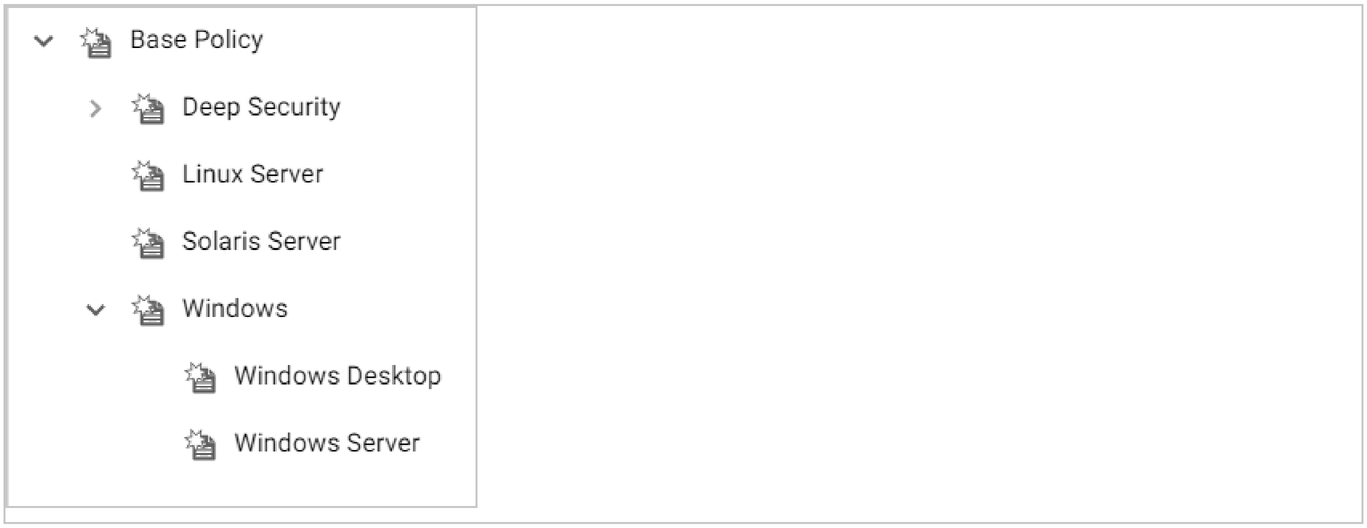
**Note:** When you export a selected policy to XML, any child policies that the policy may have are included in the exported package. The export package contains all the actual objects associated with the policy except: intrusion prevention rules, log inspection rules, integrity monitoring rules, and application types.

# Policies, inheritance, and overrides

Policies in Deep Security are intended to be created in a hierarchical structure. As an administrator, you begin with one or more base policies from which you create multiple levels of child policies that get progressively more granular in their detail. You can assign broadly applicable rules and other configuration settings at the top-level policies and then get more targeted and specific as you go down through levels of child policies, eventually arriving at rule and configuration assignments at the individual computer level.

As well as assigning more granular settings as you move down through the policy tree, you can also override settings from higher up the policy tree.

Deep Security provides a collection of policies that you can use as initial templates for the design of your own policies tailored to your environment:



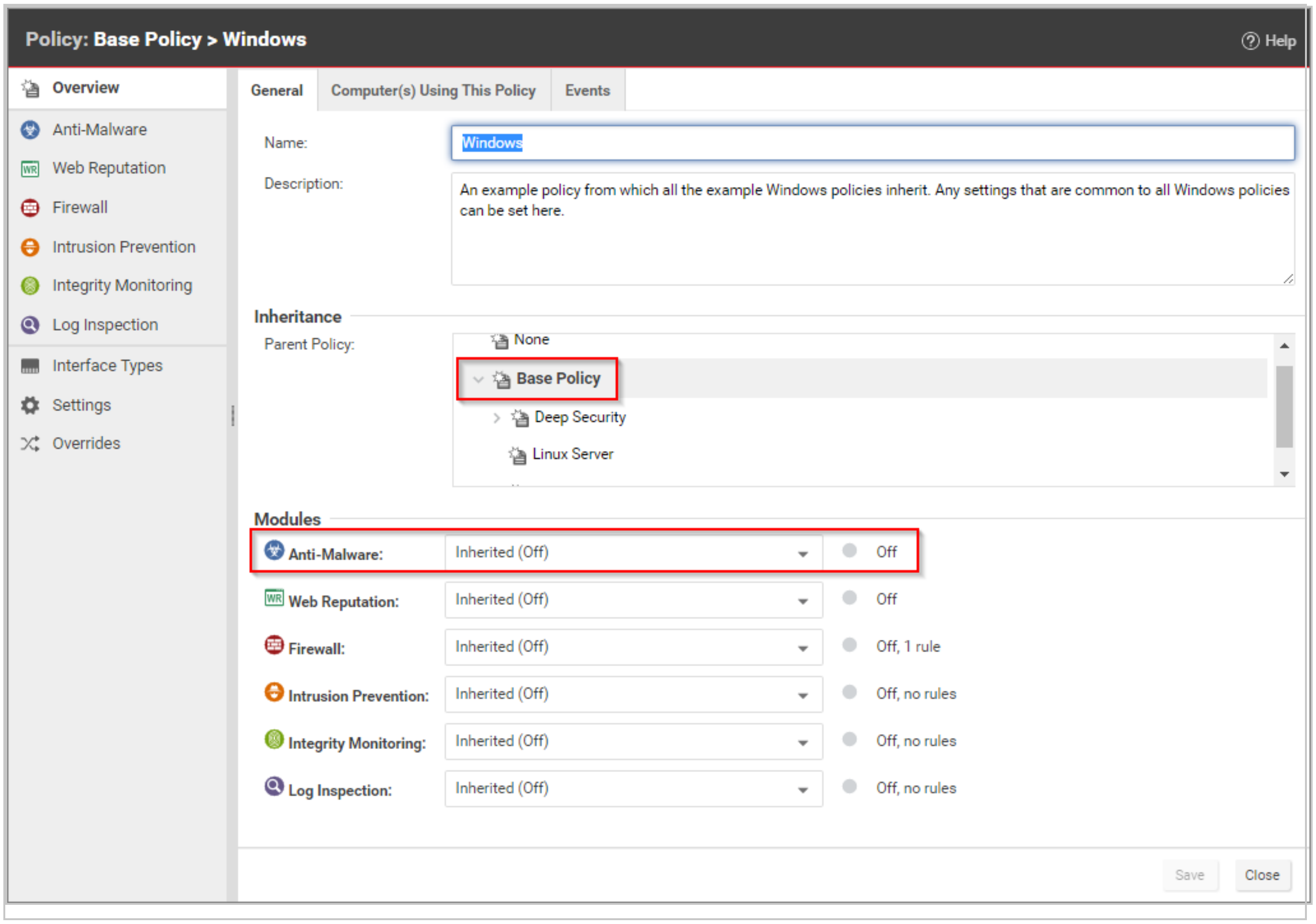
In this topic:

- "Inheritance" below
- "Overrides" on the next page
- "View the overrides on a computer or policy at a glance" on page 638

## Inheritance

Child policies inherit their settings from their parent policies. This allows you to create a policy tree that begins with a base parent policy configured with settings and rules that will apply to all computers. This parent policy can then have a set of child and further descendant policies which have progressively more specific targeted settings. Your policy trees can be built based on any kind of classification system that suits your environment. For example, the branch in the policy tree that comes with Deep Security has two child policies, one designed for a server hosting the Deep Security Manager and one designed for the Deep Security Virtual Appliance. This is a role-based tree structure. Deep Security also has three branches designed for specific operating systems, Linux, Solaris, and Windows. The windows branch has further child policies for various sub-types of Windows operating systems.

In the **Windows** policy editor on the **Overview** page, you can see that the **Windows** policy was created as a child of the **Base** policy. The policy's anti-malware setting is **Inherited (Off)**:



Name: Windows

Description: An example policy from which all the example Windows policies inherit. Any settings that are common to all Windows policies can be set here.

Inheritance

Parent Policy:
None
Base Policy
Deep Security
Linux Server

Modules

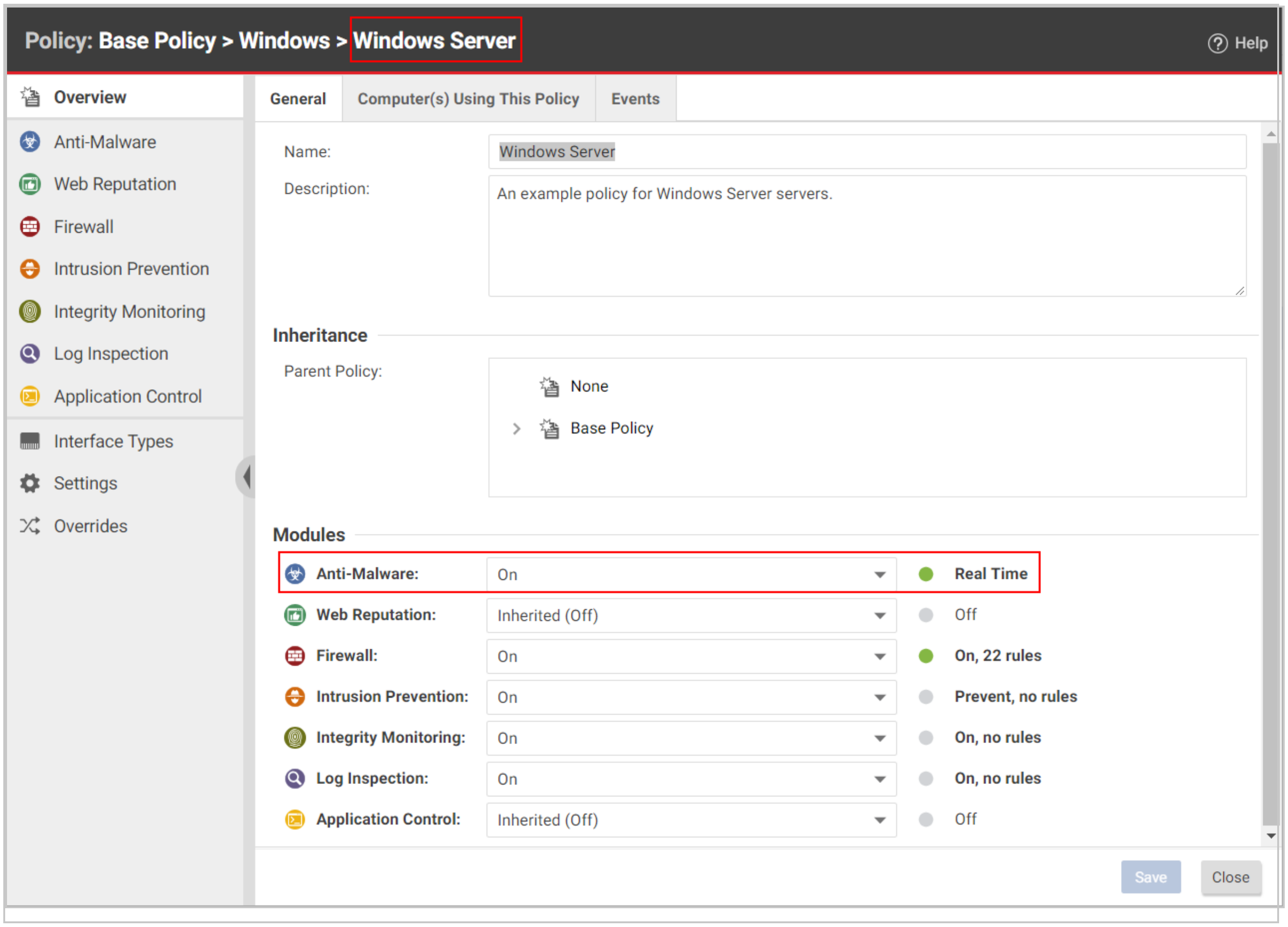
| | | |
|---|---|---|
| Anti-Malware: | Inherited (Off) | ○ Off |
| Web Reputation: | Inherited (Off) | ○ Off |
| Firewall: | Inherited (Off) | ○ Off, 1 rule |
| Intrusion Prevention: | Inherited (Off) | ○ Off, no rules |
| Integrity Monitoring: | Inherited (Off) | ○ Off, no rules |
| Log Inspection: | Inherited (Off) | ○ Off, no rules |

This means that the setting is inherited from the parent **Base** policy, and that if you were to change the anti-malware setting in the **Base** policy from **Off** to **On**, the setting would change in the **Windows** policy as well. (The **Windows** policy setting would then read **Inherited (On)**. The value in parentheses always shows you what the current inherited setting is.)

## Overrides

The **Overrides** page shows you how many settings have been overridden at this policy or specific computer level. To undo the overrides at this level, click the **Remove** button.

In this example, the **Windows Server** policy is a child policy of the **Windows** policy. Here, the anti-malware setting is no longer inherited; it is overridden and hard-set to **On**.



Policy: Base Policy > Windows > Windows Server

Name: Windows Server

Description: An example policy for Windows Server servers.

Inheritance

Parent Policy:
- None
- Base Policy

Modules

| | | |
|---|---|---|
| Anti-Malware: | On | ● Real Time |
| Web Reputation: | Inherited (Off) | ● Off |
| Firewall: | On | ● On, 22 rules |
| Intrusion Prevention: | On | ● Prevent, no rules |
| Integrity Monitoring: | On | ● On, no rules |
| Log Inspection: | On | ● On, no rules |
| Application Control: | Inherited (Off) | ● Off |

Tip: You can automate override checking, creation, and removal using the Deep Security API. For examples, see the Configure Computers to Override Policies guide in the Deep Security Automation Center.

## Override object properties

The intrusion prevention rules that are included in this policy are copies of the intrusion prevention rules stored by the Deep Security Manager which are available for use by any other policies. If you want to change the properties of a particular rule, you have two choices: modify the properties of the rule globally so that the changes you make apply to all instances where the rule is in use, or modify the properties locally so that the changes you make only apply locally. The default editing mode in a Computer or policy editor is **local**. If you click **Properties** on the **Assigned Intrusion Prevention Rules** area toolbar, any changes you make in the Properties window that appears will only apply locally. (Some properties like the rule name can't be edited locally, only globally.)

Right-clicking a rule displays a context menu which gives you the two Properties editing mode options: selecting **Properties** will open the local editor window and **Properties (Global)** will open the global editor window.

Most of the shared common objects in Deep Security can have their properties overridden at any level in the policy hierarchy right down to the individual computer level.

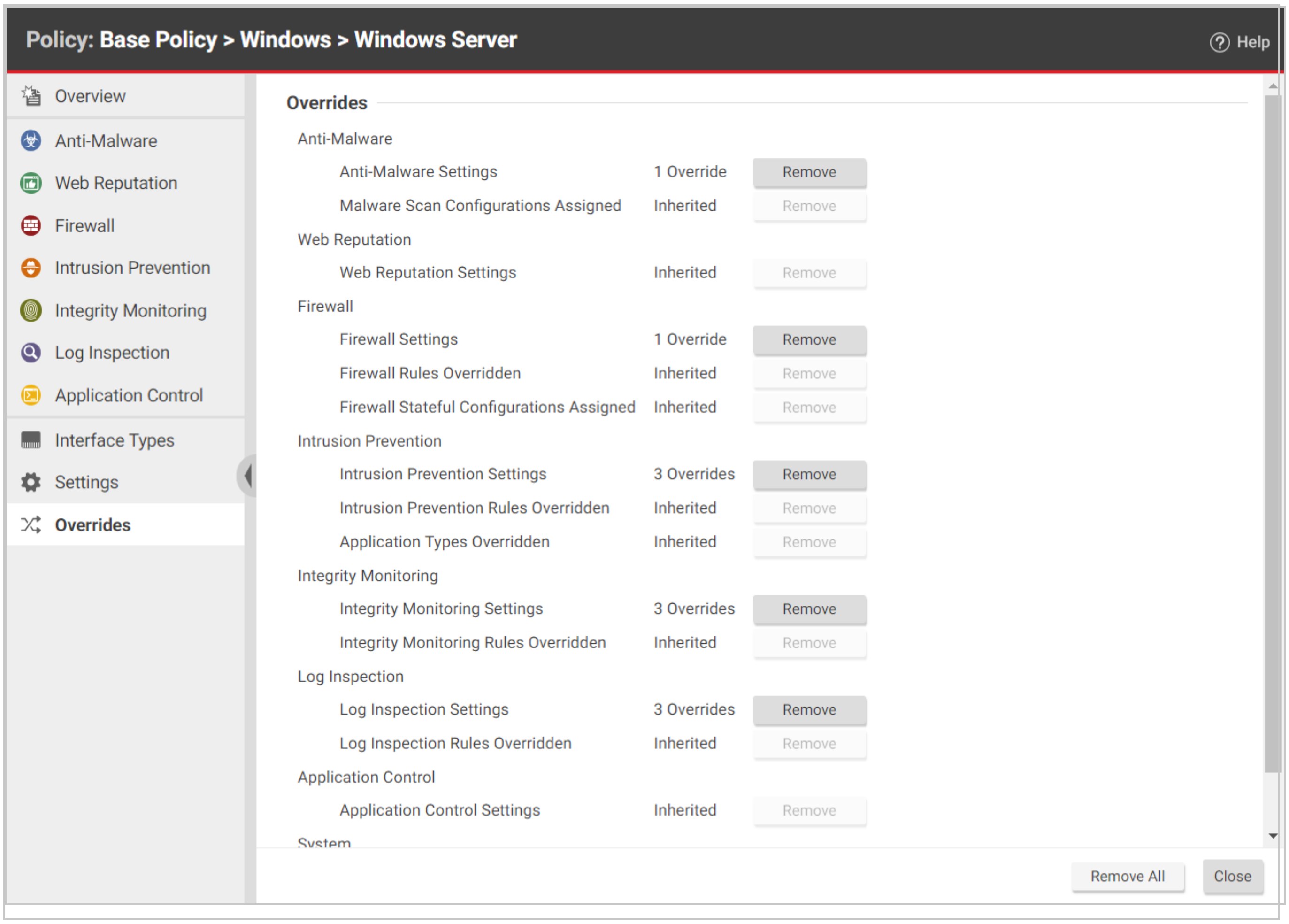
### Override rule assignments

You can always assign additional rules at any policy or computer level. However, rules that are in effect at a particular policy or computer level because their assignment is inherited from a parent policy cannot be unassigned locally. They must be unassigned at the policy level where they were initially assigned.

> Tip: If you find yourself overriding a large number of settings, you should probably consider branching your parent policy.

## View the overrides on a computer or policy at a glance

You can see the number of settings that have been overridden on a policy or a computer by going to the **Overrides** page in the computer or policy Editor:



Overrides

| | | | |
|---|---|---|---|
| Anti-Malware | | | |
| | Anti-Malware Settings | 1 Override | Remove |
| | Malware Scan Configurations Assigned | Inherited | Remove |
| Web Reputation | | | |
| | Web Reputation Settings | Inherited | Remove |
| Firewall | | | |
| | Firewall Settings | 1 Override | Remove |
| | Firewall Rules Overridden | Inherited | Remove |
| | Firewall Stateful Configurations Assigned | Inherited | Remove |
| Intrusion Prevention | | | |
| | Intrusion Prevention Settings | 3 Overrides | Remove |
| | Intrusion Prevention Rules Overridden | Inherited | Remove |
| | Application Types Overridden | Inherited | Remove |
| Integrity Monitoring | | | |
| | Integrity Monitoring Settings | 3 Overrides | Remove |
| | Integrity Monitoring Rules Overridden | Inherited | Remove |
| Log Inspection | | | |
| | Log Inspection Settings | 3 Overrides | Remove |
| | Log Inspection Rules Overridden | Inherited | Remove |
| Application Control | | | |
| | Application Control Settings | Inherited | Remove |
| System | | | |

Overrides are displayed by protection module. You can revert system or module overrides by clicking the **Remove** button.

## Manage and run recommendation scans

Deep Security can run recommendation scans on computers to help identify intrusion prevention, integrity monitoring, and log inspection rules that should be applied or removed.

> Tip: Recommendation scans provide a good starting point for establishing a list of rules that you should implement, but there are some important additional rules that are not identified by recommendation scans. You should implement those rules manually. See "Implement additional rules for common vulnerabilities" on page 647

You can configure recommendation scans and implement the recommended rules for individual computers or at the policy level. For large deployments, Trend Micro recommends managing recommendations through policies. This way, you can make all your rule assignments from a single source (the policy) rather than having to manage individual rules on individual computers. This can mean that some rules are assigned to computers on which they are not required; however, the minimal effect on performance is outweighed by the ease of management that results from using policies. If you enable recommendation scans in policies, use separate policies for scanning Windows and Linux computers, to avoid assigning Windows rules to Linux computers, and vice-versa.

- "What gets scanned?" below
- "Scan limitations" below
- "Adobe Reader rules recommendation" on page 642
- "Run a recommendation scan" on page 642
- "Automatically implement recommendations" on page 645
- "Check scan results and manually assign rules" on page 646
- "Configure recommended rules" on page 647
- "Implement additional rules for common vulnerabilities" on page 647
- "Troubleshooting: Recommendation Scan Failure" on page 649

## What gets scanned?

During a recommendation scan, Deep Security Agents scan the operating system for:

- installed applications
- the Windows registry
- open ports
- the directory listing
- the file system
- running processes and services
- environment variables
- users

## Scan limitations

Certain technical or logical limitations result in the rules for some types of software not being accurately recommended, or not recommended at all:

- On Unix/Linux systems, the recommendation scan engine might have trouble detecting software that is not installed through the operating system's default package manager, for example, Apache Struts, Wordpress, or Joomla. Applications installed using standard package managers are not a problem.
- On Unix/Linux systems, rules for desktop application vulnerabilities or local vulnerabilities (for example, browsers and media players) are not included in recommendation scans.
- Generic web application protection rules are not included in recommendation scans.
- Smart rules are generally not included in recommendation scans unless they address a major threat or a specific vulnerability. Smart rules address one or more known and unknown (zero-day) vulnerabilities. Rule lists in Deep Security Manager identify smart rules with "Smart" in the Type column.
- When dealing with rules related to a content management system (CMS), the recommendation scan cannot detect the CMS installation and installed version. It also cannot detect the plug-ins installed with a CMS and their versions. As a result, whenever a recommendation scan finds a web server installed and PHP installed or running on a system, all CMS-related intrusion prevention rules get recommended. This may result in the over-recommendation of rules, but balances the need for security vs. accuracy.
- The recommendations for the following web technologies may suggest more rules than necessary, so some tailoring may be required:
  - Red Hat JBoss
  - Eclipse Jetty
  - Apache Struts
  - Oracle WebLogic
  - WebSphere
  - Oracle Application Testing Suite
  - Oracle Golden Gate
  - Nginx
- OpenSSL rules are recommended on Windows only when OpenSSL is explicitly installed. If OpenSSL in being used internally by an application but it was not installed as a separate package, a recommendation scan does not detect it.
- On Linux systems, rules for Java-related vulnerabilities do not get recommended if web browsers are the only applicable vector.

- Recommendation scans cannot detect the Adobe Flash Player plug-in that is included in a default Chrome installation. Recommendations are based on the Chrome version, which means some unnecessary rules may be recommended.
- Recommendation scan does not work on Deep Security Manager versions earlier than 20.0.789 (20 LTS Update 2023-06-28).

## Adobe Reader rules recommendation

Adobe Reader rules are often recommended and auto-applied to address Common Vulnerabilities and Exposures (CVEs). Very few of these Adobe CVEs are used in attacks and most do not have a Proof of Concept (PoC) available, but the core Adobe software remains unpatched. This had led to many rules remaining applied and could lead to performance issues.

To reduce potential performance issues caused by a large number of rules, Trend Micro will only recommend Adobe Reader rules that are either used in an attack or have a PoC made available within 1 year of the CVE being discovered. Customers are encouraged to review all recommendations for their environment.

## Run a recommendation scan

Because changes to your environment can affect which rules are recommended, it's best to run recommendation scans on a regular basis (the best practice is to perform recommendation scans on a weekly basis). Trend Micro releases new intrusion prevention rules on Tuesdays, so it's recommended that you schedule recommendation scans shortly after those releases. The use of system resources, including CPU cycles, memory, and network bandwidth, increases during a recommendation scan so it's best to schedule the scans at non-peak times.

There are several ways to run recommendation scans:

- **Scheduled task:** Create a scheduled task that runs recommendation scans according to a schedule that you configure. You can assign the scheduled task to all computers, one individual computer, a defined computer group, or all computers protected by a particular policy. See "Create a scheduled task to regularly run recommendation scans" on the next page.
- **Ongoing scans:** Configure a policy so that all computers protected by the policy are scanned for recommendations on a regular basis. You can also configure ongoing scans for individual computers. This type of scan checks the timestamp of the last scan that occurred and then and follows the configured interval thereafter to perform future scans. This results in recommendation scans occurring at different times in your environment. This setting is

helpful in environments where an agent might not be online for more than a few days (for example, in cloud environments that are building and decommissioning instances frequently). See "Configure an ongoing scan" on the next page

- **Manual scans:** Run a single recommendation scan on one or more computers. A manual scan is useful if you've recently made significant platform or application changes and want to force a check for new recommendations instead of waiting for a scheduled task. See "Manually run a recommendation scan" on the next page.
- **Command line:** Initiate a recommendation scan via the Deep Security command-line interface. See "Command-line basics" on page 1565.
- **API:** Initiate a recommendation scan via the Deep Security API. See "Use the Deep Security API to automate tasks" on page 1598.

**Note:** Scheduled tasks and ongoing scans are each capable of running recommendation scans independently with their own settings. Use either the scheduled tasks or ongoing scans, but not both.

Once a recommendation scan has run, alerts are raised on the all computers for which recommendations have been made.

## Create a scheduled task to regularly run recommendation scans

1. In the Deep Security Manager, go to the **Administration > Scheduled Tasks** page.
2. Click **New** on the toolbar and select **New Scheduled Task** to display the **New Scheduled Task** wizard.
3. In the **Type** list, select **Scan Computers for Recommendations** and then select how often you want the scan to occur. Click **Next**.
4. Depending on your choice in step 3, the next page lets you be more specific about the scan frequency. Make your selection and click **Next**.
5. Now select which computer(s) to scan and click **Next**.

   **Note:** You can select all computers, choose one individual computer, select a group of computers, or select computers that are assigned a particular policy. For large deployments, it's best to perform all actions, including recommendation scans, through policies.

6. Give a name to your new scheduled task, select whether or not to **Run Task on 'Finish'**, click **Finish**.

## Configure an ongoing scan

1. In the Deep Security Manager, open the **Computer or Policy editor**[1], depending on whether you want to configure the scan for an individual computer or for all computers that are using a policy.

   > **Note:** For large deployments, it's best to perform all actions, including recommendation scans, through policies.

2. Click **Settings**. On the **General** tab, under **Recommendations**, the **Perform ongoing Recommendation Scans** setting enables or disables ongoing recommendation scans. The **Ongoing Scan Interval** setting specifies how often the scans occur. Both of those settings can be inherited from the computer or policy's parent (see "Policies, inheritance, and overrides" on page 634 for details about how inheritance works).

## Manually run a recommendation scan

1. In the Deep Security Manager, go to the **Computers** page.
2. Select the computer or computers you want to scan.
3. Click **Actions > Scan for Recommendations**.

## Cancel a recommendation scan

You can cancel a recommendation scan before it starts running.

1. In the Deep Security Manager, go to the **Computers** page.
2. Select the computer or computers where you want to cancel the scans.
3. Click **Actions > Cancel Recommendation Scan**.

## Exclude a rule or application type from recommendation scans

If you don't want a particular rule or application type to be included in recommendation scan results, you can exclude it from scans.

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

1. In the Deep Security Manager, open the **Computer or Policy editor**[1].

   > **Note:** For large deployments, it's best to perform all actions, including recommendation scans, through policies.

2. Depending on which type of rule you want to exclude, go to the **Intrusion Prevention**, **Integrity Monitoring**, or **Log Inspection** page.
3. On the **General** tab, click **Assign/Unassign** (for rules) or **Application Types** (for application types).
4. Double-click the rule or application type that you want to exclude.
5. Go to the **Options** tab. For rules, set **Exclude from Recommendations** to "Yes" or "Inherited (Yes)". For application types, select the **Exclude from Recommendations** checkbox.

## Automatically implement recommendations

You can configure Deep Security to automatically implement recommendation scan results when it is appropriate to do so:

1. In the Deep Security Manager, open the **Computer or Policy editor**[2].

   > **Note:** For large deployments, it's best to perform all actions, including recommendation scans, through policies.

2. Depending on which type of rules you want to implement automatically, go to the **Intrusion Prevention**, **Integrity Monitoring**, and/or **Log Inspection** pages. (You can change the setting independently for each protection module.)
3. On the **General** tab, under **Recommendations**, change the setting to "Yes" or "Inherited (Yes)".

Not all recommendations can be implemented automatically. The exceptions are:

- Rules that require configuration before they can be applied.
- Rules that are excluded from recommendation scans.

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

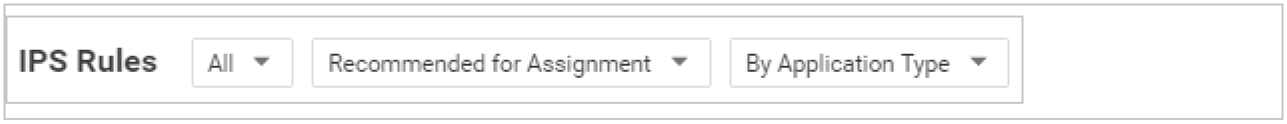
- Rules that have been automatically assigned or unassigned but that a user has overridden. For example, if Deep Security automatically assigns a rule and you subsequently unassign it, the rule is not reassigned after the next recommendation scan.
- Rules that have been assigned at a higher level in the policy hierarchy cannot be unassigned at a lower level. A rule assigned to a computer at the policy level must be unassigned at the policy level.
- Rules that Trend Micro has issued but which may pose a risk of producing false positives. (This will be addressed in the rule description.)

## Check scan results and manually assign rules

The results of the latest recommendation scan are displayed in the **Computer or Policy editor**[1], on the **General** tab of the protection module (**Intrusion Prevention**, **Integrity Monitoring**, and **Log Inspection**).

The example below describes how to deal with intrusion prevention recommendation scan results via a policy:

1. Once a recommendation scan is complete, open the policy that is assigned to the computers you have just scanned.
2. Go to **Intrusion Prevention > General**. The number of unresolved recommendations (if any) is displayed in the **Recommendations** section.
3. Click **Assign/Unassign** to open the rule assignment window.
4. Sort the rules **By Application Type** and select **Recommended for Assignment** from the display filter menu:



   This displays a list of rules that are recommended for assignment but that have not been assigned.

5. To assign a rule to the policy, select the checkbox next to the rule name. Rules flagged with a ⚙ icon have configuration options that you can set. Rules flagged with a ⚠ icon have settings that **must** be configured before the rule is enabled.)

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

Alternatively, to assign several rules at once, use the Shift or Control keys to select the rules, right-click the selection, and click **Assign Rule(s)**.

Tip: The results of a recommendation scan can also include recommendations to unassign rules. This can happen when applications are uninstalled, when security patches from a manufacturer are applied, or when unnecessary rules have been applied manually. To view rules that are recommended for unassignment, select **Recommended for Unassignment** from the display filter menu.

Note: Recommended rules are indicated by a full flag (⚑) . A partial flag (⚑) identifies an application type where only some of the rules that are part of the application type have been recommended.

## Configure recommended rules

Some rules require configuration before they can be applied. For example, some log inspection rules require that you specify the location of the log files to be inspected for change. If this is the case, an alert is raised on the computer on which the recommendation has been made. The text of the alert will contain the information required to configure the rule. In the policy or computer editor, rules flagged with a ⚙ icon have configuration options that you can set. Rules flagged with a ⚠ icon have settings that **must** be configured before the rule is enabled.

## Implement additional rules for common vulnerabilities

Recommendation scans provide a good starting point for establishing a list of rules that you should implement, but there are some additional rules for common vulnerabilities that are not identified by recommendation scans because they need to be carefully configured and tested before being implemented in "prevent" (block) mode. Trend Micro recommends that you configure and test these rules, then manually enable them in your policies (or for individual computers):

Tip: This list includes the most common of the additional rules you should configure. You can find others in Deep Security Manager by searching for rules whose type is "Smart" or "Policy".

| Rule name | Application type |
|---|---|
| 1007598 - Identified Possible Ransomware File Rename Activity Over Network Share | DCERPC Services |
| 1007596 - Identified Possible Ransomware File Extension Rename Activity Over Network Share | DCERPC Services |
| 1006906 - Identified Usage Of PsExec Command Line Tool | DCERPC Services |
| 1007064 - Executable File Uploaded On System32 Folder Through SMB Share | DCERPC Services |
| 1003222 - Block Administrative Share | DCERPC Services |
| 1001126 - DNS Domain Blocker | DNS Client |
| 1000608 - Generic SQL Injection Prevention<br>See "Configure an SQL injection prevention rule" on page 820 for details. | Web Application Common |
| 1005613 - Generic SQL Injection Prevention - 2 | Web Application Common |
| 1000552 - Generic Cross Site Scripting (XSS) Prevention | Web Application Common |
| 1006022 - Identified Suspicious Image With Embedded PHP Code | Web Application Common |
| 1005402 - Identified Suspicious User Agent In HTTP Request | Web Application Common |
| 1005934 - Identified Suspicious Command Injection Attack | Web Application Common |
| 1006823 - Identified Suspicious Command Injection Attack - 1 | Web Application Common |
| 1005933 - Identified Directory Traversal Sequence In Uri Query Parameter | Web Application Common |
| 1006067 - Identified Too Many HTTP Requests With Specific HTTP Method | Web Server Common |

| Rule name | Application type |
|---|---|
| 1005434 - Disallow Upload Of A PHP File | Web Server Common |
| 1003025 - Web Server Restrict Executable File Uploads | Web Server Common |
| 1007212 - Disallow Upload Of An Archive File | Web Server Common |
| 1007213 - Disallow Upload Of A Class File | Web Server Common |

## Troubleshooting: Recommendation Scan Failure

If you are receiving a Recommendation Scan Failure on your server, follow the steps below to resolve the issue. If the issue continues to persist after troubleshooting, create a diagnostic package from the agent and contact support.

### Communication

Typically for communication issues "protocol error" will appear in the body of the error message.

If you don't have open inbound firewall ports from the Deep Security Manger to the agent, open the ports or switch to agent-initiated communication. For more information, see "Activate and protect agents using agent-initiated activation and communication" on page 1386.

### Server resources

Monitor the CPU and memory resources on the server. If the memory or CPU is becoming exhausted during the scan, increase the resources.

### Timeout values

Increase the timeout values for the recommendation scan.

1. Open the command prompt and navigate to the Deep Security Manager installation folder.
2. Enter the commands below (if this is a multi-tenant environment, add the tenant name):

```
dsm_c -action changesetting -name
settings.configuration.agentSocketTimeoutOverride -value 1200
```

```
dsm_c -action changesetting -name
settings.configuration.defaultSocketChannelTimeout -value 1200000
```

```
dsm_c -action changesetting -name
settings.configuration.recoScanKeepAliveTimeInterval -value 180000
```

# Detect and configure the interfaces available on a computer

The Computer and Policy editors contain an **Interfaces** (in the Computer editor) and **Interface Types** (in the Policy editor) section that displays the interfaces detected on the computer. If a policy with multiple interface assignments has been assigned to the computer, interfaces that match the patterns defined in the policy will be identified.

The **Interface Types** section of the Policy editor provides additional capabilities:

## Configure a policy for multiple interfaces

If you have computers with more than one interface, you can assign various elements of a policy (firewall rules, etc.) to each interface.

1. In the Policy editor, click **Interface Types**.
2. In the Network Interface Specificity section, select **Rules can apply to specific interfaces**
3. In the Interface Type sections that appear, type the names and pattern matching strings.

The interface type name is used only for reference. Common names include "LAN", "WAN", "DMZ", and "Wi-Fi", though any name can be used to map to your network's topology.

The interface name used for all container network interfaces and host virtual interfaces is "integrated_veth", which has a MAC address of 02:00:00:00:00:00.

The matches define a wildcard-based interface name to auto map the interfaces to the appropriate interface type. Examples would be "Local Area Connection *", "eth*", or"Wireless *". When an interface cannot be mapped automatically, an alert is triggered. You can manually map it from the **Interfaces** page in the computer editor for a particular computer.

**Note:** If Deep Security detects interfaces on the computer that don't match any of these entries, the manager will trigger an alert.

## Enforce interface isolation

When Interface Isolation is enabled, the firewall will try to match the regular expression patterns to interface names on the local computer. To enforce interface isolation, click **Enable Interface Isolation** option on the **Policy or Computer Editor > Firewall > Interface Isolation** tab and enter string patterns that will match the names of the interfaces on a computer (in order of priority).

**Warning:** Before you enable Interface Isolation make sure that you have configured the interface patterns in the proper order and that you have removed or added all necessary string patterns. Only interfaces matching the highest priority pattern will be permitted to transmit traffic. Other interfaces (which match any of the remaining patterns on the list) will be "restricted". Restricted Interfaces will block all traffic unless an Allow Firewall Rule is used to allow specific traffic to pass through.

Selecting **Limit to one active interface** will restrict traffic to only a single interface even if more than one interface matches the highest priority pattern.

**Note:** Deep Security uses POSIX basic regular expressions to match interface names. For information on basic POSIX regular expressions, see https://pubs.opengroup.org/onlinepubs/009695399/basedefs/xbd_chap09.html#tag_09_03

# Overview section of the computer editor

The computer editor **Overview** page has the following tabbed sections:

- "General tab" below
- "Actions tab" on page 655
- "TPM tab" on page 656
- "System Events tab" on page 657
- "Exceptions tab" on page 657

## General tab

- **Hostname:** Appears in the **Name** column on the **Computers** page. The name must be either the IP address of the computer or the hostname of the computer. Either a fully qualified hostname or a relative hostname can be used if a hostname is used instead of an

IP address. You have to specify a hostname that can be resolved or a valid IP address that the Deep Security Manager can access. This is because the communication between the Deep Security Manager and the agent computers are based on the hostname. For relay-enabled agents, all of the computers within the relay group should be able to reach the specified IP address or hostname. If the Deep Security Manager cannot access the target computer the communication direction should be set to Agent/Appliance Initiated (Settings > Computer).

- **(Last IP Used: *<IP_address>*)**: The last IP used by the computer. **Last IP Used** may not always show the IP address of the Deep Security Agent's host. Instead, it could be the IP address of a proxy, load balancer, elastic load balancer (ELB), etc., that the agent uses to communicate with Deep Security Manager.
- **Display Name:** Appears in the Display Name column and in brackets next to the Hostname value.
- **Description:** a description of the computer.
- **Platform:** Details of the computer's OS will appear here.
- **Group:** The computer group to which the computer belongs appears in the list. You can reassign the computer to any other existing computer group.
- **Policy:** The policy (if any) that has been assigned to this computer.

> **Note:** Keep in mind that if you unassign a policy from a computer, rules may still be in effect on the computer if they were assigned independently of the policy.

- **Asset Importance:** Deep Security Manager uses a ranking system to quantify the importance of security events. Rules are assigned a severity level (high, medium, low, etc.), and assets (computers) are assigned an "asset importance" level. These levels have numerical values. When a rule is triggered on a computer the asset importance value and the severity level value are multiplied together. This produces a score which is used to sort events by importance. (Event ranking can be seen in the **Events** pages.) Use this **Asset Importance** list to assign an asset importance level to this computer. (To edit the numerical values associated with severity and importance levels, go to **Administration > System Settings > Ranking**.)
- **Download Security Updates From:** Use the dropdown list to select which relay group the agent/appliance on this computer will download security updates from. (not displayed if agent is acting as a relay.)

## Computer status

The Status area displays the latest available information about the computer and the protection modules in effect on it. Whether the computer is protected by an agent or an appliance (or both in the case of combined mode) is displayed in the top row.

- **Status:**
  - When the computer is unmanaged the status represents the state of the agent or appliance with respect to activation. The status will display either "Discovered" or "New" followed by the agent or appliance state in brackets ("No Agent/Appliance", "Unknown", "Reactivation Required", "Activation Required", or "Deactivation Required").
  - When the computer is managed and no computer errors are present, the status will display "Managed" followed by the state of the agent or appliance in brackets ("Online" or "Offline").
  - When the computer is managed and the agent or appliance is in the process of performing an action (e.g. "Integrity Scan in Progress", "Upgrading Agent (Install Program Sent)", etc.) the task status will be displayed.
  - When there are errors on the computer (e.g., "Offline", "Update Failed", etc.) the status will display the error. When more than one error is present, the status will display "Multiple Errors" and each error will be listed beneath.

## Protection module status

With Deep Security 9.5 and later, protection modules are deployed to agents on an as-needed basis. Only core functionality is included when an agent is first installed.

The **Status** area provides information about the state of the Deep Security modules. The status reflects the state of a module on the agent as well as its configuration in Deep Security Manager. A status of "On" indicates that the module is configured in Deep Security Manager and is installed and operating on the Deep Security Agent.

A green status light is displayed for a module when it is "On" and working. In addition, modules that allow individual rule assignment must have at least one rule assigned before they will display a green light.

- **Anti-Malware:** Whether Anti-Malware protection is on or off and whether it is configured for real-time or on-demand scans.
- **Web Reputation:** Whether Web Reputation is on or off.

- **Device Control:** Whether Device Control is on or off.
- **Firewall:** Whether the Firewall is on or off and how many rules are in effect.
- **Intrusion Prevention:** Whether Intrusion Prevention is on or off and how many rules are in effect.
- **Integrity Monitoring:** Whether Integrity Monitoring is on or off and how many rules are in effect.
- **Log Inspection:** Whether Log Inspection is on or off and how many rules are in effect.
- **Application Control**: Whether Application Control is on or off.
- **Online:** Indicates whether the manager can currently communicate with the agent or appliance.
- **Last Communication:** The last time the manager successfully communicated with the agent or appliance on this computer.
- **Check Status:** This button allows you to force the manager to perform an immediate heartbeat operation to check the status of the agent or appliance. Check Status will not perform a security update of the agent or appliance. When manager to agent or appliance communications is set to "Agent/Appliance Initiated" the **Check Status** button is disabled. Checking status will not update the logs for this computer. To update the logs for this computer, go to the **Actions** tab.
- **Clear Warnings/Errors:** Dismisses any alerts or errors on this computer.
- **ESXi server:** If the computer is a virtual machine protected by a virtual appliance, the ESXi server that hosts them is displayed.
- **Appliance:** If the computer is a virtual machine protected by a virtual appliance, the protecting appliance is displayed.
- **ESXi Version:** If the computer is an ESXi server, the ESXi version number is displayed.
- **Filter Driver version:** If the computer is an ESXi server, the filter driver version number is displayed. If you are using Deep Security Virtual Appliance 10.0 or later with ESXi 6.0 or later, "N/A" will be displayed because no filter driver is in use.
- **Guests:** If the computer is an ESXi server, the virtual appliance and guests are displayed.
- **Appliance Version:** If the computer is a virtual appliance, the appliance version number is displayed.
- **Protected Guests On:** If the computer is a virtual appliance, the IP of the ESXi server and the protected guest are displayed.

### VMware virtual machine summary

This section displays a summary of hardware and software configuration information about the virtual machine on which the agent or appliance is running (VMware virtual machines only).

## Actions tab

### Activation

A newly installed Deep Security agent or appliance needs to be "activated" by the Deep Security Manager before policies, rules, requests for event logs, etc. can be sent to it. The activation procedure includes the exchange of SSL keys which uniquely identify a manager (or one of its nodes) and an agent/appliance to each other. Once activated by a Deep Security Manager, an agent/appliance will only accept instructions or communicate with the Deep Security Manager which activated it (or one of its nodes).

An unactivated agent or appliance can be activated by any Deep Security Manager.

Agents and appliances can only be deactivated locally on the computer or from the Deep Security Manager which activated it. If an agent or appliance is already activated, the button in this area will read **Reactivate** rather than **Activate**. Reactivation has the same effect as activation. A reactivation will reset the agent or appliance to the state it was in after first being installed and initiate the exchange of a new set of SSL keys.

### Policy

When you change the configuration of an agent or appliance on a computer using the Deep Security Manager (apply a new Intrusion Prevention rule, change logging settings, etc.) the Deep Security Manager has to send the new information to the agent or appliance. This is a "Send Policy" instruction. Policy updates usually happen immediately but you can force an update by clicking the **Send Policy** button.

### Agent Software

This displays the version of the agent or appliance currently running on the computer. If a newer version of the agent or appliance is available for the computer's platform you can click the **Upgrade Agent** or **Upgrade Appliance** button to remotely upgrade the agent or appliance from the Deep Security Manager. You can configure the Deep Security Manager to trigger an alert if new versions of the agent or appliance software running on any of your computers by going to the **Administration > System Settings > Updates** tab.

**Note:** Before updating or uninstalling a Deep Security Agent or Relay on Windows, you must disable agent self-protection. To do this, on the Deep Security Manager, go to **Computer editor**[1] **> Settings > General**. In **Agent Self Protection**, and then either deselect **Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent** or enter a password for local override.

### Support

The **Create Diagnostic Package** button creates a snapshot of the state of the agent or appliance on the computer. Your support provider may request this for troubleshooting purposes.

If you have lost communication with the computer, a diagnostics package can be created locally. For more information, see "Create a diagnostic package" on page 1723.

## TPM tab

**Note:** The TPM tab will appear in place of the Actions tab for ESXi servers.

A Trusted Platform Module (TPM) is a type of chip that is used for hardware authentication. VMware uses the TPM with its ESXi hypervisors. During the boot sequence, an ESXi writes a SHA-1 hash of each hypervisor component to a set of registers as it loads. An unexpected change in these values from one boot sequence to the next can indicate a possible security issue worth investigating. Deep Security can monitor the TPM on an ESXi after every boot and raise an Alert if it detects any changes. If you select the option to enable TPM monitoring on an ESXi that doesn't support it, the option will be automatically disabled.

**Enable TPM Monitoring:** Select to enable Trusted Platform Module monitoring.

**Raise an alert when TPM Monitoring fails to obtain valid register values:** Select to have Deep Security raise an alert if the Trusted Platform Module fails to obtain valid register values for the hypervisor components during the ESXi boot sequence.

**TPM Register Data Imported:** Indicates whether the Trusted Protection Module data has been imported.

**TPM Last Checked:** Indicates when the Trusted Protection Module was last checked. You can click **Check Now** to start a check of the Trusted Platform Module.

[1] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

**Note:** The minimum requirements for TPM monitoring are

- TPM/TXT installed and enabled on the ESXi (consult your VMware documentation for details)
- The Deep Security Integrity Monitoring and Application Control modules must be properly licensed.

### System Events tab

For information about events, see "System events" on page 1233.

### Exceptions tab

#### USB Device Exception rule count limitation

The current supported USB device exception rule count for each computer is 1000.

## Overview section of the policy editor

The Overview section of the policy editor has the following tabbed sections:

- "General tab" below
- "Computer(s) Using This Policy tab" on the next page
- "Events tab" on the next page
- "Exceptions tab" on the next page

### General tab

#### General

- **Name:** Appears in the Display Name column and in brackets next to the Hostname value.
- **Description:** a description of the computer.

#### Inheritance

Identifies the parent policy (if any) from which the current policy inherits its settings.

### Modules

- **Anti-Malware:** Whether anti-malware protection is on or off and whether it is configured for real-time or on-demand scans.
- **Web Reputation:** Whether web reputation is on or off.
- **Device Control:** Whether Device Control is on or off.
- **Firewall:** Whether the firewall is on or off and how many rules are in effect.
- **Intrusion Prevention:** Whether intrusion prevention is on or off and how many rules are in effect.
- **Integrity Monitoring:** Whether integrity monitoring is on or off and how many rules are in effect.
- **Log Inspection:** Whether log inspection is on or off and how many rules are in effect.
- **Application Control:** Whether application control is on or off.

## Computer(s) Using This Policy tab

Lists computers to which this policy has been assigned.

## Events tab

For information about events, see "System events" on page 1233.

## Exceptions tab

### USB Device Exception rule count limitation

The current supported USB device exception rule count for each computer is 1000.

# Network engine settings

To edit the network engine settings of a policy or computer, open the **Policy editor**[1] or the **Computer editor**[2] for the policy or computer to configure and click **Settings > Advanced** .

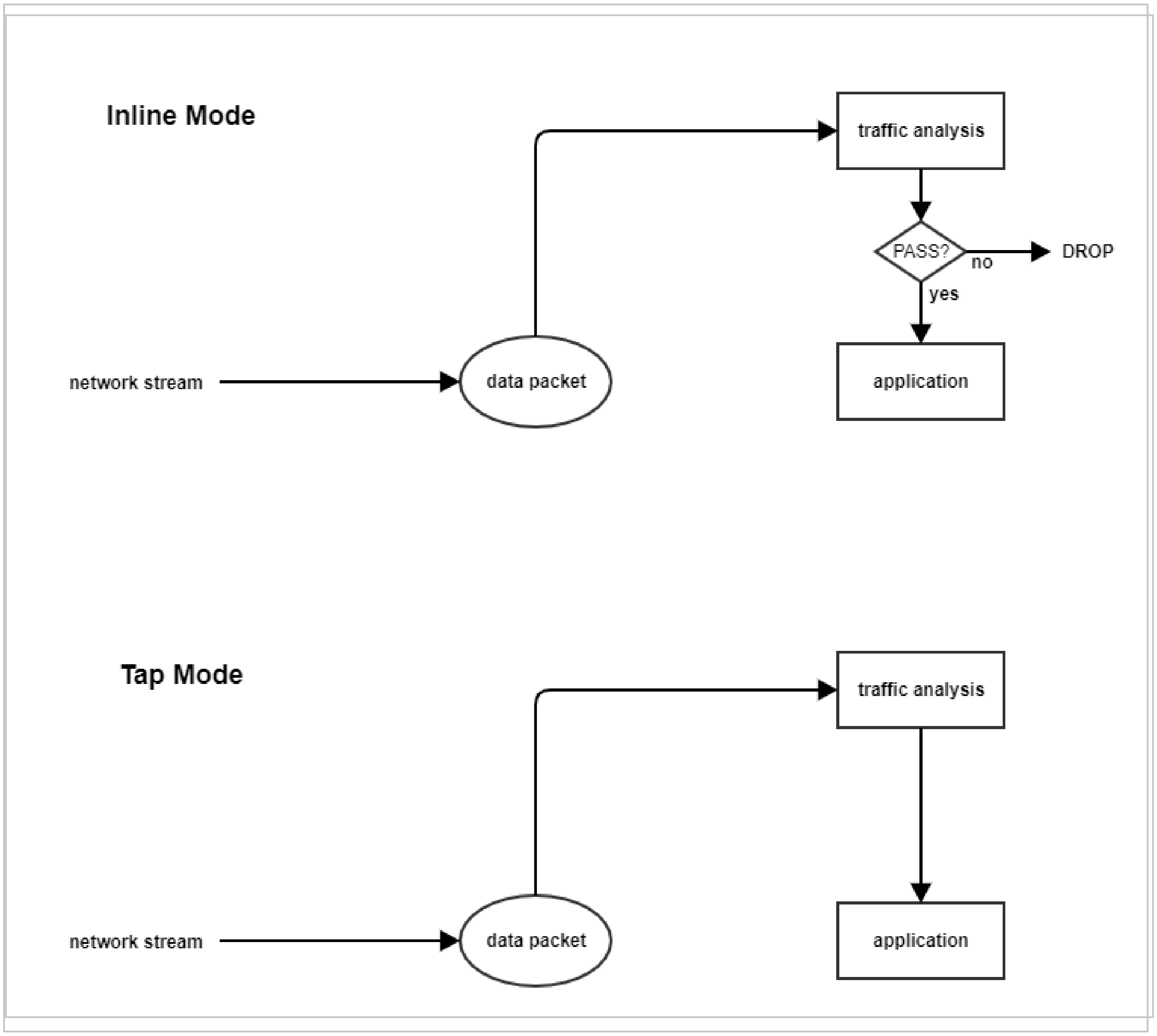
[1] To open the Policy editor, go to the Policies page and double-click the policy that you want to edit (or select the policy and click Details).

[2] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

**Note:** The **Advanced** tab also contains **Events** settings. For information on those settings, see "Limit log file sizes" on page 1052. It also contains the **Generate an Alert when Agent configuration package exceeds maximum size** setting, which controls the display of the **Agent configuration package too large** setting.

The following settings are available:

- **Network Engine Mode** : The network engine is a component within the Intrusion Prevention, Firewall, and Web Reputation modules that decides whether to block or allow packets. For the Firewall and Intrusion Prevention modules, the network engine performs a packet sanity check and also makes sure each packet passes the Firewall and Intrusion Prevention rules (called, rules matching). The network engine can operate inline or in tap mode. When operating inline, the packet stream passes through the network engine and is either dropped or passed based on the rules you've set. Stateful tables are maintained, Firewall rules are applied and traffic normalization is carried out so that Intrusion Prevention and Firewall rules can be applied. When operating in tap mode, the packet is always passed, with the exception of driver hooking issue or interface isolation. In tap mode, packet delay is also introduced, which can create a drop in throughput.



- **Network Engine Status Check**: This setting determines if the agent will monitor the status of the Network Engine. This is enabled by default, but can be disabled. For related events, see Network Engine Status (Windows OS).
- **Failure Response**: The settings here determine how the network engine behaves when it finds faulty packets. The default is to block them (Fail closed), but you can let some of them through (Fail open) for the reasons explained below.
  - **Network Engine System Failure**: This setting determines whether the network engine blocks or allows faulty packets that occur as a result of system failures on the network engine host, such as out of memory failures, allocated memory failures, and network engine (DPI) decoding failures occur. The options are:

    - **Fail closed** (default): The network engine blocks the faulty packet. It does not perform rules matching. This option provides the highest level of security.
    - **Fail open**: The network engine allows the faulty packet through, does not perform rules matching, and logs an event. Consider using **Fail open** if your agent or virtual appliance frequently encounters network exceptions because of heavy loads or lack of resources.
  - **Network Packet Sanity Check Failure**: This setting determines whether the network engine blocks or allows packets that fail the packet sanity checks. Examples of sanity check failures: Firewall sanity check failures, network layer 2, 3, or 4 attribute check failures, TCP state check failures. The options are:
    - **Fail closed** (default): The network engine blocks the failed packet. It does not perform any rules matching. This option provides the highest level of security.
    - **Fail open**: The network engine allows the failed packet, does not perform any rules matching on it, and logs an event. Consider using **Fail open** if you want to disable the packet sanity checks, but preserve rules matching functionality.
- **Anti-Evasion Posture**: The anti-evasion setting controls the network engine handling of abnormal packets that may be attempting to evade analysis. For details, see "Configure anti-evasion settings" on page 844.
- **Advanced Network Engine Options**: If you deselect the **Inherited** check box, you can customize these settings:
  - **CLOSED timeout:** For gateway use. When a gateway passes on a "hard close" (RST), the side of the gateway that received the RST will keep the connection alive for this amount of time before closing it.
  - **SYN_SENT Timeout:** How long to stay in the SYN-SENT state before closing the connection.
  - **SYN_RCVD Timeout:** How long to stay in the SYN_RCVD state before closing the connection.
  - **FIN_WAIT1 Timeout:** How long to stay in the FIN-WAIT1 state before closing the connection.
  - **ESTABLISHED Timeout:** How long to stay in the ESTABLISHED state before closing the connection.
  - **ERROR Timeout:** How long to maintain a connection in an Error state. (For UDP connections, the error can be caused by any of a variety of UDP problems. For TCP connections, the errors are probably due to packets being dropped by the Firewall.)

- **DISCONNECT Timeout:** How long to maintain idle connections before disconnecting.
- **CLOSE_WAIT Timeout:** How long to stay in the CLOSE-WAIT state before closing the connection.
- **CLOSING Timeout:** How long to stay in the CLOSING state before closing the connection.
- **LAST_ACK Timeout:** How long to stay in the LAST-ACK state before closing the connection.
- **ACK Storm timeout:** The maximum period of time between retransmitted ACKs within an ACK Storm. In other words, if ACKs are being retransmitted at a lower frequency then this timeout, they will NOT be considered part of an ACK Storm.
- **Boot Start Timeout:** For gateway use. When a gateway is booted, there may already exist established connections passing through the gateway. This timeout defines the amount of time to allow non-SYN packets that could be part of a connection that was established before the gateway was booted to close.
- **Cold Start Timeout:** Amount of time to allow non-SYN packets that could belong to a connection that was established before the stateful mechanism was started.
- **UDP Timeout:** Maximum duration of a UDP connection.
- **ICMP Timeout:** Maximum duration of an ICMP connection.
- **Allow Null IP:** Allow or block packets with no source or destination IP address.
- **Block IPv6 on Agents and Appliances versions 8 and earlier:** Block or Allow IPv6 packets on older version 8.0 agents and appliances.

  Deep Security Agents and Appliances versions 8.0 and older are unable to apply Firewall or DPI rules to IPv6 network traffic and so the default setting for these older versions is to block IPv6 traffic.

- **Block IPv6 on Agents and Appliances versions 9 and later:** Block or Allow IPv6 packets on agents and appliances that are version 9 or later.
- **Connection Cleanup Timeout:** Time between cleanup of closed connections (see next).
- **Maximum Connections per Cleanup:** Maximum number of closed connections to cleanup per periodic connection cleanup (see previous).
- **Block Same Src-Dest IP Address:** Block or allow packets with same source and destination IP address. (Doesn't apply to loopback interface.)
- **Maximum TCP Connections:** Maximum simultaneous TCP Connections.

- **Maximum UDP Connections:** Maximum simultaneous UDP Connections.
- **Maximum ICMP Connections:** Maximum simultaneous ICMP Connections.
- **Maximum Events per Second:** Maximum number of events that can be written per second.
- **TCP MSS Limit:** TCP MSS is a parameter in the TCP header that defines the maximum segment size of TCP segments, in bytes. The TCP MSS Limit setting defines the minimum value allowed for TCP MSS parameter. Having a lower limit for this parameter is important because it prevents kernel panic and denial of service (DoS) attacks that may occur when a remote attacker sets up a TCP connection with a very small maximum segment size (MSS). See CVE-2019-11477, CVE-2019-11478, and CVE-2019-11479 for details on these attacks. The TCP MSS Limit default is 128 bytes, which shields against most attack sizes. A value of No Limit means that there is no lower limit and any TCP MSS value is accepted.

  > **Note:** The TCP MSS Limit option only works with the following Deep Security Agent versions:
  > Deep Security Agent 20
  > Deep Security Agent 12.0 update 1 or later
  > Deep Security Agent 11.0 update 13 or later
  > Deep Security Agent 10.0 update 20 or later

- **Number of Event Nodes:** The maximum amount of kernel memory the driver will use to store log and event information for folding at any one time.

  Event folding occurs when many events of the same type occur in succession. In such cases, the agent or appliance will fold all the events into one.

- **Ignore Status Code:** This option lets you ignore certain types of events. If, for example, you are getting a lot of "Invalid Flags" you can simply ignore all instances of that event.
- **Ignore Status Code:** Same as above.
- **Ignore Status Code:** Same as above.
- **Advanced Logging Policy:**
  - **Bypass:** No filtering of events. Overrides the Ignore Status Code settings and other advanced settings, but does not override logging settings defined in the Deep Security Manager. For example, if Firewall stateful configuration logging options set from a Firewall Stateful Configuration Properties window in the Deep Security

  Manager will not be affected.
  - **Normal:** All events are logged except dropped retransmits.
  - **Default:** Will switch to Tap Mode if the engine is in tap mode, and will switch to Normal if the engine is in inline mode.
  - **Backwards Compatibility Mode:** For support use only.
  - **Verbose Mode:** Same as Normal but including dropped retransmits.
  - **Stateful and Normalization Suppression:** Ignores dropped retransmit, out of connection, invalid flags, invalid sequence, invalid ack, unsolicited udp, unsolicited ICMP, out of allowed policy.
  - **Stateful, Normalization, and Frag Suppression:** Ignores everything that **Stateful and Normalization Suppression** ignores as well as events related to fragmentation.
  - **Stateful, Frag, and Verifier Suppression:** Ignores everything "**Stateful, Normalization, and Frag Suppression**" ignores as well as verifier-related events.
  - **Tap Mode:** Ignores dropped retransmit, out of connection, invalid flags, invalid sequence, invalid ack, max ack retransmit, packet on closed connection.

  For a more comprehensive list of which events are ignored in **Stateful and Normalization Suppression; Stateful, Normalization, and Frag Suppression; Stateful, Frag, and Verifier Suppression; and Tap** modes, see "Reduce the number of logged events" on page 1063.

- **Silent TCP Connection Drop:** When Silent TCP Connection Drop is on, a RST packet is only sent to the local stack. No RST packet is sent on the wire. This reduces the amount of information sent back to a potential attacker.

  If you enable the Silent TCP Connection Drop you must also adjust the DISCONNECT Timeout. Possible values for DISCONNECT Timeout range from 0 seconds to 10 minutes. This must be set high enough that the connection is closed by the application before it is closed by the Deep Security agent or appliance. Factors that will affect the DISCONNECT Timeout value include the operating system, the applications that are creating the connections, and network topology.

- **Enable Debug Mode:** When in debug mode, the agent/appliance captures a certain number of packets (specified by the setting below: Number of Packets to retain in Debug Mode). When a rule is triggered and debug mode is on, the agent/appliance will keep a record of the last X packets that passed before the rule was triggered. It will return those packets to the manager as debug events.

> **Note:** Debug mode can very easily cause excessive log generation and should only be used under Client Services supervision.

- **Number of Packets to retain in Debug Mode:** The number of packets to retain and log when debug mode is on.
- **Log All Packet Data:** Record the packet data for events that are not associated with specific Firewall or Intrusion Prevention rules. That is, log packet data for events such as "Dropped Retransmit" or "Invalid ACK".

  > **Note:** Events that have been aggregated because of event folding cannot have their packet data saved.

- **Log only one packet within period:** If this option is enabled and **Log All Packet Data** is not, most logs will contain only the header data. A full packet will be attached periodically, as specified by the **Period for Log only one packet within period** setting.
- **Period for Log only one packet within period:** When **Log only one packet within period** is enabled, this setting specifies how often the log will contain full packet data.
- **Maximum data size to store when packet data is captured:** The maximum size of header or packet data to be attached to a log.
- **Generate Connection Events for TCP:** Generates a Firewall event every time a TCP connection is established.
- **Generate Connection Events for ICMP:** Generates a Firewall event every time an ICMP connection is established.
- **Generate Connection Events for UDP:** Generates a Firewall event every time a UDP connection is established.
- **Bypass CISCO WAAS Connections:** This mode bypasses stateful analysis of TCP sequence numbers for connections initiated with the proprietary CISCO WAAS TCP option selected. This protocol carries extra information in invalid TCP Sequence and ACK numbers that interfere with stateful Firewall checks. Only enable this option if you are using CISCO WAAS and you are seeing connections with Invalid SEQ or Invalid ACK in the Firewall logs. When this option is selected, TCP stateful sequence number checks are still performed for non WAAS enabled connections.

- **Drop Evasive Retransmit:** Incoming packets containing data that has already been processed will be dropped to avoid possible evasive retransmit attack techniques.
- **Verify TCP Checksum:** The segment's checksum field data will be used to assess the integrity of the segment.
- **Minimum Fragment Offset:** Defines the minimum acceptable IP fragment offset. Packets with offsets less than this will be dropped with reason "IP fragment offset too small". If set to 0 no limit is enforced. (default 60)
- **Minimum Fragment Size:** Defines the minimum acceptable IP fragment size. Fragmented packets that are smaller than this will be dropped with reason "First fragment too small" as potentially malicious. (default 120)
- **SSL Session Size:** Sets the maximum number of SSL session entries maintained for SSL session keys.
- **SSL Session Time:** Sets how long SSL session renewal keys are valid before they expire.
- **Filter IPv4 Tunnels:** Not used by this version of Deep Security.
- **Filter IPv6 Tunnels:** Not used by this version of Deep Security.
- **Strict Teredo Port Check:** Not used by this version of Deep Security.
- **Drop Teredo Anomalies:** Not used by this version of Deep Security.
- **Maximum Tunnel Depth:** Not used by this version of Deep Security.
- **Action if Maximum Tunnel Depth Exceeded:** Not used by this version of Deep Security.
- **Drop IPv6 Extension Type 0:** Not used by this version of Deep Security.
- **Drop IPv6 Fragments Lower Than minimum MTU:** Drop IPv6 fragments that do not meet the minimum MTU size specified by IETF RFC 2460.
- **Drop IPv6 Reserved Addresses**: Drop these reserved addresses:
  - IETF reserved 0000::/8
  - IETF reserved 0100::/8
  - IETF reserved 0200::/7
  - IETF reserved 0400::/6
  - IETF reserved 0800::/5
  - IETF reserved 1000::/4
  - IETF reserved 4000::/2

  - IETF reserved 8000::/2
  - IETF reserved C000::/3
  - IETF reserved E000::/4
  - IETF reserved F000::/5
  - IETF reserved F800::/6

  Note that the following are allowed IPv6 addresses:

  - 64:ff9b::/96 - The well known prefix used in an algorithmic mapping between IPv4 and IPv6 addresses, as per RFC 6052.
  - 64:ff9b:1::/48 - Prefix reserved for Local-Use IPv4/IPv6 Translation, as per RFC 8215.

  For more information, see Internet Protocol Version 6 Address Space.

- **Drop IPv6 Site Local Addresses:** Drop site local addresses FEC0::/10.
- **Drop IPv6 Bogon Addresses:** Drop these addresses:
  - "loopback"::1
  - "IPv4 compatible address", ::/96
  - "IPv4 mapped address" ::FFFF:0.0.0.0/96
  - "IPv4 mapped address", ::/8
  - "OSI NSAP prefix (deprecated by RFC4048)" 0200::/7
  - "6bone (deprecated)", 3ffe::/16
  - "Documentation prefix", 2001:db8::/32
- **Drop 6to4 Bogon Addresses:** Drop these addresses:
  - "6to4 IPv4 multicast", 2002:e000:: /20
  - "6to4 IPv4 loopback", 2002:7f00:: /24
  - "6to4 IPv4 default", 2002:0000:: /24
  - "6to4 IPv4 invalid", 2002:ff00:: /24
  - "6to4 IPv4 10.0.0.0/8", 2002:0a00:: /24
  - "6to4 IPv4 172.16.0.0/12", 2002:ac10:: /28
  - "6to4 IPv4 192.168.0.0/16", 2002:c0a8:: /32
- **Drop IP Packet with Zero Payload:** Drop IP packets that have a zero-length payload.

- **Drop Unknown SSL Protocol:** Drop connection if a client attempts to connect to the Deep Security Manager with the wrong protocol. By default, any protocol other than http/1.1 will cause an error.
- **Force Allow DHCP DNS:** Controls whether the following hidden Firewall rules are enabled:

| Rule type | Priority | Direction | Protocol | Source port | Destination port |
|---|---|---|---|---|---|
| Force Allow | 4 | Outgoing | DNS | Any | 53 |
| Force Allow | 4 | Outgoing | DHCP | 68 | 67 |
| Force Allow | 4 | Incoming | DHCP | 67 | 68 |

  When the rules are enabled, agent computers can connect with the manager using the listed protocols and ports. The following values for this property are available:
  - Inherited: Inherits the setting from the policy
  - Turn off rules: Disables the rules. Note that this setting can cause agent computers to appear offline
  - Allow DNS Query: Enable only the DNS-related rule
  - Allow DNS Query and DHCP Client: Enable all 3 rules

- **Force Allow ICMP type3 code4:** Controls whether the following hidden Firewall rules are enabled:

| Rule type | Priority | Direction | Protocol | Type | Code |
|---|---|---|---|---|---|
| Force Allow | 4 | Incoming | ICMP | 3 | 4 |

  When enabled, these rules allow relay computers to connect with the manager so that the relay's heartbeat is transmitted. The following values are available:
  - Inherited: Inherits the setting from the policy.
  - Turn off rules: Disables the rule. This value can cause connection timeouts or "Destination cannot be reached" responses.
  - Add Force Allow rule for ICMP type3 code4: Enables the rule.

- **Fragment Timeout:** If configured to do so, the Intrusion Prevention rules will inspect the content of a packet (or packet fragment) if that content is considered suspicious. This setting determines how long after inspecting to wait for the remaining packet fragments before discarding the packet.
- **Maximum number of fragmented IP packets to keep:** Specifies the maximum number of fragmented packets that Deep Security will keep.
- **Send ICMP to indicate fragmented packet timeout exceeded:** When this setting is enabled and the fragment timeout is exceeded, an ICMP packet is sent to the remote computer.
- **Bypass MAC addresses that don't belong to host:** Bypass incoming packets whose destination MAC address does not belong to the host. Enabling this option reduces the number of network events caused by fetching packets that are created due to NIC teaming or a NIC in promiscuous mode on agents and appliances that are version 10.2 or later.

# User mode solution

User mode provides event generation and basic functions for Anti-Malware without any driver requirements. This solution allows some protection for systems that lack the driver support required to run in kernel mode, and provides the auto option to automatically enable the best protection available at any given time.

For details on basic functions, see Anti-Malware Engine has only Basic Functions.

## Available modes

The following modes are available:

- Kernel mode generates events and provides full Anti-Malware functionality, but can only be enabled on systems with the required driver support.
- User mode generates events and enables basic functions for Anti-Malware without any driver requirements. This mode can be enabled to run on a system without using drivers, even if the system supports the drivers required to run in kernel mode.
- Auto mode switches between kernel mode and user mode to provide the best protection available at any given time. Kernel mode is prioritized, but Deep Security Agent switches to user mode automatically during any driver support gaps that prevent kernel mode operation. If a system that lacks the required drivers to run in Kernel mode later obtains

them (from a system update, for example), then the agent automatically switches to use Kernel mode and give the system full protection from Anti-Malware.

## Use drivers for system protection

If you choose to use drivers for system protection, you can configure the driver mode as follows:

1. Go to **Computer** (or **Policy**) **> System > General > Choose whether to use Drivers for System Protection**
2. Select either **Auto**, **Kernel Mode**, or **User Mode** from the menu.
3. Click **Save**.

## Supported agents

| Operating System | Feature support in User mode |
|---|---|
| | Anti-Malware |
| AlmaLinux 9 (64-bit) | ✓ |
| Amazon Linux (64-bit) | |
| Amazon Linux 2 (64-bit) | ✓ |
| Amazon Linux 2 (AWS Arm-based Graviton 2) | |
| Amazon Linux 2 (AWS Arm-based Graviton 3) | |
| Amazon Linux 2023 (64-bit) | ✓ |
| Debian 8 (64-bit) | |
| Debian 9 (64-bit) | |
| Debian 10 (64-bit) | ✓ |
| Debian 11 (64-bit) | ✓ |
| Debian 12 (64-bit) | ✓ |
| Oracle Linux 6 (32-bit) | |

| Operating System | Feature support in User mode |
|---|---|
| | Anti-Malware |
| Oracle Linux 6 (64-bit) | |
| Oracle Linux 7 (64-bit) | |
| Oracle Linux 8 (64-bit) | ✓ |
| Oracle Linux 9 (64-bit) | ✓ |
| Red Hat Enterprise Linux 6 (32-bit) | |
| Red Hat Enterprise Linux 6 (64-bit) | |
| Red Hat Enterprise Linux 7 (64-bit) | |
| Red Hat Enterprise Linux 8 (64-bit) | |
| Red Hat Enterprise Linux 8 (AWS ARM-Based Graviton 2) | |
| Red Hat Enterprise Linux 8.6 (PowerPC little-endian) | |
| Red Hat Enterprise Linux 9 (64-bit) | ✓ |
| Red Hat Enterprise Linux Workstation 7 (64-bit) | |
| SUSE Linux Enterprise Server 12 (64-bit) | |
| SUSE Linux Enterprise Server 12 (PowerPC little-endian) | |
| SUSE Linux Enterprise Server 15 (64-bit) | ✓ |
| SUSE Linux Enterprise Server 15 (PowerPC little-endian) | |
| Ubuntu 16.04 (64-bit) | |
| Ubuntu 18.04 (64-bit) | |
| Ubuntu 18.04 (AWS ARM-Based Graviton 2) | |
| Ubuntu 20.04 (64-bit) | ✓ |

| Operating System | Feature support in User mode |
|---|---|
| | Anti-Malware |
| Ubuntu 20.04 (AWS ARM-Based Graviton 2) | |
| Ubuntu 22.04 (64-bit) | ✓ |
| Ubuntu 22.04 (AWS ARM-Based Graviton 2) | |

# Define rules, lists, and other common objects used by policies

## About common objects

The Common Objects pages (located under **Policies > Common Objects** in Deep Security Manager) provide a way to define objects once so that you can reuse them various policies and rules. When you use one of the common objects in the policy or computer editor, its settings can be overridden for that specific policy or computer. For more information on how common object properties can be inherited and overridden at the policy or computer level, see "Policies, inheritance, and overrides" on page 634.

### Rules

Some protection modules make use of rules:

- "Create a firewall rule" on page 864
- Configure an intrusion prevention rule for use in policies
- "Create an Integrity Monitoring rule" on page 909
- "Define a Log Inspection rule for use in policies" on page 964

### Lists

- "Create a list of directories for use in policies" on page 718
- "Create a list of file extensions for use in policies" on page 721
- "Create a list of files for use in policies" on page 722
- "Create a list of IP addresses for use in policies" on page 725

- "Create a list of MAC addresses for use in policies" on page 727
- "Create a list of ports for use in policies" on page 726

### Other

- "Define contexts for use in policies" on page 728
- "Define stateful firewall configurations" on page 889
- "Configure malware scans and exclusions" on page 745
- "Define a schedule that you can apply to rules" on page 734

## Create a firewall rule

Firewall rules examine the control information in individual packets, and either block or allow them according to the criteria that you define. Firewall rules can be assigned to a policy or directly to a computer.

> **Note:** This article specifically covers how to create a firewall rule. For information on how to configure the firewall module, see "Set up the Deep Security firewall" on page 851.

To create a new firewall rule, you need to:

1. "Add a new rule" below.
2. "Select the behavior and protocol of the rule" on the next page.
3. "Select a Packet Source and Packet Destination" on page 676.

When you're done with your firewall rule, you can also learn how to:

- "Configure rule events and alerts" on page 677
- "Set a schedule for the rule" on page 678
- "See policies and computers a rule is assigned to" on page 678
- "Assign a context to the rule " on page 678

### Add a new rule

There are three ways to add a new firewall rule on the **Policies** > **Common Objects** > **Rules** > **Firewall Rules** page. You can:

- Create a new rule. Click **New** > **New Firewall Rule**.
- Import a rule from an XML file. Click **New** > **Import From File**.
- Copy and then modify an existing rule. Right-click the rule in the Firewall Rules list and then click **Duplicate**. To edit the new rule, select it and then click **Properties**.

## Select the behavior and protocol of the rule

1. Enter a **Name** and **Description** for the rule.

   Tip: It is good practice to document all firewall rule changes in the Description field of the firewall rule. Make a note of when and why rules were created or deleted for easier firewall maintenance.

2. Select the **Action** that the rule should perform on packets. You can select from one of the following five actions:

   Note: Only one rule action is applied to a packet, and rules (of the same priority) are applied in the order of precedence listed below.

   - The rule can allow traffic to **bypass** the firewall. A bypass rule allows traffic to pass through the firewall and intrusion prevention engine at the fastest possible rate. Bypass rules are meant for traffic using media intensive protocols where filtering may not be desired or for traffic originating from trusted sources.

     Tip: For an example of how to create and use a bypass rule for trusted sources in a policy, see "Allow trusted traffic to bypass the firewall" on page 870.

     Note: Bypass rules are unidirectional. Explicit rules are required for each direction of traffic.

     Tip: You can achieve maximum throughput performance on a bypass rule with the following settings:
     - **Priority:** Highest
     - **Frame Type:** IP
     - **Protocol:** TCP, UDP, or other IP protocol. (Do not use the "Any" option.)
     - **Source and Destination IP and MAC:** all "Any"

  - If the protocol is TCP or UDP and the traffic direction is "incoming", the destination ports must be one or more specified ports (not "Any"), and the source ports must be "Any".
  - If the protocol is TCP or UDP and the traffic direction is "outgoing", the source ports must be one or more specified ports (Not "Any"), and the destination ports must be "Any".
  - **Schedule:** None.

- The rule can **log only**. This action will make entries in the logs but will not process traffic.
- The rule can **force allow** defined traffic (it will allow traffic defined by this rule without excluding any other traffic.)
- The rule can **deny** traffic (it will deny traffic defined by this rule.)
- The rule can **allow** traffic (it will exclusively allow traffic defined by this rule.)

**Note:** If you have no allow rules in effect on a computer, all traffic is permitted unless it is specifically blocked by a deny rule. Once you create a single allow rule, all other traffic is blocked unless it meets the requirements of the allow rule. There is one exception to this: ICMPv6 traffic is always permitted unless it is specifically blocked by a deny rule.

3. Select the **Priority** of the rule. The priority determines the order in which rules are applied. If you have selected "force allow", "deny", or "bypass" as your rule action, you can set a priority of 0 (low) to 4 (highest). Setting a priority allows you to combine the actions of rules to achieve a cascading rule effect.

**Note:** **Log only** rules can only have a priority of **4**, and **Allow** rules can only have a priority of **0**.

**Note:** High priority rules get applied before low priority rules. For example, a port 80 incoming deny rule with a priority of 3 will drop a packet before a port 80 incoming force allow rule with a priority of 2 gets applied to it.

For detailed information on how actions and priority work together, see "Firewall rule actions and priorities" on page 871.

4. Select a **Packet Direction**. Select whether this rule will be applied to **incoming** (from the network to the computer) or **outgoing**(from the computer to the network) traffic.

   > Note: An individual firewall rule only apply to a single direction of traffic. You may need to create incoming and outgoing firewall rules in pairs for specific types of traffic.

5. Select an Ethernet **Frame Type**. The term "frame" refers to Ethernet frames, and the available protocols specify the data that the frame carries. If you select "Other" as the frame type, you need to specify a frame number.

6. > Note: **IP** covers both IPv4 and IPv6. You can also select **IPv4** or **IPv6** individually

   > Note: On Solaris, Deep Security Agents will only examine packets with an IP frame type, and Linux Agents will only examine packets with IP or ARP frame types. Packets with other frame types will be allowed through. Note that the Virtual Appliance does not have these restrictions and can examine all frame types, regardless of the operating system of the virtual machine it is protecting.

   If you select the Internet Protocol (IP) frame type, you need to select the transport **Protocol**. If you select "Other" as the protocol, you also need to enter a protocol number.

## Select a Packet Source and Packet Destination

Select a combination of **IP** and **MAC** addresses, and if available for the frame type, **Port** and **Specific Flags** for the Packet Source and Packet Destination.

> Tip: You can use a previously created IP, MAC or port list.

Support for IP-based frame types is as follows:

| | IP | MAC | Port | Flags |
|---|---|---|---|---|
| Any | ✓ | ✓ | | |
| ICMP | ✓ | ✓ | | ✓ |
| ICMPV6 | ✓ | ✓ | | ✓ |
| IGMP | ✓ | ✓ | | |

| | IP | MAC | Port | Flags |
|---|---|---|---|---|
| GGP | ✓ | ✓ | | |
| TCP | ✓ | ✓ | ✓ | ✓ |
| PUP | ✓ | ✓ | | |
| UDP | ✓ | ✓ | ✓ | |
| IDP | ✓ | ✓ | | |
| ND | ✓ | ✓ | | |
| RAW | ✓ | ✓ | | |
| TCP+UDP | ✓ | ✓ | ✓ | ✓ |

**Note:** ARP and REVARP frame types only support using MAC addresses as packet sources and destinations.

You can select **Any Flags** or individually select the following flags:

- **URG**
- **ACK**
- **PSH**
- **RST**
- **SYN**
- **FIN**

## Configure rule events and alerts

When a firewall rule is triggered, it logs an event in the Deep Security Manager and records the packet data.

**Note:** Note that rules using the "Allow", "Force Allow" and "Bypass" actions will not log any events.

#### Alerts

You can configure rules to also trigger an alert if they log an event. To do so, open the properties for a rule, click on **Options**, and then select **Alert when this rule logs an event**.

> Note: Only firewall rules with an action set to "Deny" or "Log Only" can be configured to trigger an alert.

### Set a schedule for the rule

Select whether the firewall rule should only be active during a scheduled time.

For more information on how to do so, see "Define a schedule that you can apply to rules" on page 734.

### Assign a context to the rule

Rule contexts allow you to set firewall rules uniquely for different network environments. Contexts are commonly used to allow for different rules to be in effect for laptops when they are on and off-site.

For more information on how to create a context, see "Define contexts for use in policies" on page 728.

> Tip: For an example of a policy that implements firewall rules using contexts, look at the properties of the "Windows Mobile Laptop" Policy.

### See policies and computers a rule is assigned to

You can see which policies and computers are assigned to a firewall rule on the **Assigned To** tab. Click on a policy or computer in the list to see their properties.

### Export a rule

You can export all firewall rules to a .csv or .xml file by clicking **Export** and selecting the corresponding export action from the list. You can also export specific rules by first selecting them, clicking **Export** and then selecting the corresponding export action from the list.

### Delete a rule

To delete a rule, right-click the rule in the Firewall Rules list, click **Delete** and then click **OK**.

**Note:** Firewall Rules that are assigned to one or more computers or that are part of a policy cannot be deleted.

## Configure intrusion prevention rules

Perform the following tasks to configure and work with intrusion prevention rules:

- "See the list of intrusion prevention rules" below
- "See information about an intrusion prevention rule" on the next page
- "See information about the associated vulnerability (Trend Micro rules only)" on page 682
- "Assign and unassign rules" on page 682
- "Automatically assign updated required rules" on page 683
- "Configure event logging for rules" on page 683
- "Generate alerts" on page 684
- "Setting configuration options (Trend Micro rules only)" on page 684
- "Schedule active times" on page 685
- "Exclude from recommendations" on page 685
- "Set the context for a rule" on page 686
- "Override the behavior mode for a rule" on page 686
- "Override rule and application type configurations" on page 687
- "Export and import rules" on page 687
- "Configure an SQL injection prevention rule" on page 820

For an overview of the intrusion prevention module, see "About Intrusion Prevention" on page 800.

### See the list of intrusion prevention rules

The Policies page provides a list of intrusion prevention rules. You can search for intrusion prevention rules, and open and edit rule properties. In the list, rules are grouped by application type, and some rule properties appear in different columns.

**Tip:** The "TippingPoint" column contains the equivalent Trend Micro TippingPoint rule ID. In the Advanced Search for intrusion prevention, you can search on the TippingPoint rule ID. You can also see the TippingPoint rule ID in the list of assigned intrusion prevention rules in the policy and computer editor.

To see the list, click **Policies**, and then below **Common Objects/Rules** click **Intrusion Prevention Rules**.

## See information about an intrusion prevention rule

The properties of intrusion prevention rules include information about the rule and the exploit against which it protects.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.

### General Information

- **Name:** The name of the intrusion prevention rule.
- **Description:** The description of the intrusion prevention rule.
- **Minimum Agent/Appliance Version:** The minimum version of the Deep Security **Agent or Appliance**[1] required to support this intrusion prevention rule.

### Details

Clicking **New** ( ) or **Properties** ( ) displays the **Intrusion Prevention Rule Properties** window.

**Note:** Note the **Configuration** tab. Intrusion Prevention Rules from Trend Micro are not directly editable through Deep Security Manager. Instead, if the Intrusion Prevention Rule requires (or allows) configuration, those configuration options will be available on the **Configuration** tab. Custom Intrusion Prevention Rules that you write yourself will be editable, in which case the **Rules** tab will be visible.

[1] The Deep Securty Agent and Deep Security Virtual Appliance are the components that enforce the Deep Security policies that you have defined. Agents are deployed directly on a computer. Appliances are used in VMware vSphere environments to provide agentless protection. They are not available with Deep Security as a Service.

## See the list of intrusion prevention rules

The Policies page provides a list of intrusion prevention rules. You can search for intrusion prevention rules, and open and edit rule properties. In the list, rules are grouped by application type, and some rule properties appear in different columns.

> Tip: The "TippingPoint" column contains the equivalent Trend Micro TippingPoint rule ID. In the Advanced Search for intrusion prevention, you can search on the TippingPoint rule ID. You can also see the TippingPoint rule ID in the list of assigned intrusion prevention rules in the policy and computer editor.

To see the list, click **Policies**, and then below **Common Objects/Rules** click **Intrusion Prevention Rules**.

## General Information

- **Application Type:** The application type under which this intrusion prevention rule is grouped.

  > Tip: You can edit application types from this panel. When you edit an application type from here, the changes are applied to all security elements that use it.

- **Priority:** The priority level of the rule. Higher priority rules are applied before lower priority rules.
- **Severity:** Setting the severity of a rule has no effect on how the rule is implemented or applied. Severity levels can be useful as sorting criteria when viewing a list of intrusion prevention rules. More importantly, each severity level is associated with a severity value; this value is multiplied by a computer's Asset Value to determine the Ranking of an Event. (See **Administration > System Settings > Ranking**.)
- **CVSS Score:** A measure of the severity of the vulnerability according the National Vulnerability Database.

### Identification (Trend Micro rules only)

- **Type:** Can be either Smart (one or more known and unknown (zero day) vulnerabilities), Exploit (a specific exploit, usually signature based), or Vulnerability (a specific vulnerability for which one or more exploits may exist).
- **Issued:** The date the rule was released. This does not indicate when the rule was downloaded.

- **Last Updated:** The last time the rule was modified either locally or during Security Update download.
- **Identifier:** The rule's unique identification tag.

## See information about the associated vulnerability (Trend Micro rules only)

Rules that Trend Micro provides can include information about the vulnerability against which the rule protects. When applicable, the Common Vulnerability Scoring System (CVSS) is displayed. (For information on this scoring system, see the CVSS page at the National Vulnerability Database.)

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Click the **Vulnerabilities** tab.

## Assign and unassign rules

To apply intrusion prevention rules during agent scans, you assign them to the appropriate policies and computers. When the rule is no longer necessary because the vulnerability has been patched you can unassign the rule.

If you cannot unassign intrusion prevention rules from a **Computer editor**[1], it is likely because the rules are currently assigned in a policy. Rules assigned at the policy level must be removed using the **Policy editor**[2] and cannot be removed at the computer level.

When you make a change to a policy, it affects all computers using the policy. For example, when you unassign a rule from a policy you remove the rule from all computers that are protected by that policy. To continue to apply the rule to other computers, create a new policy for that group of computers. (See "Policies, inheritance, and overrides" on page 634.)

Tip: To see the policies and computers to which a rule is assigned, see the Assigned To tab of the rule properties.

1. Go to the **Policies** page, right-click the policy to configure and click **Details**.
2. Click **Intrusion Prevention > General**.
   The list of rules that are assigned to the policy appear in the **Assigned Intrusion Prevention Rules** list.

[1] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2] To open the Policy editor, go to the Policies page and double-click the policy that you want to edit (or select the policy and click Details).

3. Under **Assigned Intrusion Prevention Rules**, click **Assign/Unassign**.
4. To assign a rule, select the check box next to the rule.
5. To unassign a rule, deselect the check box next to the rule.
6. Click **OK**.

## Automatically assign updated required rules

Security updates can include new or updated application types and intrusion prevention rules which require the assignment of secondary intrusion prevention rules. Deep Security can automatically assign these rules if they are required. You enable these automatic assignments in the the policy or computer properties.

1. Go to the **Policies** page, right-click the policy to configure and click **Details**.
2. Click **Intrusion Prevention > Advanced**.
3. To enable the automatic assignments, in the **Rule Updates** area, select **Yes**.
4. Click **OK**.

## Configure event logging for rules

Configure whether events are logged for a rule, and whether to include packet data in the log.

> **Note:** Deep Security can display X-Forwarded-For headers in intrusion prevention events when they are available in the packet data. This information can be useful when the Deep Security Agent is behind a load balancer or proxy. The X-Forwarded-For header data appears in the event's Properties window. To include the header data, include packet data in the log. In addition, rule 1006540 " Enable X-Forwarded-For HTTP Header Logging" must be assigned.

Because it would be impractical to record all packet data every time a rule triggers an event, Deep Security records the data only the first time the event occurs within a specified period of time. The default time is five minutes, however you can change the time period using the "Period for Log only one packet within period" property of a policy's Advanced Network Engine settings. (See Advanced Network Engine Options.)

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" on page 687.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.

3. On the General tab, go to the Events area and select the desired options:
   - To disable logging for the rule, select **Disable Event Logging**.
   - To log an event when a packet is dropped or blocked, select **Generate Event on Packet Drop**.
   - To include the packet data in the log entry, select **Always Include Packet Data**.
   - To log several packets that precede and follow the packet that the rule detected, select **Enable Debug Mode**.Use debug mode only when your support provider instructs you to do so.

Additionally, to include packet data in the log, the policy to which the rule is assigned must allow rules to capture packet data:

1. On the Policies page, open the policy that is assigned the rule.
2. Click **Intrusion Prevention > Advanced**.
3. In the **Event Data** area, select **Yes**.

## Generate alerts

Generate an alert when an intrusion prevention rule triggers an event.

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" on page 687.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Click the Options tab, and in the **Alert** area select **On**.
4. Click **OK**.

## Setting configuration options (Trend Micro rules only)

Some intrusion prevention rules that Trend Micro provides have one or more configuration options such as header length, allowed extensions for HTTP, or cookie length. Some options require you to configure them. If you assign a rule without setting a required option, an alert is generated that informs you about the required option. (This also applies to any rules that are downloaded and automatically applied by way of a Security Update.)

Intrusion prevention rules that have configuration options appear in the Intrusion Prevention Rules list with a small gear over their icon ⚙.

**Note:** Custom intrusion prevention rules that you write yourself include a **Rules** tab where you can edit the rules.

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" on page 687.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Click the **Configuration** tab.
4. Configure the properties and then click **OK**.

## Schedule active times

Schedule a time during which an intrusion prevention rule is active. Intrusion prevention rules that are active only at scheduled times appear in the Intrusion Prevention Rules page with a small clock over their icon .

**Note:** With Agent-based protection, schedules use the same time zone as the endpoint operating system. With Agentless protection, schedules use the same time zone as the Deep Security Virtual Appliance.

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" on page 687.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Click the **Options** tab.
4. In the **Schedule** area, select **New** or select a frequency.
5. Edit the schedule as required.
6. Click **OK**.

## Exclude from recommendations

Exclude intrusion prevention rules from rule recommendations of recommendation scans.

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" on page 687.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Click the **Options**tab.
4. In the **Recommendations Options** area, select **Exclude from Recommendations**.
5. Click **OK**.

## Set the context for a rule

Set the context in which the rule is applied.

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" on the next page.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Click the **Options** tab.
4. In the **Context** area, select **New** or select a context.
5. Edit the context as required.
6. Click **OK**.

## Override the behavior mode for a rule

Set the behavior mode of an intrusion prevention rule to Detect when testing new rules. In Detect mode, the rule creates a log entry prefaced with the words "detect only:" and does not interfere with traffic. Some intrusion prevention rules are designed to operate only in Detect mode. For these rules, you cannot change the behavior mode.

**Note:** If you disable logging for the rule, the rule activity is not logged regardless of the behavior mode.

For more information about behavior modes, see "Use behavior modes to test rules" on page 802.

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" on the next page.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Select **Detect Only**.

## Override rule and application type configurations

From a Computer or Policy editor[1] , you can edit an intrusion prevention rule so that your changes apply only in the context of the policy or computer. You can also edit the rule so that the changes apply globally so that the changes affect other policies and computers that are assigned the rule. Similarly, you can configure application types for a single policy or computer, or globally.

1. Go to the **Policies** page, right-click the policy to configure and click **Details**.
2. Click **Intrusion Prevention**.
3. To edit a rule, right-click the rule and select one of the following commands:
   - **Properties**: Edit the rule only for the policy.
   - **Properties (Global)**: Edit the rule globally, for all policies and computers.
4. To edit the application type of a rule, right-click the rule and select one of the following commands:
   - **Application Type Properties**: Edit the application type only for the policy.
   - **Application Type Properties (Global)**: Edit the application type globally, for all policies and computers.
5. Click **OK**.

Tip: When you select the rule and click Properties, you are editing the rule only for the policy that you are editing.

Note: You cannot assign one port to more than eight application types. If they are, the rules will not function on that port.

## Export and import rules

You can export one or more intrusion prevention rules to an XML or CSV file, and import rules from an XML file.

1. Click **Policies > Intrusion Prevention Rules**.
2. To export one or more rules, select them and click **Export > Export Selected to CSV** or **Export > Export Selected to XML**.
3. To export all rules, click **Export > Export to CSV** or **Export > Export to XML**.
4. To import rules, click **New > Import From File** and follow the instructions on the wizard.

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

# Create an Integrity Monitoring rule

Integrity Monitoring rules describe how Deep Security Agents should scan for and detect changes to a computer's files, directories, and registry keys and values, as well as changes in installed software, processes, listening ports, and running services. Integrity Monitoring rules can be assigned directly to computers or can be made part of a policy.

**Note:** This article specifically covers how to create an Integrity Monitoring rule. For information on how to configure the Integrity Monitoring module, see "Set up Integrity Monitoring" on page 901.

There are two types of Integrity Monitoring rules: those that you have created, and those that are issued by Trend Micro. For more information on how to configure rules issued by Trend Micro, see the "Configure Trend Micro Integrity Monitoring rules" on page 690 section.

To create a new Integrity Monitoring rule, you need to:

1. "Add a new rule" below.
2. "Enter Integrity Monitoring rule information " on the next page.
3. "Select a rule template and define rule attributes" on the next page.

When you're done with your rule, you can also learn how to

- "Configure rule events and alerts" on page 691
- "See policies and computers a rule is assigned to" on page 692
- "Export a rule" on page 692
- "Delete a rule" on page 692

## Add a new rule

There are three ways to add an Integrity Monitoring rule on the **Policies** > **Common Objects** > **Rules** > **Integrity Monitoring Rules** page. You can:

- Create a new rule. Click **New** > **New Integrity Monitoring Rule**.
- Import a rule from an XML file. Click **New** > **Import From File**.
- Copy and then modify an existing rule. Right-click the rule in the Integrity Monitoring Rules list and then click **Duplicate**. To edit the new rule, select it and then click **Properties**.

## Enter Integrity Monitoring rule information

1. Enter a **Name** and **Description** for the rule.

   > **Tip:** It is good practice to document all Integrity Monitoring rule changes in the Description field of the rule. Make a note of when and why rules were created or deleted for easier maintenance.

2. Set the **Severity** of the rule.

   > **Note:** Setting the severity of a rule has no effect on how the rule is implemented or applied. Severity levels can be useful as sorting criteria when viewing a list of Integrity Monitoring rules. More importantly, each severity level is associated with a severity value; this value is multiplied by a computer's Asset Value to determine the ranking of an event. (See **Administration > System Settings > Ranking**.)

## Select a rule template and define rule attributes

Go to the **Content** tab and select from one of the following three templates:

### Registry Value template

Create an Integrity Monitoring rule to specifically monitor changes to registry values.

> **Note:** The Registry Value template is only for Windows-based computers .

1. Select the **Base Key** to monitor and whether or not to monitor contents of sub keys.
2. List **Value Names** to be included or excluded. You can use "?" and "*" as wildcard characters.
3. Enter **Attributes** to monitor. Entering "STANDARD" will monitor changes in registry size, content and type. For more information on Registry Value template attributes see the "RegistryValueSet" on page 945 documentation.

### File template

Create an Integrity Monitoring rule to specifically monitor changes to files.

1. Enter a **Base Directory** for the rule (for example, `C:\Program Files\MySQL` .) Select **Include Sub Directories** to include the contents of all subdirectories relative to the base directory. Wildcards are not supported for base directories.

2. Use the **File Names** fields to include or exclude specific files. You can use wildcards (" `?` " for a single character and " `*` " for zero or more characters.

   > **Note:** Leaving the **File Names** fields blank will cause the rule to monitor all files in the base directory. This can use significant system resources if the base directory contains numerous or large files.

3. Enter **Attributes** to monitor. Entering "STANDARD" will monitor changes in file creation date, last modified date, permissions, owner, group, size, content, flags (Windows), and SymLinkPath (Linux). For more information on File template attributes see the "FileSet" on page 929 documentation.

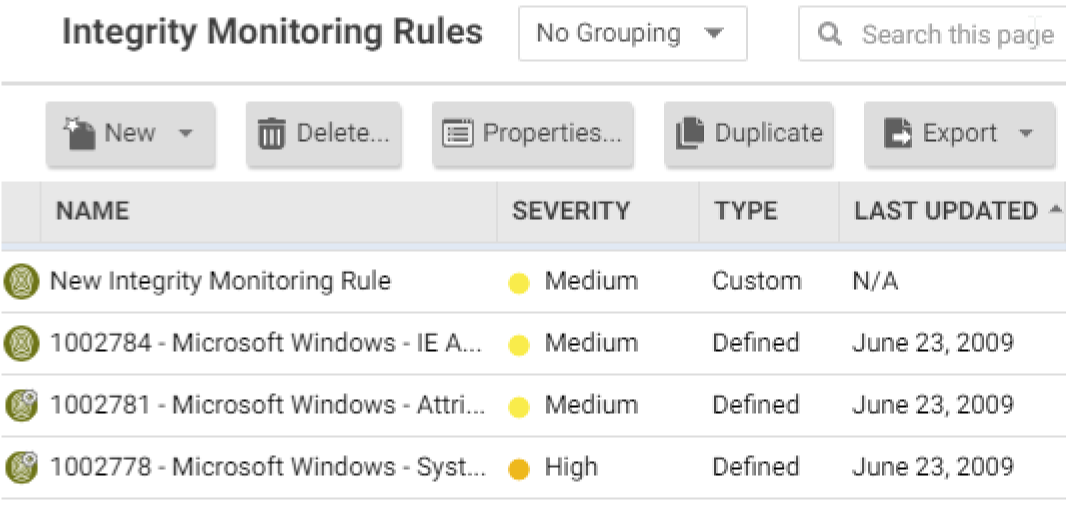
### Custom (XML) template

Create a custom Integrity Monitoring rule template to monitor directories, registry values, registry keys, services, processes, installed software, ports, groups, users, files, and the WQL using the Deep Security XML-based "About the Integrity Monitoring rules language" on page 913.

> **Tip:** You can create your rule in your preferred text editor and paste it to the **Content** field when you are done.

## Configure Trend Micro Integrity Monitoring rules

Integrity Monitoring rules issued by Trend Micro cannot be edited in the same way as the custom rules you create. Some Trend Micro rules cannot be modified at all, while other rules may offer limited configuration options. Both of these rule types will show as "Defined" under the "Type" column, but rules that can be configured will display a gear in the Integrity Monitoring icon (⚙).



| NAME | SEVERITY | TYPE | LAST UPDATED |
|---|---|---|---|
| New Integrity Monitoring Rule | ● Medium | Custom | N/A |
| 1002784 - Microsoft Windows - IE A... | ● Medium | Defined | June 23, 2009 |
| 1002781 - Microsoft Windows - Attri... | ● Medium | Defined | June 23, 2009 |
| 1002778 - Microsoft Windows - Syst... | ● High | Defined | June 23, 2009 |

You can access the configuration options for a rule by opening the properties for the rule and clicking on the **Configuration** tab.

Rules issued by Trend Micro also show the following additional information under the **General** tab:

- When the rule was first issued and last updated, as well as a unique identifier for the rule.
- The minimum versions of the Agent and the Deep Security Manager that are required for the rule to function.

Although you cannot edit rules issued by Trend Micro directly, you can duplicate them and then edit the copy.

## Configure rule events and alerts

Any changes detected by an Integrity Monitoring rule is logged as an event in the Deep Security Manager.

### Real-time event monitoring

By default, events are logged at the time they occur. If you only want events to be logged when you manually perform a scan for changes, deselect **Allow Real Time Monitoring**.

### Alerts

You can also configure the rules to trigger an alert when they log an event. To do so, open the properties for a rule, click on **Options**, and then select **Alert when this rule logs an event**.

### See policies and computers a rule is assigned to

You can see which policies and computers are assigned to an Integrity Monitoring rule on the **Assigned To** tab. Click on a policy or computer in the list to see their properties.

### Export a rule

You can export all Integrity Monitoring rules to a .csv or .xml file by clicking **Export** and selecting the corresponding export action from the list. You can also export specific rules by first selecting them, clicking **Export** and then selecting the corresponding export action from the list.

### Delete a rule

To delete a rule, right-click the rule in the Integrity Monitoring Rules list, click **Delete** and then click **OK**.

> **Note:** Integrity Monitoring rules that are assigned to one or more computers or that are part of a policy cannot be deleted.

## Define a Log Inspection rule for use in policies

The OSSEC Log Inspection engine is integrated into Deep Security Agents and gives Deep Security the ability to inspect the logs and events generated by the operating system and applications running on the computer. Deep Security Manager ships with a standard set of OSSEC Log Inspection rules that you can assign to computers or policies. You can also create custom rules if there is no existing rule that fits your requirements.

You cannot modify Log Inspection Rules issued by Trend Micro, but you can duplicate them and then modify them.

Log Inspection Rules assigned to one or more computers or are part of a Policy cannot be deleted.

To create Log Inspection rules, perform these basic steps:

- "Create a new Log Inspection rule" on the next page
- "Decoders" on page 695
- "Subrules" on page 696

- "Examples" on page 704
- "Log Inspection rule severity levels and their recommended use" on page 712
- "strftime() conversion specifiers " on page 713
- "Examine a Log Inspection rule" on page 714

For an overview of the Log Inspection module, see "About Log Inspection" on page 959.

## Create a new Log Inspection rule

1. In the Deep Security Manager, go to **Policies** > **Common Objects** > **Rules** > **Log Inspection Rules**.
2. Click **New** > **New Log Inspection Rule**.
3. On the **General** tab, enter a name and an optional description for the rule.
4. The **Content** tab is where you define the rule. The easiest way to define a rule is to select **Basic Rule** and use the options provided to define the rule. If you need further customization, you can select **Custom (XML)** to switch to an XML view of the rule that you are defining.

   Any changes you make in the **Custom (XML)** view are lost if you switch back to the Basic Rule view.

   For further assistance in writing your own Log Inspection rules using the XML-based language, consult the OSSEC documentation or contact your support provider.

   These options are available for the Basic Rule template:

   - **Rule ID:** The Rule ID is a unique identifier for the rule. OSSEC defines 100000 - 109999 as the space for user-defined rules. Deep Security Manager prepopulates the field with a new unique Rule ID.
   - **Level:** Assign a level to the rule. Zero (0) means the rule never logs an event, although other rules that watch for this rule may fire.
   - **Groups:** Assign the rule to one or more comma-separated groups. This can be useful when dependency is used because you can create rules that fire on the firing of a rule, or a rule that belongs to a specific group.
   - **Rule Description:** Description of the rule.
   - **Pattern Matching:** This is the pattern the rule will look for in the logs. The rule is triggered on a match. Pattern matching supports Regular Expressions or simpler String

Patterns. The String Pattern pattern type is faster than RegEx but it only supports three special operations:

- **^ (caret)**: specifies the beginning of text
- **$ (dollar sign)**: specifies the end of text
- **| (pipe)**: to create a "OR" between multiple patterns

For information on the regular expression syntax used by the Log Inspection module, see https://www.ossec.net/docs/syntax/regex.html.

- **Dependency:** Setting a dependency on another rule causes your rule to only log an event if the rule specified in this area has also triggered.
- **Frequency** is the number of times the rule has to match within a specific time frame before the rule is triggered.
- **Time Frame** is the period of time in seconds within which the rule has to trigger a certain number of times (the frequency, above) to log an event.

  The **Content** tab only appears for Log Inspection rules that you create yourself. Log Inspection rules issued by Trend Micro have a **Configuration** tab instead that displays the Log Inspection rule's configuration options,if there are any.

5. On the **Files** tab, type the full path to the files you want your rule to monitor and specify the type of file it is.

   The glob character is supported when used in the file name. The glob character is also supported when used in the directory portion of the path no more than twice. For example, `/home/user1/testlog*.txt`, `/home/*/testlog1.txt`, `/home/*/testlog*.txt`, `/home/*/user*/testlog*.txt` are all valid, whereas `/home/*/demo*/user*/testlog1.txt` is invalid.

6. On the **Options** tab, in the **Alert** section, select whether this rule triggers an alert in the Deep Security Manager.

   **Alert Minimum Severity** sets the minimum severity level that will trigger an Alert for rules made using the Basic Rule or Custom (XML) template.

   The Basic Rule template creates one rule at a time. To write multiple rules in a single template you can use the Custom (XML) template. If you create multiple rules with different

Levels within a Custom (XML) template, you can use the **Alert Minimum Severity** setting to select the minimum severity that will trigger an Alert for all of the rules in that template.

7. The **Assigned To** tab lists the policies and computers that are using this Log Inspection rule. Because you are creating a new rule, it has not been assigned yet.
8. Click **OK**. The rule is ready to be assigned to policies and computers.

## Decoders

A Log Inspection rule consists of a list of files to monitor for changes and a set of conditions to be met for the rule to trigger. When the Log Inspection engine detects a change in a monitored log file, the change is parsed by a decoder. Decoders parse the raw log entry into the following fields:

- **log:** the message section of the event
- **full_log:** the entire event
- **location:** where the log came from
- **hostname:** hostname of the event source
- **program_name:** program name from the syslog header of the event
- **srcip:** the source IP address within the event
- **dstip:** the destination IP address within the event
- **srcport:** the source port number within the event
- **dstport:** the destination port number within the event
- **protocol:** the protocol within the event
- **action:** the action taken within the event
- **srcuser:** the originating user within the event
- **dstuser:** the destination user within the event
- **id:** any ID decoded as the ID from the event
- **status:** the decoded status within the event
- **command:** the command being called within the event
- **url:** the URL within the event
- **data:** any additional data extracted from the event
- **systemname:** the system name within the event

Rules examine this decoded data looking for information that matches the conditions defined in the rule.

If the matches are at a sufficiently high severity level, any of the following actions can be taken:

- An alert can be raised. Configurable on the **Options** tab of the Log Inspection Rule's **Properties** window.
- The event can be written to syslog. Configurable in the **SIEM** area on **Administration > System Settings > Event Forwarding** tab.
- The event can be sent to the Deep Security Manager. Configurable in the **Log Inspection Syslog Configuration** setting on the **Policy or Computer Editor > Settings > Event Forwarding** tab.

## Subrules

A single Log Inspection rule can contain multiple subrules. These subrules can be of two types: atomic or composite. An atomic rule evaluates a single event and a composite rule examines multiple events and can evaluate frequency, repetition, and correlation between events.

### Groups

Each rule, or grouping of rules, must be defined within a `<group></group>` element. The attribute name must contain the rules you want to be a part of this group. In the following example, it indicates that the group contains the syslog and SSHD rules:

```
                        <group name="syslog,sshd,">
                        </group>
```

Notice the trailing comma in the group name. Trailing commas are required if you intend to use the `<if_group></if_group>` tag to conditionally append another subrule to this one.

When a set of Log Inspection rules are sent to an agent, the Log Inspection engine on the agent takes the XML data from each assigned rule and assembles it into what becomes a single long Log Inspection rule. Some group definitions are common to all Log Inspection rules created by Trend Micro. For this reason Trend Micro has included a rule called Default Rules Configuration, which defines these groups and which always gets assigned together with any other Trend Micro rules. If you select a rule for assignment and do not also select the Default Rules Configuration rule, a notice appears informing you that the rule will be assigned automatically. If you create your own Log Inspection rule and assign it to a Computer without assigning any Trend Micro-written rules, you must either copy the content of the Default Rules Configuration rule into your new rule or also select the Default Rules Configuration rule for assignment to the Computer.

### Rules, ID, and Level

A group can contain as many rules as you require. The rules are defined using the `<rule></rule>` element and must have at least two attributes, the `id` and the `level`. The `id` is a unique identifier for that signature and the `level` is the severity of the alert. In the following example, two rules are created, each with a different rule ID and level:

```
<group name="syslog,sshd,">
       <rule id="100120" level="5">
       </rule>
       <rule id="100121" level="6">
       </rule>
</group>
```

Custom rules must have ID values of 100,000 or greater.

You can define additional subgroups within the parent group using the `<group></group>` tag. This subgroup can reference any of the groups listed in the following table:

| Group Type | Group Name | Description |
|---|---|---|
| Reconnaissance | connection_attempt<br>web_scan<br>recon | Connection attempt<br>Web scan<br>Generic scan |
| Authentication Control | authentication_success<br>authentication_failed<br>invalid_login<br>login_denied<br>authentication_failures<br>adduser<br>account_changed | Success<br>Failure<br>Invalid<br>Login Denied<br>Multiple Failures<br>User account added<br>User Account changed or removed |
| Attack/Misuse | automatic_attack<br>exploit_attempt<br>invalid_access<br>spam<br>multiple_spam<br>sql_injection<br>attack<br>virus | Worm (nontargeted attack)<br>Exploit pattern<br>Invalid access<br>Spam<br>Multiple spam messages<br>SQL injection<br>Generic attack<br>Virus detected |
| Access Control | access_denied<br>access_allowed<br>unknown_resource<br>firewall_drop<br>multiple_drops<br>client_misconfig<br>client_error | Access denied<br>Access allowed<br>Access to nonexistent resource<br>Firewall drop<br>Multiple firewall drops<br>Client misconfiguration<br>Client error |
| Network Control | new_host | New computer detected |

| Group Type | Group Name | Description |
|---|---|---|
| | ip_spoof | Possible ARP spoofing |
| System Monitor | service_start<br>system_error<br>system_shutdown<br>logs_cleared<br>invalid_request<br>promisc<br>policy_changed<br>config_changed<br>low_diskspace<br>time_changed | Service start<br>System error<br>Shutdown<br>Logs cleared<br>Invalid request<br>Interface switched to promiscuous mode<br>Policy changed<br>Configuration changed<br>Low disk space<br>Time changed |

If event auto-tagging is enabled, the event is labeled with the group name. Log Inspection rules provided by Trend Micro make use of a translation table that changes the group to a more user-friendly version. For example, login_denied would appear as Login Denied. Custom rules are listed by their group name as it appears in the rule.

### Description

Include a `<description></description>` tag. The description text appears in the event if the rule is triggered.

```
<group name="syslog,sshd,">
       <rule id="100120" level="5">
               <group>authentication_success</group>
               <description>SSHD testing authentication success</description>
       </rule>
       <rule id="100121" level="6">
               <description>SSHD rule testing 2</description>
       </rule>
</group>
```

### Decoded As

The `<decoded_as></decoded_as>` tag instructs the Log Inspection engine to only apply the rule if the specified decoder has decoded the log.

```
<rule id="100123" level="5">
       <decoded_as>sshd</decoded_as>
       <description>Logging every decoded sshd message</description>
</rule>
```

To view the available decoders, go to the **Log Inspection Rule** page and click **Decoders.** Right-click on **1002791-Default Log Decoders** and select **Properties**. Go the **Configuration** tab and click **View Decoders**.

### Match

To look for a specific string in a log, use the `<match></match>`. Here is a Linux sshd failed password log:

```
Jan 1 12:34:56 linux_server sshd[1231]: Failed password for invalid
      user jsmith from 192.168.1.123 port 1799 ssh2
```

Use the **<match></match>** tag to search for the "password failed" string.

```
<rule id="100124" level="5">
       <decoded_as>sshd</decoded_as>
       <match>^Failed password</match>
       <description>Failed SSHD password attempt</description>
</rule>
```

Notice the regex caret ( ^ ) indicating the beginning of a string. Although "Failed password" does not appear at the beginning of the log, the Log Inspection decoder brakes the log into sections. See "Decoders" on page 695 for more information. One of those sections is "log", which is the message part of the log, as opposed to "full_log" which is the log in its entirety.

The following table lists supported regex syntax:

| Regex syntax | Description |
|---|---|
| \w | A-Z, a-z, 0-9 single letters and numerals |
| \d | 0-9 single numerals |
| \s | single space |
| \t | single tab |
| \p | ()*+,-.:;<=>?[] |
| \W | not \w |
| \D | not \d |
| \S | not \s |
| \. | anything |
| + | match one or more of any of the above (for example, \w+, \d+) |
| * | match zero or more of any of the above (for example, \w*, \d*) |
| ^ | indicates the beginning of a string (^somestring) |
| $ | specify the end of a string (somestring$) |
| \| | indicate an "OR" between multiple strings |

### Conditional statements

Rule evaluation can be conditional upon other rules having been evaluated as true. The `<if_sid></if_sid>` tag instructs the Log Inspection engine to only evaluate this subrule if the rule identified in the tag has been evaluated as true. The following example shows three rules: 100123, 100124, and 100125. Rules 100124 and 100125 have been modified to be children of the 100123 rule using the `<if_sid></if_sid>` tag:

```
<group name="syslog,sshd,">
       <rule id="100123" level="2">
               <decoded_as>sshd</decoded_as>
               <description>Logging every decoded sshd message</description>
       </rule>
       <rule id="100124" level="7">
               <if_sid>100123</if_sid>
               <match>^Failed password</match>
               <group>authentication_failure</group>
               <description>Failed SSHD password attempt</description>
       </rule>
       <rule id="100125" level="3">
               <if_sid>100123</if_sid>
               <match>^Accepted password</match>
               <group>authentication_success</group>
               <description>Successful SSHD password attempt</description>
       </rule>
</group>
```

### Hierarchy of evaluation

The `<if_sid></if_sid>` tag essentially creates a hierarchical set of rules. That is, by including an `<if_sid></if_sid>` tag in a rule, the rule becomes a child of the rule referenced by the `<if_sid></if_sid>` tag. Before applying any rules to a log, the Log Inspection engine assesses the `<if_sid></if_sid>` tags and builds a hierarchy of parent and child rules.

The hierarchical parent-child structure can be used to improve the efficiency of your rules. If a parent rule does not evaluate as true, the Log Inspection engine ignores the children of that parent.

Although the `<if_sid></if_sid>` tag can be used to refer to subrules within an entirely different Log Inspection rule, you should avoid doing this because it makes the rule very difficult to review later.

The list of available atomic rule conditional options is shown in the following table:

| Tag | Description | Notes |
|---|---|---|
| match | A pattern | Any string to match against the event (log). |
| regex | A regular expression | Any regular expression to match against the event (log). |
| decoded_as | A string | Any prematched string. |
| srcip | A source IP address | Any IP address that is decoded as the source IP address. Use ! to negate the IP address. |
| dstip | A destination IP address | Any IP address that is decoded as the destination IP address. Use ! to negate the IP address. |
| srcport | A source port number | Any source port (match format). |
| dstport | A destination port number | Any destination port (match format). |
| user | A username | Any username that is decoded as a username. |
| program_name | A program name | Any program name that is decoded from the syslog process name. |
| hostname | A system hostname | Any hostname that is decoded as a syslog hostname. |
| time | A time range in the format<br>hh:mm - hh:mm or<br>hh:mm am - hh:mm pm | The time range that the event must fall within for the rule to trigger. |
| weekday | A weekday (sunday, monday, tuesday, and so on) | Day of the week that the event must fall on for the rule to trigger. |
| id | An ID | Any ID that is decoded from the event. |
| url | A URL | Any URL that is decoded from the event. |

Use the `<if_sid>100125</if_sid>` tag to make this rule depend on the 100125 rule. This rule is checked only for SSHD messages that already matched the successful login rule.

```
<rule id="100127" level="10">
       <if_sid>100125</if_sid>
       <time>6 pm - 8:30 am</time>
       <description>Login outside business hours.</description>
       <group>policy_violation</group>
</rule>
```

### Restrictions on the Size of the Log Entry

The following example takes the previous example and adds the `maxsize` attribute which tells the Log Inspection engine to only evaluate rules that are less than the maxsize number of characters:

```
<rule id="100127" level="10" maxsize="2000">
       <if_sid>100125</if_sid>
```

```
        <time>6 pm - 8:30 am</time>
        <description>Login outside business hours.</description>
        <group>policy_violation</group>
</rule>
```

The following table lists possible atomic rule tree-based options:

| Tag | Description | Notes |
|---|---|---|
| if_sid | A rule ID | Adds this rule as a child rule of the rules that match the specified signature ID. |
| if_group | A group ID | Adds this rule as a child rule of the rules that match the specified group. |
| if_level | A rule level | Adds this rule as a child rule of the rules that match the specified severity level. |
| description | A string | A description of the rule. |
| info | A string | Extra information about the rule. |
| cve | A CVE number | Any Common Vulnerabilities and Exposures (CVE) number that you would like associated with the rule. |
| options | alert_by_ email<br>no_email_ alert<br>no_log | Additional rule options to indicate if the Alert should generate an e-mail, alert_by_email, should not generate an email, no_email_alert, or should not log anything at all, no_log. |

### Composite Rules

Atomic rules examine single log entries. To correlate multiple entries, you must use composite rules. Composite rules are supposed to match the current log with those already received. Composite rules require two additional options: the `frequency` option specifies how many times an event or pattern must occur before the rule generates an alert, and the `timeframe` option tells the Log Inspection engine how far back, in seconds, it should look for previous logs. All composite rules have the following structure:

```
<rule id="100130" level="10" frequency="x" timeframe="y">
</rule>
```

For example, you could create a composite rule that creates a higher severity alert after five failed passwords within a period of 10 minutes. Using the `<if_matched_sid></if_matched_sid>` tag you can indicate which rule needs to be seen within the desired frequency and timeframe for your new rule to create an alert. In the following example, the `frequency` attribute is set to trigger when five instances of the event are seen and the `timeframe` attribute is set to specify the time window as 600 seconds.

The `<if_matched_sid></if_matched_sid>` tag is used to define which other rule the composite rule will watch:

```
<rule id="100130" level="10" frequency="5" timeframe="600">
       <if_matched_sid>100124</if_matched_sid>
       <description>5 Failed passwords within 10 minutes</description>
</rule>
```

There are several additional tags that you can use to create more granular composite rules. These rules, as shown in the following table, allow you to specify that certain parts of the event must be the same. This allows you to tune your composite rules and reduce false positives:

| Tag | Description |
|---|---|
| same_source_ip | Specifies that the source IP address must be the same. |
| same_dest_ip | Specifies that the destination IP address must be the same. |
| same_dst_port | Specifies that the destination port must be the same. |
| same_location | Specifies that the location (hostname or agent name) must be the same. |
| same_user | Specifies that the decoded username must be the same. |
| same_id | Specifies that the decoded id must be the same. |

If you wanted your composite rule to alert on every authentication failure, instead of a specific rule ID, you could replace the `<if_matched_sid></if_matched_sid>` tag with the `<if_matched_ group></if_matched_ group>` tag. This allows you to specify a category, such as `authentication_ failure`, to search for authentication failures across your entire infrastructure.

```
<rule id="100130" level="10" frequency="5" timeframe="600">
       <if_matched_group>authentication_failure</if_matched_group>
       <same_source_ip />
       <description>5 Failed passwords within 10 minutes</description>
</rule>
```

In addition to `<if_matched_sid></if_matched_sid>` and `<if_matched_group></if_ matched_ group>` tags, you can also use the `<if_matched_regex></if_matched_regex>` tag to specify a regular expression to search through logs as they are received.

```
<rule id="100130" level="10" frequency="5" timeframe="600">
       <if_matched_regex>^Failed password</if_matched_regex>
       <same_source_ip />
       <description>5 Failed passwords within 10 minutes</description>
</rule>
```

## Examples

Deep Security includes many default Log Inspection rules for dozens of common and popular applications. Through Security Updates, new rules are added regularly. In spite of the growing list of applications supported by Log Inspection rules, you may find the need to create a custom rule for an unsupported or custom application.

The following example creates a custom CMS (content management system) hosted on Microsoft Windows Server with IIS and .Net platform, with a Microsoft SQL Server database as the data repository.

The first step is to identify the following application logging attributes:

1. Where does the application log to?
2. Which Log Inspection decoder can be used to decode the log file?
3. What is the general format of a log file message?

For the CMS example, the answers are as follows:

1. Windows Event Viewer
2. Windows Event Log (eventlog)
3. Windows Event Log Format with the following core attributes:
   - Source: CMS
   - Category: None
   - Event: <Application Event ID>

The second step is to identify the categories of log events by application feature, and then organize the categories into a hierarchy of cascading groups for inspection. Not all inspected groups need to raise events; a match can be used as a conditional statement. For each group, identify the log format attributes which the rule can use as matching criteria. This can also be performed by inspecting all application logs for patterns and logical groupings of log events.

For example, the CMS application supports the following functionality for which Log Inspection rules are created:

- CMS Application Log (Source: CMS)
  - Authentication (Event: 100 to 119)
    - User Login successful (Event: 100)
    - User Login unsuccessful (Event: 101)

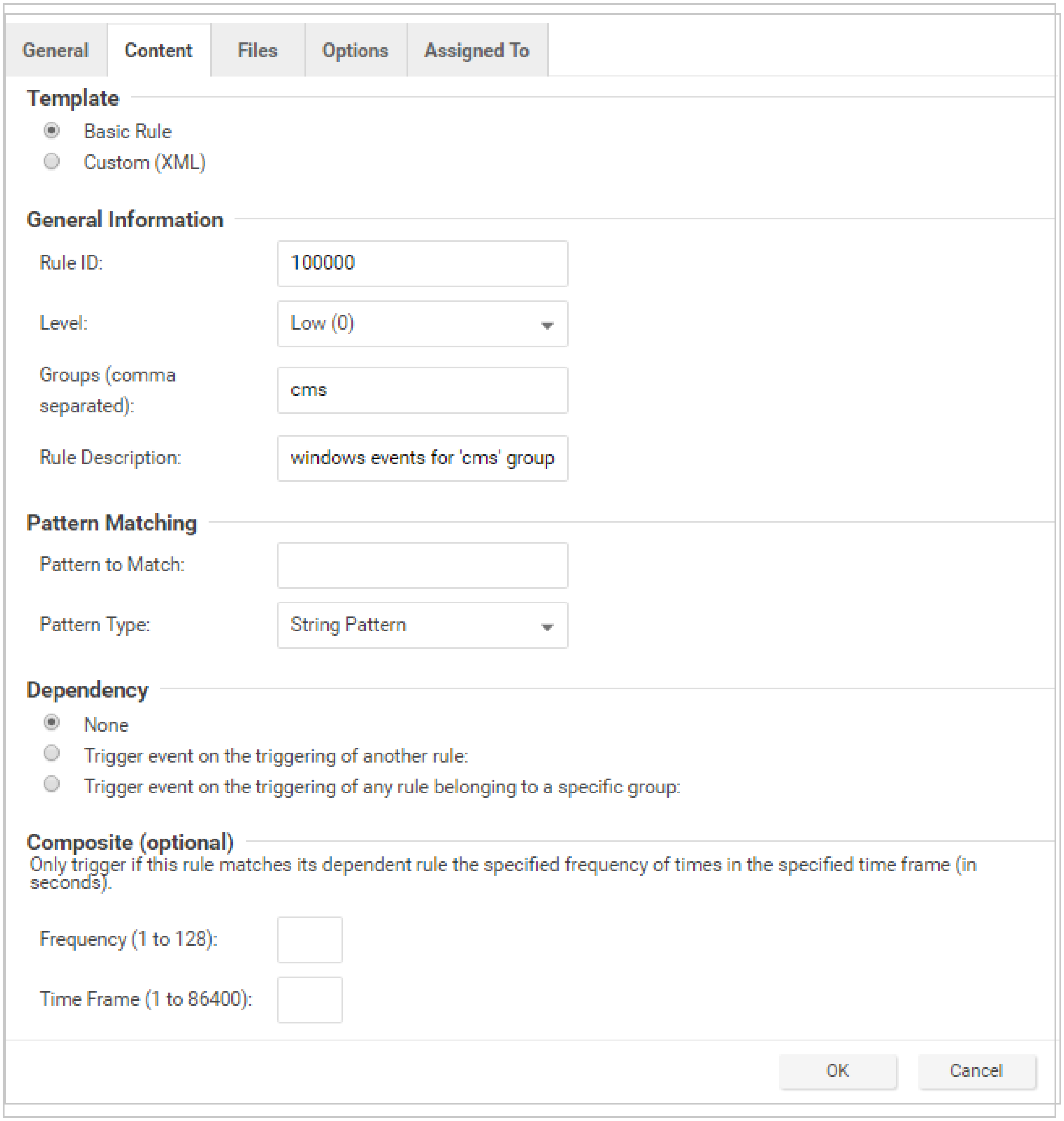
    - Administrator Login successful (Event: 105)
    - Administrator Login unsuccessful (Event: 106)
- General Errors (Type: Error)
    - Database error (Event: 200 to 205)
    - Runtime error (Event: 206-249)
- Application Audit (Type: Information)
    - Content
        - New content added (Event: 450 to 459)
        - Existing content modified (Event: 460 to 469)
        - Existing content deleted (Event: 470 to 479)
    - Administration
        - User
            - New User created (Event: 445 to 446)
            - Existing User deleted (Event: 447 to 449)

This structure provides you with a good basis for rule creation. You can now create a new Log Inspection rule in Deep Security Manager.

**To create the new CMS Log Inspection Rule:**

1. In Deep Security Manager, go to **Policies > Common Objects > Rules > Log Inspection Rules** and click **New** to display the **New Log Inspection Rule Properties** window.
2. Give the new rule a name and a description, and then select the **Content** tab.
3. Select **Basic Rule**. The quickest way to create a new custom rule is to start with a basic rule template.
4. The **Rule ID** field is automatically populated with an unused ID number of 100,000 or greater, the IDs reserved for custom rules.
5. Set the **Level** setting to **Low (0)**.
6. Give the rule an appropriate Group name. In this case, "cms".

7. Provide a short rule description.



**Template**

● Basic Rule
○ Custom (XML)

**General Information**

Rule ID: 100000

Level: Low (0)

Groups (comma separated): cms

Rule Description: windows events for 'cms' group

**Pattern Matching**

Pattern to Match:

Pattern Type: String Pattern

**Dependency**

● None
○ Trigger event on the triggering of another rule:
○ Trigger event on the triggering of any rule belonging to a specific group:

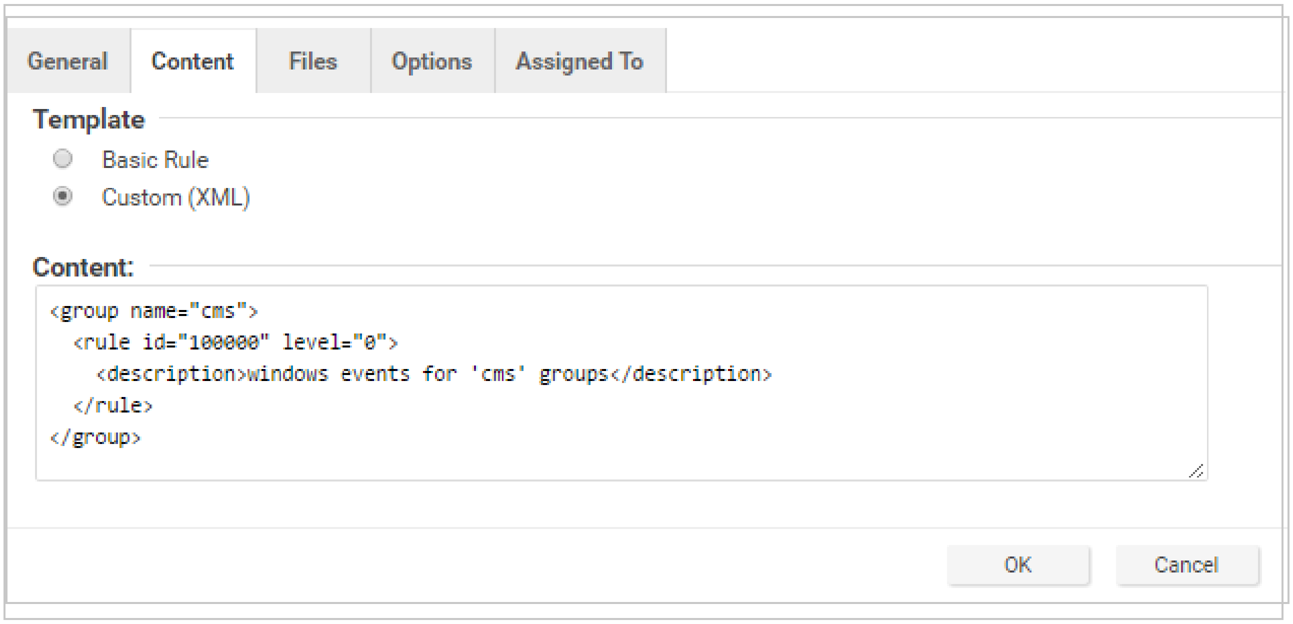
**Composite (optional)**

Only trigger if this rule matches its dependent rule the specified frequency of times in the specified time frame (in seconds).

Frequency (1 to 128):

Time Frame (1 to 86400):

8. Select **Custom (XML)**. The options you selected for your Basic rule will be converted to XML.



Template

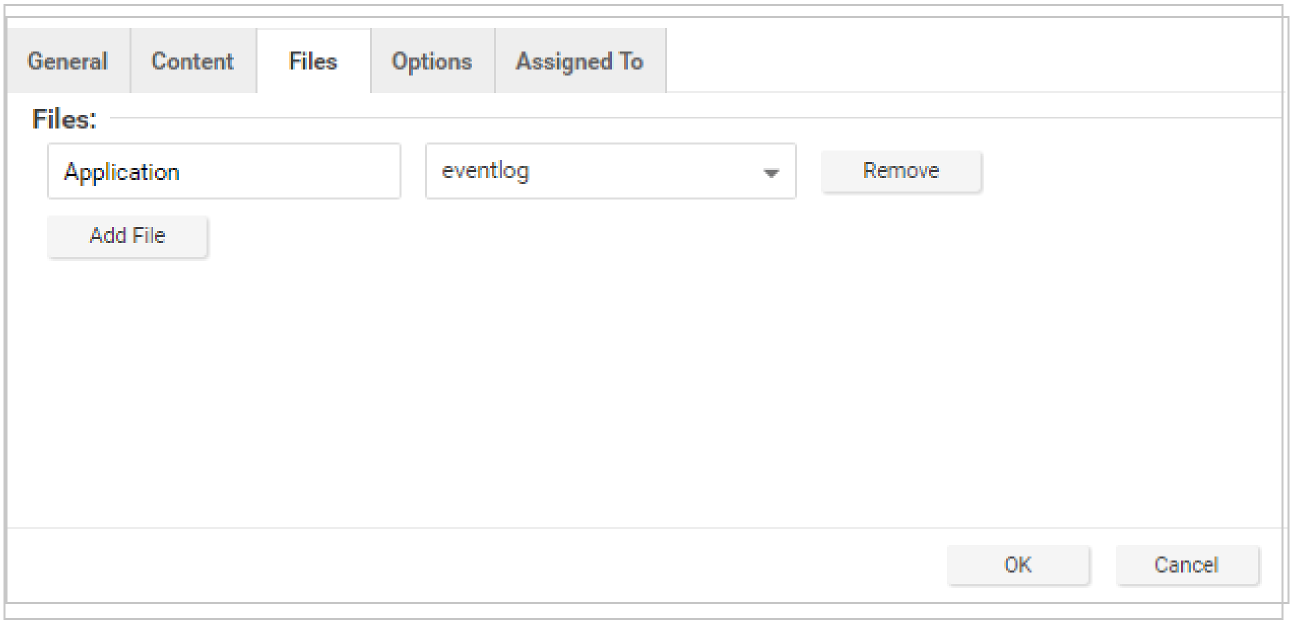
○ Basic Rule

● Custom (XML)

Content:

```
<group name="cms">
  <rule id="100000" level="0">
    <description>windows events for 'cms' groups</description>
  </rule>
</group>
```

9. Select the **Files** tab, and then click the **Add File** to add any application log files and log types to which to apply the rule. In this case, Application, and eventlog as the file type.



Files:

Application | eventlog

**Eventlog** is a unique file type in Deep Security because the location and filename of the log files do not have to be specified. Instead, it is sufficient to type the log name as it is displayed in the Windows Event Viewer. Other log names for the eventlog file type might be Security, System, Internet Explorer, or any other section listed in the Windows Event Viewer. Other file types require the log file's location and filename. C/C++ strftime()

conversion specifiers are available for matching on filenames. See the table for a list of some of the more useful ones.

10. Click **OK** to save the basic rule.
11. Working with the basic rule Custom (XML) created, you can begin adding new rules to the group based on the log groupings identified previously. You need to set the base rule criteria to the initial rule. In the following example, the CMS base rule has identified Windows Event Logs with a Source attribute of `CMS`:

```
<group name="cms">
       <rule id="100000" level="0">
               <category>windows</category>
               <extra_data>^CMS</extra_data>
               <description>Windows events from source 'CMS' group
messages.</description>
       </rule>
```

12. Proceed by building subsequent rules from the identified log groups. The following example identifies the authentication and login success and failure and logs by Event IDs.

```
<rule id="100001" level="0">
       <if_sid>100000</if_sid>
       <id>^100|^101|^102|^103|^104|^105|^106|^107|^108|^109|^110</id>
       <group>authentication</group>
       <description>CMS Authentication event.</description>
</rule>

<rule id="100002" level="0">
       <if_group>authentication</if_group>
       <id>100</id>
       <description>CMS User Login success event.</description>
</rule>
<rule id="100003" level="4">
       <if_group>authentication</if_group>
       <id>101</id>
       <group>authentication_failure</group>
       <description>CMS User Login failure event.</description>
</rule>
<rule id="100004" level="0">
       <if_group>authentication</if_group>
       <id>105</id>
       <description>CMS Administrator Login success event.</description>
</rule>
<rule id="100005" level="4">
       <if_group>authentication</if_group>
       <id>106</id>
       <group>authentication_failure</group>
       <description>CMS Administrator Login failure event.</description>
</rule>
```

13. Add any composite or correlation rules using the established rules. The following example shows a high severity composite rule that is applied to instances where the repeated login failures have occurred five times within a 10 second time period:

```
<rule id="100006" level="10" frequency="5" timeframe="10">
       <if_matched_group>authentication_failure</if_matched_group>
       <description>CMS Repeated Authentication Login failure
event.</description>
</rule>
```

14. Review all rules for appropriate severity levels. For example, error logs should have a severity of level 5 or higher. Informational rules would have a lower severity.
15. Open the newly-created rule, select the **Configuration** tab, and copy your custom rule XML into the rule field. Click **Apply** or **OK** to save the change.

Once the rule is assigned to a policy or computer, the Log Inspection engine should begin inspecting the designated log file immediately.

**The complete Custom CMS Log Inspection Rule:**

```
<group name="cms">
        <rule id="100000" level="0">
               <category>windows</category>
               <extra_data>^CMS</extra_data>
               <description>Windows events from source 'CMS' group
messages.</description>
       </rule>
        <rule id="100001" level="0">
               <if_sid>100000</if_sid>
               <id>^100|^101|^102|^103|^104|^105|^106|^107|^108|^109|^110</id>
               <group>authentication</group>
               <description>CMS Authentication event.</description>
       </rule>
```

```
        <rule id="100002" level="0">
                <if_group>authentication</if_group>
                <id>100</id>
                <description>CMS User Login success event.</description>
        </rule>

        <rule id="100003" level="4">
                <if_group>authentication</if_group>
                <id>101</id>
                <group>authentication_failure</group>
                <description>CMS User Login failure event.</description>
        </rule>

        <rule id="100004" level="0">
                <if_group>authentication</if_group>
                <id>105</id>
                <description>CMS Administrator Login success event.</description>
        </rule>

        <rule id="100005" level="4">
                <if_group>authentication</if_group>
                <id>106</id>
                <group>authentication_failure</group>
                <description>CMS Administrator Login failure event.</description>
        </rule>

        <rule id="100006" level="10" frequency="5" timeframe="10">
                <if_matched_group>authentication_failure</if_matched_group>
                <description>CMS Repeated Authentication Login failure
event.</description>
        </rule>

        <rule id="100007" level="5">
                <if_sid>100000</if_sid>
                <status>^ERROR</status>
                <description>CMS General error event.</description>
                <group>cms_error</group>
        </rule>

        <rule id="100008" level="10">
```

```
                <if_group>cms_error</if_group>
                <id>^200|^201|^202|^203|^204|^205</id>
                <description>CMS Database error event.</description>
        </rule>

        <rule id="100009" level="10">
                <if_group>cms_error</if_group>
                <id>^206|^207|^208|^209|^230|^231|^232|^233|^234|^235|^236|^237|^238|
                        ^239^|240|^241|^242|^243|^244|^245|^246|^247|^248|^249</id>
                <description>CMS Runtime error event.</description>
        </rule>

        <rule id="100010" level="0">
                <if_sid>100000</if_sid>
                <status>^INFORMATION</status>
                <description>CMS General informational event.</description>
                <group>cms_information</group>
        </rule>

        <rule id="100011" level="5">
                <if_group>cms_information</if_group>
                <id>^450|^451|^452|^453|^454|^455|^456|^457|^458|^459</id>
                <description>CMS New Content added event.</description>
        </rule>

        <rule id="100012" level="5">
                <if_group>cms_information</if_group>
                <id>^460|^461|^462|^463|^464|^465|^466|^467|^468|^469</id>
                <description>CMS Existing Content modified event.</description>
        </rule>

        <rule id="100013" level="5">
                <if_group>cms_information</if_group>
                <id>^470|^471|^472|^473|^474|^475|^476|^477|^478|^479</id>
                <description>CMS Existing Content deleted event.</description>
        </rule>

        <rule id="100014" level="5">
                <if_group>cms_information</if_group>
                <id>^445|^446</id>
                <description>CMS User created event.</description>
        </rule>

        <rule id="100015" level="5">
                <if_group>cms_information</if_group>
                <id>^447|449</id>
                <description>CMS User deleted event.</description>
        </rule>

</group>
```

## Log Inspection rule severity levels and their recommended use

| Level | Description | Notes |
|---|---|---|
| Level 0 | Ignored, no action taken | Primarily used to avoid false positives. These rules are scanned before all the others and include events with no security relevance. |
| Level 1 | no predefined use | |
| Level 2 | System low priority notification | System notification or status messages that have no security relevance. |
| Level 3 | Successful or authorized events | Successful login attempts, firewall allow events, and so on. |
| Level 4 | System low priority errors | Errors related to bad configurations or unused devices or applications. They have no security relevance and are usually caused by default installations or software testing. |
| Level 5 | User-generated errors | Missed passwords, denied actions, and so on. These messages typically have no security relevance. |
| Level 6 | Low relevance attacks | Indicate a worm or a virus that provide no threat to the system such as a Windows worm attacking a Linux server. They also include frequently triggered IDS events and common error events. |
| Level 7 | no predefined use | |
| Level 8 | no predefined use | |
| Level 9 | Error from invalid source | Include attempts to login as an unknown user or from an invalid source. The message might have security relevance especially if repeated. They also include errors regarding the **admin** or **root** account. |
| Level 10 | Multiple user generated errors | Include multiple bad passwords, multiple failed logins, and so on. They might indicate an attack, or it might be just that a user forgot his or her credentials. |
| Level 11 | no predefined use | |
| Level 12 | High- | Include error or warning messages from the system, kernel, and so on. |

| Level | Description | Notes |
|---|---|---|
| | importance event | They might indicate an attack against a specific application. |
| Level 13 | Unusual error (high importance) | Common attack patterns such as a buffer overflow attempt, a larger than normal syslog message, or a larger than normal URL string. |
| Level 14 | High importance security event | Typically the result of the correlation of multiple attack rules and indicative of an attack. |
| Level 15 | Attack Successful | Very small chance of false positive. Immediate attention is necessary. |

## strftime() conversion specifiers

| Specifier | Description |
|---|---|
| %a | Abbreviated weekday name (for example, Thu) |
| %A | Full weekday name (for example, Thursday) |
| %b | Abbreviated month name (for example, Aug) |
| %B | Full month name (for example, August) |
| %c | Date and time representation (for example, Thu Sep 22 12:23:45 2007) |
| %d | Day of the month (01 - 31) (for example, 20) |
| %H | Hour in 24 h format (00 - 23) (for example, 13) |
| %I | Hour in 12 h format (01 - 12) (for example, 02) |
| %j | Day of the year (001 - 366) (for example, 235) |
| %m | Month as a decimal number (01 - 12) (for example, 02) |
| %M | Minute (00 - 59) (for example, 12) |
| %p | AM or PM designation (for example, AM) |
| %S | Second (00 - 61) (for example, 55) |
| %U | Week number with the first Sunday as the first day of week one (00 - 53) (for example, 52) |
| %w | Weekday as a decimal number with Sunday as 0 (0 - 6) (for example, 2) |
| %W | Week number with the first Monday as the first day of week one (00 - 53) (for example, 21) |
| %x | Date representation (for example, 02/24/79) |
| %X | Time representation (for example, 04:12:51) |
| %y | Year, last two digits (00 - 99) (for example, 76) |
| %Y | Year (for example, 2008) |
| %Z | Time zone name or abbreviation (for example, EST) |
| %% | A % sign (for example, %) |

For more information, see the following:

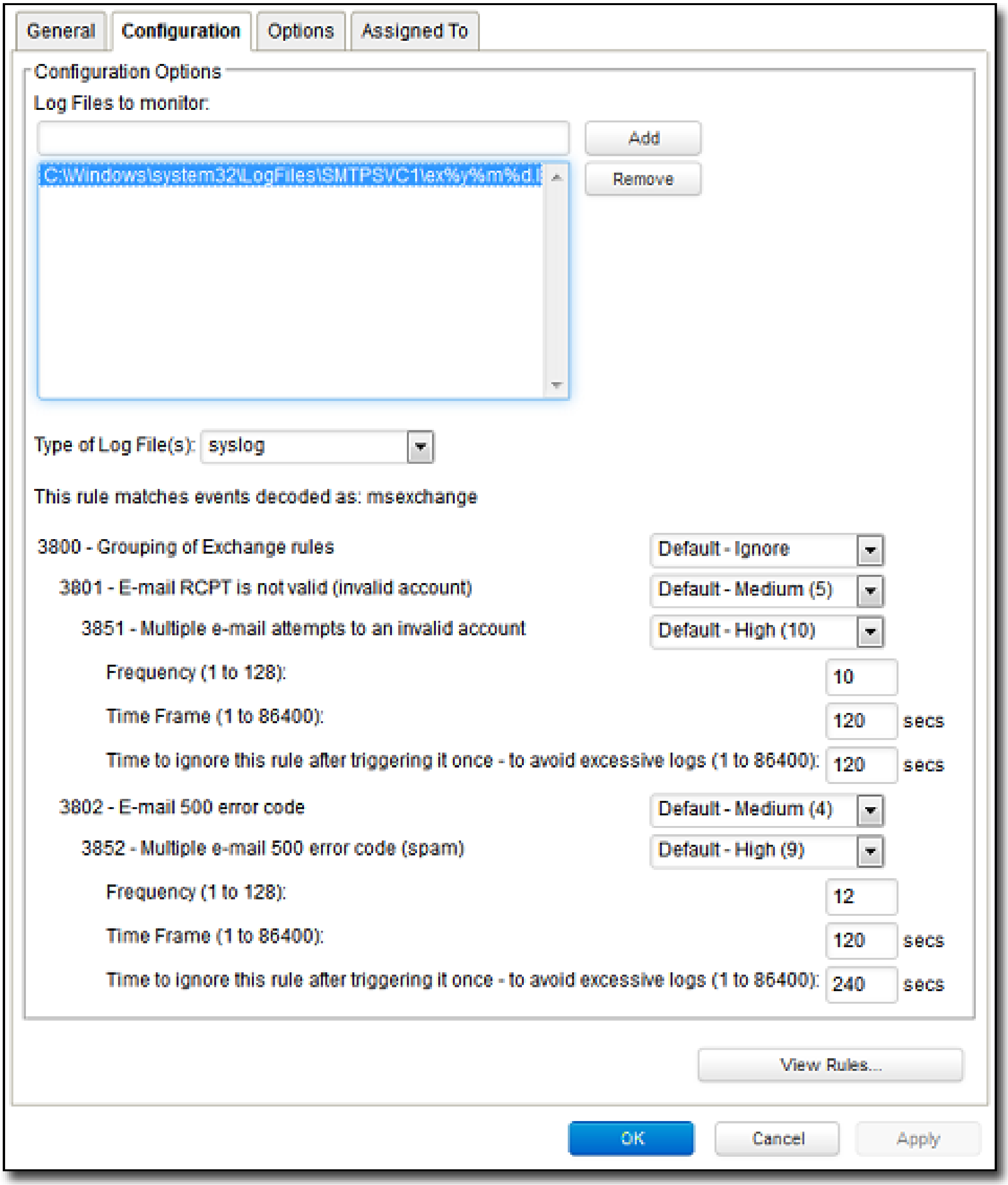
- https://www.php.net/manual/en/function.strftime.php
- www.cplusplus.com/reference/clibrary/ctime/

## Examine a Log Inspection rule

Log Inspection rules are located in Deep Security Manager at **Policies > Common Objects > Rules > Log Inspection Rules**.

### Log Inspection rule structure and the event matching process

The following illustrations shows the contents of the **Configuration** tab of the **Properties** window of the Microsoft Exchange Log Inspection rule:



Configuration Options

Log Files to monitor:

C:\Windows\system32\LogFiles\SMTPSVC1\ex%y%m%d.l

Type of Log File(s): syslog

This rule matches events decoded as: msexchange

3800 - Grouping of Exchange rules: Default - Ignore

3801 - E-mail RCPT is not valid (invalid account): Default - Medium (5)

3851 - Multiple e-mail attempts to an invalid account: Default - High (10)

Frequency (1 to 128): 10

Time Frame (1 to 86400): 120 secs

Time to ignore this rule after triggering it once - to avoid excessive logs (1 to 86400): 120 secs

3802 - E-mail 500 error code: Default - Medium (4)

3852 - Multiple e-mail 500 error code (spam): Default - High (9)

Frequency (1 to 128): 12

Time Frame (1 to 86400): 120 secs

Time to ignore this rule after triggering it once - to avoid excessive logs (1 to 86400): 240 secs

The following is the rule structure:

- 3800 - Grouping of Exchange Rules - Ignore
    - 3801 - Email rcpt is not valid (invalid account) - Medium (4)
        - 3851 - Multiple email attempts to an invalid account - High (9)
            - Frequency - 10
            - Time Frame - 120
            - Ignore - 120
    - 3802 - Email 500 error code - Medium (4)
        - 3852 - Email 500 error code (spam) - High (9)
            - Frequency - 12
            - Time Frame - 120
            - Ignore - 240

The Log Inspection engine applies log events to this structure and checks if a match occurs. For example, if an Exchange event occurs, and this event is an email receipt to an invalid account, the event will match line 3800 (because it is an Exchange event). The event is then be applied to line 3800's subrules: 3801 and 3802.

If there is no further match, this cascade of matches stops at 3800. Because 3800 has a severity level of Ignore, no Log Inspection event would be recorded.

However, an email receipt to an invalid account does match one of 3800's sub-rules: sub-rule 3801. Subrule 3801 has a severity level of Medium(4). If the matching stopped here, a Log Inspection event with a severity level of Medium(4) would be recorded.

But there is still another subrule to be applied to the event: subrule 3851. Subrule 3851 with its three attributes matches if the same event has occurred 10 times within the last 120 seconds. If so, a Log Inspection event with a severity High(9) is recorded. The Ignore attribute tells subrule 3851 to ignore individual events that match subrule 3801 for the next 120 seconds. This is useful for reducing noise.

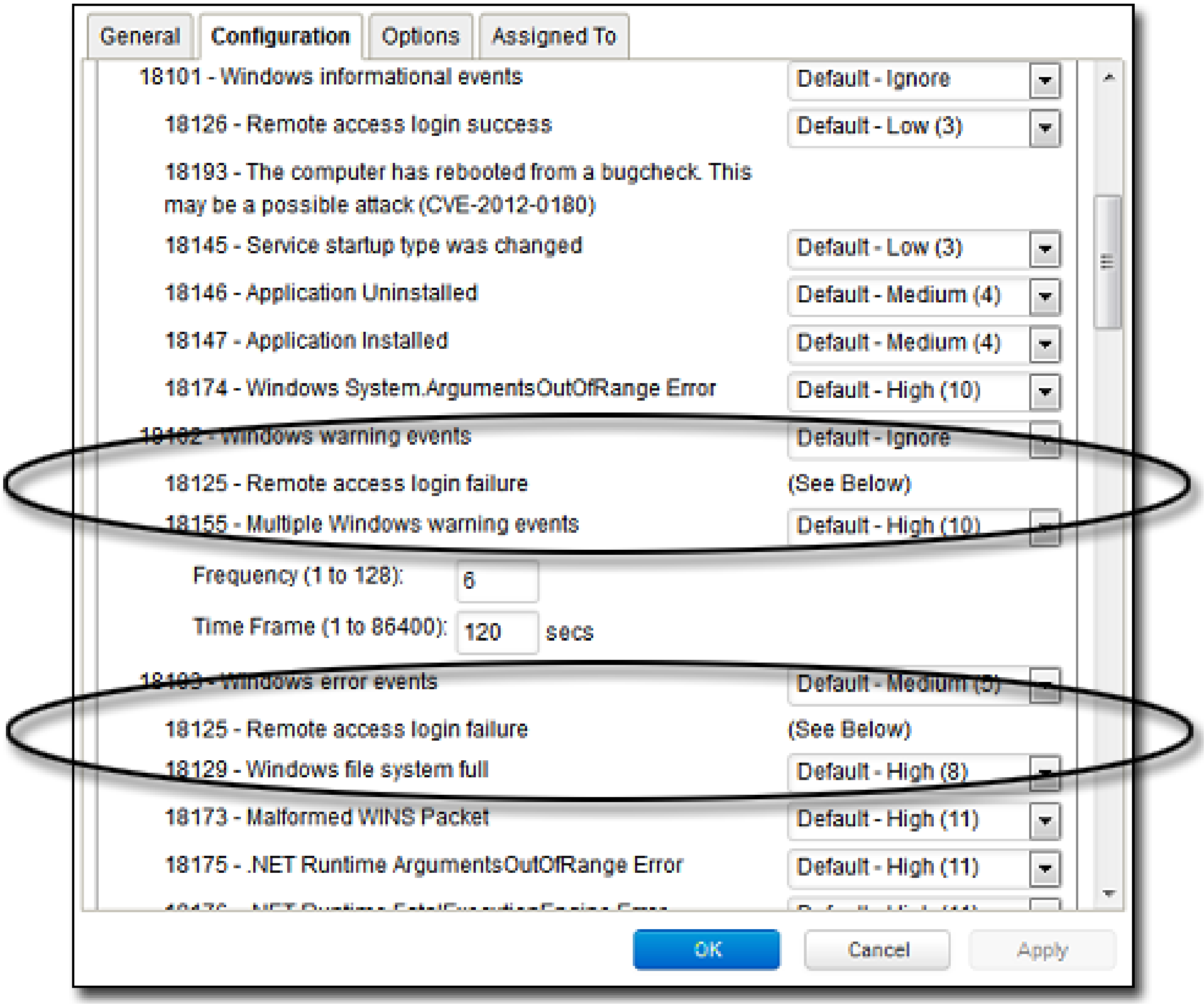
Assuming the parameters of subrule 3851 have been matched, a Log Inspection event with Severity High(9) is now recorded.

Looking at the Options tab of the Microsoft Exchange Rule, you can see that Deep Security Manager raises an alert if any subrules with a severity level of Medium(4) have been matched. Since this is the case in this example, the alert is raised (if **Alert when this rule logs an event** is selected).

### Duplicate Subrules

Some Log Inspection rules have duplicate subrules. To see an example, open the Microsoft Windows Events rule and select the **Configuration** tab. Note that subrule 18125 (Remote access login failure) appears under subrules 18102 and 18103. Also note that in both cases subrule 18125 does not have a severity value, it only says "See Below".

Instead of being listed twice, Rule 18125 is listed once at the bottom of the **Configuration** page:



| | |
|---|---|
| 18101 - Windows informational events | Default - Ignore |
| 18126 - Remote access login success | Default - Low (3) |
| 18193 - The computer has rebooted from a bugcheck. This may be a possible attack (CVE-2012-0180) | |
| 18145 - Service startup type was changed | Default - Low (3) |
| 18146 - Application Uninstalled | Default - Medium (4) |
| 18147 - Application Installed | Default - Medium (4) |
| 18174 - Windows System.ArgumentsOutOfRange Error | Default - High (10) |
| 18102 - Windows warning events | Default - Ignore |
| 18125 - Remote access login failure | (See Below) |
| 18155 - Multiple Windows warning events | Default - High (10) |
| Frequency (1 to 128): | 6 |
| Time Frame (1 to 86400): | 120 secs |
| 18103 - Windows error events | Default - Medium (5) |
| 18125 - Remote access login failure | (See Below) |
| 18129 - Windows file system full | Default - High (8) |
| 18173 - Malformed WINS Packet | Default - High (11) |
| 18175 - .NET Runtime ArgumentsOutOfRange Error | Default - High (11) |

## Create a list of directories for use in policies

Create lists of directory paths for use in multiple policies. A single list is easier to manage than several identical lists that are each created in a different policy. The most common use cases for these lists are for Anti-Malware scan inclusions or exclusions. For more information, see "Specify the files to scan" on page 750.

To create a directory list that is similar to an existing one, duplicate the list and then edit it.

The following table describes the syntax for defining directory list items. The use of forward slashes and backslashes is supported for both Windows and Linux conventions:

| Directory | Format | Description | Examples |
|---|---|---|---|
| Directory | DIRECTORY | Includes all files in the specified directory and all files in all subdirectories. | ***C:\Program Files\***<br>Includes all files in the `Program Files` directory and all subdirectories. |
| Network Resource | \\NETWORK RESOURCE | Includes files on a computer included as a network resource on a targeted computer. | ***\\12.34.56.78\\***<br>***\\some-comp-name\***<br>Includes all files on a network resource (and its subfolders) identified using an IP or a hostname.<br><br>***\\12.34.56.78\somefolder\\***<br>***\\some-comp-name\somefolder\\***<br>Includes all files in the folder `somefolder` and its subfolders on a network resource identified using an IP or a hostname. |
| Directory with wildcard (*) | DIRECTORY*\ | Includes any subdirectories with any subdirectory name, but does not include the files in the specified directory. | ***C:\abc\*\\***<br>Includes all files in all subdirectories of `abc` but does not include the files in the `abc` directory.<br><br>***C:\abc\wx*z\***<br>*Matches:*<br>C:\abc\wxz\<br>C:\abc\wx123z\<br>*Does not match:*<br>C:\abc\wxz<br>C:\abc\wx123z |

| Directory | Format | Description | Examples |
|---|---|---|---|
| | | | ***C:\abc\*wx***<br>*Matches:*<br>C:\abc\wx\<br>C:\abc\123wx\<br>*Does not match:*<br>C:\abc\wx<br>C:\abc\123wx |
| Directory with wildcard (*) | DIRECTORY* | Includes any subdirectories with a matching name, but does not include the files in that directory and any subdirectories. | ***C:\abc\****<br>*Matches:*<br>C:\abc\<br>C:\abc\1<br>C:\abc\123<br>*Does not match:*<br>C:\abc<br>C:\abc\123\<br>C:\abc\123\456<br>C:\abx\<br>C:\xyz\<br><br>***C:\abc\*wx***<br>*Matches:*<br>C:\abc\wx<br>C:\abc\123wx<br>*Does not match:*<br>C:\abc\wx\<br>C:\abc\123wx\<br><br>***C:\abc\wx*z***<br>*Matches:*<br>C:\abc\wxz<br>C:\abc\wx123z<br>*Does not match:*<br>C:\abc\wxz\<br>C:\abc\wx123z\<br><br>***C:\abc\wx****<br>*Matches:*<br>C:\abc\wx<br>C:\abc\wx\<br>C:\abc\wx12<br>C:\abc\wx12\345\<br>C:\abc\wxz\<br>*Does not match:*<br>C:\abc\wx123z\ |
| Environment variable | ${ENV VAR} | Includes all files and subdirectories defined by an environment variable with the format ${ENV VAR}. Windows | ***${windir}***<br>If the variable resolves to `c:\windows`. Includes all |

| Directory | Format | Description | Examples |
|---|---|---|---|
| | | common environment variables, such as `windir`, `programfiles`, and so on, are supported. For a Virtual Appliance and Linux, the value pairs for the environment variable must be defined in **Policy or Computer Editor > Settings > General > Environment Variable Overrides.** | the files in `c:\windows` and all its subdirectories. |
| Comments | DIRECTORY #Comment | Allows you to add comments to your inclusion definitions. | ***c:\abc #Include the abc directory*** |

1. Click **Policies > Common Objects > Lists > Directory Lists**.
2. Click **New > New Directory List**.
3. Type a name and, optionally, a description.
4. In the **Directory(s)** list, add the directory paths, one per line.
5. Click **OK**.

## Import and export directory lists

You can export one or more directory lists to an XML or CSV file, and import lists from an XML file.

1. Click **Policies > Common Objects > Lists > Directory Lists**.
2. To export one or more lists, select them and click **Export > Export Selected to CSV** or **Export > Export Selected to XML**.
3. To export all lists, click **Export > Export to CSV** or **Export > Export to XML**.
4. To import lists, click **New > Import From File** and follow the instructions on the wizard.

## View policies that use directory list

It is useful to see which policies use a directory list to be aware of which policies are affected by any changes you make. For example, you can ensure no policies use a directory list before deleting it.

1. Click **Policies > Common Objects > Lists > Directory Lists**.
2. Select the directory list and click **Properties**.
3. Click the **Assigned To** tab.

## Create a list of file extensions for use in policies

Create lists of file extensions so that you can use them in multiple malware scan configurations. A single list is easier to manage than several identical lists that are each created in a different rule. For example, one list of file extensions can be used by multiple malware scan configurations as files to include in a scan. Another list of file extensions can be used by multiple malware scan configurations as files to exclude from a scan.

Tip: To create a file extension list that is similar to an existing one, duplicate the list and then edit it.

You can insert comments into your list by preceding the text with a pound sign ("#").

1. Click **Policies > Common Objects > Lists > File Extension Lists**.
2. Click **New > New File Extension List**.
3. Type a name and, optionally, a description.
4. In the **File Extension(s)** list, add the extensions, one per line.
5. Click **OK**.

### Import and export file extension lists

You can export one or more file extension lists to an XML or CSV file, and import lists from an XML file.

1. Click **Policies > Common Objects > Lists > File Extension Lists**.
2. To export one or more lists, select them and click **Export > Export Selected to CSV** or **Export > Export Selected to XML**.
3. To export all lists, click **Export > Export to CSV** or **Export > Export to XML**.
4. To import lists, click **New > Import From File** and follow the instructions on the wizard.

### See which malware scan configurations use a file extension list

It is useful to see which malware scan configurations use a file extension list to be aware of which rules are affected by any changes you make. For example, you can ensure no scan configurations use a file extension list before deleting it.

1. Click **Policies > Common Objects > Lists > File Extension Lists**.
2. Select the list and click **Properties**.
3. Click the **Assigned To** tab.

## Create a list of files for use in policies

Create lists of file paths to use in multiple policies. A single list is easier to manage than several identical lists that are each created in a different policy. The most common use cases for these lists are for Anti-Malware scan inclusions or exclusions. For more information, see "Specify the files to scan" on page 750.

To create a file list that is similar to an existing one, duplicate the list and then edit it.

The following table describes the syntax for defining file list items. The use of forward slashes and backslashes is supported for both Windows and Linux conventions:

| Inclusion | Format | Description | Example |
|---|---|---|---|
| File | FILE | Includes all files with the specified file name regardless of its location or directory. | ***abc.doc***<br>Includes all files named "abc.doc" in all directories. Does not include `abc.exe`. |
| File path | FILEPATH | Includes the single file specified by the file path. | ***C:\Documents\abc.doc***<br>Includes only the file named `abc.doc` in the `Documents` directory. |
| File path with wildcard (*) | FILEPATH | Excludes all the files specified by the file path. | ***C:\Documents\abc.co**** (For Windows Agent platforms only) Excludes any file that has file name of `abc` and extension beginning with `.co` in the `Documents` directory. |
| Filename is a wildcard (*) | FILEPATH* | Excludes all files under the path, but does not include the files in unspecified subdirectories. | ***C:\Documents\****<br>Excludes all files under the directory C:\Documents\<br><br>***C:\Documents\SubDirName*****<br>Excludes all files within subdirectories with a folder name that begins with `SubDirName`. Does not exclude all files under `C:\Documents\` or any other subdirectories.<br><br>***C:\Documents\*****<br>Excludes all files within all `direct` subdirectories under `C:\Documents`. Does not exclude files in subsequent subdirectories. |

| Inclusion | Format | Description | Example |
|---|---|---|---|
| **File with wildcard (*)** | FILE* | Includes all files with a matching pattern in the file name. | ***abc*.exe***<br>Includes any file that has prefix of `abc` and extension of `.exe`.<br><br>***.db***<br>*Matches:*<br>123.db<br>abc.db<br>*Does not match:*<br>123db<br>123.abd<br>cbc.dba<br><br>***db***<br>*Matches:*<br>123.db<br>123db<br>ac.db<br>acdb<br>db<br>*Does not match:*<br>db123<br><br>***wxy*.db***<br>*Matches:*<br>wxy.db<br>wxy123.db<br>*Does not match:*<br>wxydb |
| File with wildcard (*) | FILE.EXT* | Includes all files with a matching pattern in the file extension. | ***abc.v****<br>Includes any file that has file name of "abc" and extension beginning with `.v`.<br><br>***abc.*pp***<br>*Matches:*<br>abc.pp<br>abc.app<br>*Does not match:*<br>wxy.app<br><br>***abc.a*p***<br>*Matches:*<br>abc.ap<br>abc.a123p<br>*Does not match:*<br>abc.pp |

| Inclusion | Format | Description | Example |
|---|---|---|---|
| | | | ***abc.**** <br> *Matches:* <br> abc.123 <br> abc.xyz <br> *Does not match:* <br> wxy.123 |
| File with wildcard (*) | FILE*.EXT* | Includes all files with a matching pattern in the file name and in the extension. | ***a*c.a*p*** <br> *Matches:* <br> ac.ap <br> a123c.ap <br> ac.a456p <br> a123c.a456p <br> *Does not match:* <br> ad.aa |
| Environment variable | ${ENV VAR} | Includes files specified by an environment variable with the format ${ENV VAR}. Windows common environment variables, such as `windir`, `programfiles`, and so on, are supported. <br> For a Virtual Appliance and Linux, the value pairs for the environment variable must be defined in **Policy or Computer Editor > Settings > General > Environment Variable Overrides.** | ***${myDBFile}*** <br> Includes the file `myDBFile`. |
| Comments | FILEPATH #Comment | Allows you to add comments to your inclusion definitions. | ***C:\Documents\abc.doc #This a comment*** |

1. Click **Policies > Common Objects > Lists > File Lists**.
2. Click **New > New File List**.
3. Type a name and, optionally, a description.
4. In the **File(s)** list, add the file paths, one per line.
5. Click **OK**.

## Import and export file lists

You can export one or more file lists to an XML or CSV file, and import lists from an XML file.

1. Click **Policies > Common Objects > Lists > File Lists**.
2. To export one or more lists, select them and click **Export > Export Selected to CSV** or **Export > Export Selected to XML**.

3. To export all lists, click **Export > Export to CSV** or **Export > Export to XML**.
4. To import lists, click **New > Import From File** and follow the instructions on the wizard.

### See which policies use a file list

It is useful to see which policies use a file list to be aware of which policies are affected by any changes you make. For example, you can ensure no policies use a file list before deleting it.

1. Click **Policies > Common Objects > Lists > File Lists**.
2. Select the file list and click **Properties**.
3. Click the **Assigned To** tab.

## Create a list of IP addresses for use in policies

Create lists of IP addresses so that you can use them in multiple firewall rules. A single list is easier to manage than several identical lists that are each defined in a different rule.

Tip: To create an IP list that is similar to an existing one, duplicate the list and then edit it.

You can enter an individual IP address, or you can enter IP ranges and masked IPs. You can also insert comments into your IP list by preceding the text with a hash sign ("#").

Masked IP examples are 192.168.0/24, 192.168.2.0/255.255.255.0, and for IPV6 2001:0DB8::CD30:0:0:0:0/ffff:ffff:fff0::. IP range examples are 192.168.0.2 - 192.168.0.125 and, for IPV6, FF01::101 - FF01::102

1. Click **Policies > Common Objects > Lists > IP Lists**.
2. Click **New > New IP List**.
3. Type a name and, optionally, a description.
4. In the **IP(s)** list, add the IP addresses, masked IP addresses, or IP ranges (one per line).
5. Click **OK**.

### Import and export IP lists

You can export one or more IP lists to an XML or CSV file, and import lists from an XML file.

1. Click **Policies > Common Objects > Lists > IP Lists**.
2. To export one or more lists, select them and click **Export > Export Selected to CSV** or **Export > Export Selected to XML**.
3. To export all lists, click **Export > Export to CSV** or **Export > Export to XML**.
4. To import lists, click **New > Import From File** and follow the instructions on the wizard.

### See which rules use an IP list

It is useful to see which firewall rules use an IP list to be aware of which rules are affected by any changes you make. For example, you can ensure no firewall rules use an IP list before deleting it.

1. Click **Policies > Common Objects > Lists > IP Lists**.
2. Select the IP list and click **Properties**.
3. Click the **Assigned To** tab.

## Create a list of ports for use in policies

Create lists of port numbers so that you can use them in multiple rules. A single list is easier to manage than several identical lists that are each created in a different rule.

**Tip:** To create a port list that is similar to an existing one, duplicate the list and then edit it.

Individual ports and port ranges can be included on the list, for example 80, and 20-21. You can insert comments into your port list by preceding the text with a pound sign ("#").

**Note:** For a listing commonly accepted port number assignments, see the Internet Assigned Numbers Authority (IANA). For a list of port numbers used by Deep Security Manager, Relay, or Agent, see "Port numbers, URLs, and IP addresses" on page 478.

1. Click **Policies > Common Objects > Lists > Port Lists**.
2. Click **New > New Port List**.
3. Type a name and, optionally, a description.
4. In the **Port(s)** list, add the port numbers, one per line.
5. Click **OK**.

### Import and export port lists

You can export one or more port lists to an XML or CSV file, and import lists from an XML file.

1. Click **Policies > Common Objects > Lists > Port Lists**.
2. To export one or more lists, select them and click **Export > Export Selected to CSV** or **Export > Export Selected to XML**.
3. To export all lists, click **Export > Export to CSV** or **Export > Export to XML**.
4. To import lists, click **New > Import From File** and follow the instructions on the wizard.

### See which rules use a port list

It is useful to see which rules use a port list to be aware of which rules are affected by any changes you make. For example, you can ensure no rules use a port list before deleting it.

1. Click **Policies > Common Objects > Lists > Port Lists**.
2. Select the port list and click **Properties**.
3. Click the **Assigned To** tab.

## Create a list of MAC addresses for use in policies

Create lists of MAC addresses so that you can use them in multiple policies. A single list is easier to manage than several identical lists that are each created in a different policy.

Tip: To create a MAC list that is similar to an existing one, duplicate the list and then edit it.

MAC lists support MAC addresses in both hyphen- and colon-separated formats, for example 0A-0F-FF-F0-A0-AF and 0A:0F:FF:F0:A0:AF. You can insert comments into your MAC list by preceding the text with a pound sign ("#").

1. Click **Policies > Common Objects > Lists > MAC Lists**.
2. Click **New > New MAC List**.
3. Type a name and, optionally, a description.
4. In the **MAC(s)** list, add the MAC addresses, one per line.
5. Click **OK**.

### Import and export MAC lists

You can export one or more MAC lists to an XML or CSV file, and import lists from an XML file.

1. Click **Policies > Common Objects > Lists > MAC Lists**.
2. To export one or more lists, select them and click **Export > Export Selected to CSV** or **Export > Export Selected to XML**.
3. To export all lists, click **Export > Export to CSV** or **Export > Export to XML**.
4. To import lists, click **New > Import From File** and follow the instructions on the wizard.

### See which policies use a MAC list

It is useful to see which policies use a MAC list to be aware of which policies are affected by any changes you make. For example, you can ensure no policies use a MAC list before deleting it.

1. Click **Policies > Common Objects > Lists > MAC Lists**.
2. Select the MAC list and click **Properties**.
3. Click the **Assigned To** tab.

## Define contexts for use in policies

Contexts are a powerful way of implementing different security policies depending on a computer's network environment.

Contexts are designed to be associated with firewall and intrusion prevention rules. If the conditions defined in the context associated with a rule are met, the rule is applied.

### Configure settings used to determine whether a computer has internet connectivity

1. In the Deep Security Manager, go to **Administration > System Settings > Contexts**.
2. In the **URL for testing Internet Connectivity Status** box, enter the URL to which an HTTP request will be sent to test for internet connectivity. (You must include "http://".)
3. In the **Regular Expression for returned content used to confirm Internet Connectivity Status** box, enter a regular expression that will be applied to the returned content to confirm that HTTP communication was successful. (If you are certain of the returned content, you can use a simple string of characters.)
4. In the **Test Interval** list, select the time interval between connectivity tests.

For example, to test Internet connectivity, you could use the URL "**http://www.example.com**", and the string "**This domain is established to be used for illustrative examples in documents**" which is returned by the server at that URL.

### Define a context

1. In the Deep Security Manager, go to **Policies > Common Objects > Other > Contexts** and then click **New > New Context**.
2. In the **General Information** area, enter the name and description of the context rule. This area also displays the earliest version of the Deep Security Agent the rule will be compatible with.
3. In the **Options** area, specify when the context will be applied:
   - **Context applies when connection is:** Specifying an option here will determine whether the Firewall rule is in effect depending on the ability of the computer to connect to its domain controller or its internet connectivity. (Conditions for testing internet connectivity can be configured in **Administration > System Settings > Contexts**.)

If the domain controller can be contacted directly (via ICMP), the connection is "Local". If it can be contacted via VPN only, then the connection is "Remote".

The time interval between domain controller connectivity tests is the same as the internet connectivity test interval, which is configurable in **Administration > System Settings > Contexts**. The internet connectivity test is only performed if the computer is unable to connect to its domain controller.

- **Context Applies to Interface Isolation Restricted Interfaces:** This context will apply to network interfaces on which traffic has been restricted through the use of interface isolation. This is primarily used for "Allow" or "Force Allow" Firewall rules. See "Detect and configure the interfaces available on a computer" on page 650.

After you assign the context to a rule, it is displayed on the **Assigned To** tab for the context. (To link a security rule to a context, go to the **Options** tab in the security rule's **Properties** window and select the context from the "Context" list.)

## Define stateful firewall configurations

Deep Security's stateful firewall configuration mechanism analyzes each packet in the context of traffic history, correctness of TCP and IP header values, and TCP connection state transitions. In the case of stateless protocols like UDP and ICMP, a pseudo-stateful mechanism is implemented based on historical traffic analysis. Packets are handled by the stateful mechanism as follows:

1. A packet is passed to the stateful routine if it has been allowed through by the static firewall rule conditions,
2. The packet is examined to determine whether it belongs to an existing connection, and
3. The TCP header is examined for correctness (e.g. sequence numbers, flag combinations, etc.).

To create a new stateful configuration, you need to:

1. "Add a stateful configuration " on the next page.
2. "Enter stateful configuration information" on the next page.
3. "Select packet inspection options" on the next page.

When you're done with your stateful configuration, you can also learn how to

- "See policies and computers a stateful configuration is assigned to" on page 734
- "Export a stateful configuration " on page 734
- "Delete a stateful configuration " on page 734

## Add a stateful configuration

There are three ways to define a stateful configuration on the **Policies > Common Objects > Other > Firewall Stateful Configurations** page:

- Create a new configuration. Click **New** > **New Firewall Stateful Configuration**.
- Import a configuration from an XML file. Click **New** > **Import From File**.
- Copy and then modify an existing configuration. Right-click the configuration in the Firewall Stateful Configurations list and then click **Duplicate**. To edit the new configuration, select it and then click **Properties**.

## Enter stateful configuration information

Enter a **Name** and **Description** for the configuration.

## Select packet inspection options

You can define options for IP, TCP, UDP and ICMP packet inspection, end enable Active or Passive FTP.

### IP packet inspection

Under the **General** tab, select the **Deny all incoming fragmented packets** to drop any fragmented packets. Dropped packets will bypass fragmentation analysis and generate an "IP fragmented packet" log entry. Packets with a total length smaller than the IP header length are dropped silently.

**Warning:** Attackers sometimes create and send fragmented packets in an attempt to bypass Firewall Rules.

**Note:** The Firewall Engine, by default, performs a series of checks on fragmented packets. This is default behavior and cannot be reconfigured. Packets with the following characteristics are dropped:

- **Invalid fragmentation flags/offset:** A packet is dropped when either the **DF** and **MF** flags in the IP header are set to 1, or the header contains the **DF** flag set to 1 and an **Offset** value different than 0.
- **First fragment too small:** A packet is dropped if its **MF** flag is set to 1, its **Offset** value is at 0, and it has total length of less than 120 bytes (the maximum combined header length).

- **IP fragment out of boundary:** A packet is dropped if its **Offset** flag value combined with the total packet length exceeds the maximum datagram length of 65535 bytes.
- **IP fragment offset too small:** A packet is dropped if it has a non-zero **Offset** flag with a value that is smaller than 60 bytes.

### TCP packet inspection

Under the **TCP** tab, select which of the following options you would like to enable:

- **Deny TCP packets containing CWR, ECE flags:** These flags are set when there is network congestion.

  Note: RFC 3168 defines two of the six bits from the Reserved field to be used for ECN (Explicit Congestion Notification), as follows:
  - Bits 8 to 15: CWR-ECE-URG-ACK-PSH-RST-SYN-FIN
  - TCP Header Flags Bit Name Reference:
    - Bit 8: CWR (Congestion Window Reduced) [RFC3168]
    - Bit 9: ECE (ECN-Echo) [RFC3168]

  Warning: Automated packet transmission (such as that generated by a denial of service attack, among other things) will often produce packets in which these flags are set.

- **Enable TCP stateful inspection:** Enable stateful inspection at the TCP level. If you enable stateful TCP inspection, the following options become available:
  - **Enable TCP stateful logging:** TCP stateful inspection events will be logged.
  - **Limit the number of incoming connections from a single computer to:** Limiting the number of connections from a single computer can lessen the effect of a denial of service attack.
  - **Limit the number of outgoing connections to a single computer to:** Limiting the number of outgoing connections to a single computer can significantly reduce the effects of Nimda-like worms.
  - **Limit the number of half-open connections from a single computer to:** Setting a limit here can protect you from DoS attacks like SYN Flood. Although most servers have timeout settings for closing half-open connections, setting a value here can prevent half-open connections from becoming a significant problem. If the specified limit for

SYN-SENT (remote) entries is reached, subsequent TCP packets from that specific computer will be dropped.

> Note: When deciding on how many open connections from a single computer to allow, choose your number from somewhere between what you would consider a reasonable number of half-open connections from a single computer for the type of protocol being used, and how many half-open connections from a single computer your system can maintain without getting congested.

- **Enable ACK Storm protection when the number of already acknowledged packets exceeds:** Set this option to log an event that an ACK Storm attack has occurred.
  - **Drop Connection when ACK Storm detected:** Set this option to drop the connection if such an attack is detected.

> Note: ACK Storm protection options are only available on Deep Security Agent 8.0 and earlier.

### FTP Options

Under the **FTP Options** tab, you can enable the following options:

> Note: The following FTP options are available in Deep Security Agent version 8.0 and earlier.

- **Active FTP**
  - **Allow Incoming:** Allow Active FTP when this computer is acting as a server.
  - **Allow Outgoing:** Allow Active FTP when this computer is acting as client.
- **Passive FTP**
  - **Allow Incoming:** Allow Passive FTP when this computer is acting as a server.
  - **Allow Outgoing:** Allow Passive FTP when this computer is acting as a client.

### UDP packet inspection

Under the **UDP** tab, you can enable the following options:

- **Enable UDP stateful inspection:** Select to enable stateful inspection of UDP traffic.

  > Note: The UDP stateful mechanism drops unsolicited incoming UDP packets. For every outgoing UDP packet, the rule will update its UDP "stateful" table and will then only allow

a UDP response if it occurs within 60 seconds of the request. If you wish to allow specific incoming UDP traffic, you will have to create a **Force Allow** rule. For example, if you are running a DNS server, you will have to create a **Force Allow** rule to allow incoming UDP packets to destination port 53.

Warning: Without stateful inspection of UDP traffic, an attacker can masquerade as a DNS server and send unsolicited UDP "replies" from source port 53 to computers behind a firewall.

- **Enable UDP stateful logging:** Selecting this option will enable the logging of UDP stateful inspection events.

### ICMP packet inspection

Under the **ICMP** tab, you can enable the following options:

Note: ICMP stateful inspection is available in Deep Security Agent version 8.0 or earlier.

- **Enable ICMP stateful inspection:** Select to enable stateful inspection of ICMP traffic.

Note: The ICMP (pseudo-)stateful mechanism drops incoming unsolicited ICMP packets. For every outgoing ICMP packet, the rule will create or update its ICMP "stateful" table and will then only allow a ICMP response if it occurs within 60 seconds of the request. (ICMP pair types supported: Type 0 & 8, 13 & 14, 15 & 16, 17 & 18.)

Warning: With stateful ICMP inspection enabled, you can, for example, only allow an ICMP echo-reply in if an echo-request has been sent out. Unrequested echo-replies could be a sign of several kinds of attack including a Smurf amplification attack, a Tribe Flood Network communication between master and daemon, or a Loki 2 back-door.

- **Enable ICMP stateful logging:** Selecting this option will enable the logging of ICMP stateful inspection events.

### Export a stateful configuration

You can export all stateful configurations to a .csv or .xml file by clicking **Export** and selecting the corresponding export action from the list. You can also export specific stateful configurations by first selecting them, clicking **Export** and then selecting the corresponding export action from the list.

### Delete a stateful configuration

To delete a stateful configuration, right-click the configuration in the Firewall Stateful Configurations list, click **Delete** and then click **OK**.

> **Note:** Stateful configurations that are assigned to one or more computers or that are part of a policy cannot be deleted.

### See policies and computers a stateful configuration is assigned to

You can see which policies and computers are assigned to a stateful inspection configuration on the **Assigned To** tab. Click on a policy or computer in the list to see their properties.

## Define a schedule that you can apply to rules

Schedules are reusable timetables that you can assign to rules, agent upgrades, and more.

1. In Deep Security Manager, go to **Policies > Common Objects > Other > Schedules**.
2. Click **New > New Schedule.**
3. In the **General Information** area, enter a name and description used to identify the schedule.
4. Click a time block in the grid to select it. To deselect it, click it while pressing Shift. Schedule periods are defined by hour-long time blocks.

After you assign the schedule to a rule, it is displayed on the **Assigned To** tab for the schedule. To link a security rule to a schedule, go to the **Options** tab in the security rule's **Properties** window and select the schedule from the "Schedule" list.

> **Note:** With agent-based protection, schedules use the same time zone as the protected computer's operating system. With agentless protection, schedules use the same time zone as the Deep Security Virtual Appliance.

# Configure protection modules

## Configure Anti-Malware

### About Anti-Malware

The Deep Security anti-malware module provides agent computers with both real-time and on-demand protection against file-based threats, including malware, viruses, Trojans, and spyware. To identify threats, the anti-malware module checks files on the local hard drive against a comprehensive threat database. The anti-malware module also checks files for certain characteristics, such as compression and known exploit code.

Portions of the threat database are hosted on Trend Micro servers or stored locally as patterns. Deep Security Agents periodically download anti-malware patterns and updates to ensure protection against the latest threats.

> **Note:** A newly installed Deep Security Agent cannot provide anti-malware protection until it has contacted an update server to download anti-malware patterns and updates. Ensure that your Deep Security Agents can communicate with a Deep Security Relay or the Trend Micro Update Server after installation.

The anti-malware module eliminates threats while minimizing the impact on system performance. The anti-malware module can clean, delete, or quarantine malicious files. It can also terminate processes and delete other system objects that are associated with identified threats.

To turn on and configure the anti-malware module, see "Enable and configure Anti-Malware" on page 742.

- "Types of malware scans" on the next page
- "Malware scan configurations" on page 737
- "Malware events" on page 738
- "SmartScan" on page 738
- "Predictive Machine Learning" on page 739
- "Types of malware scans" on the next page

## Types of malware scans

The anti-malware module performs several types of scans. See also "Select the types of scans to run" on page 743.

### Real-time scan

Scan immediately each time a file is received, opened, downloaded, copied, or modified, Deep Security scans the file for security risks. If Deep Security detects no security risk, the file remains in its location and users can proceed to access the file. If Deep Security detects a security risk, it displays a notification message that shows the name of the infected file and the specific security risk.

Real-time scans are in effect continuously unless another time period is configured using the Schedule option.

> Tip: You can configure real-time scanning to run when it will not have a large impact on performance; for example, when a file server is scheduled to back up files.

This scan can run on all platforms supported by the anti-malware module.

### Manual scan

Runs a full system scan on all processes and files on a computer. The time required to complete a scan depends on the number of files to scan and the computer's hardware resources. A manual scan requires more time than a Quick Scan.

A manual scan executes when **Full Scan for Malware** is clicked.

This scan can be run on all platforms supported by the anti-malware module.

### Scheduled scan

Runs automatically on the configured date and time. Use scheduled scan to automate routine scans and improve scan management efficiency.

A scheduled scan runs according to the date and time you specify when you create a **Scan computers for Malware task** using scheduled tasks (see "Schedule Deep Security to perform tasks" on page 1600).

This scan can be run on all platforms supported by the anti-malware module.

### Quick scan

Only scans a computer's critical system areas for currently active threats. A Quick Scan will look for currently active malware but it will not perform deep file scans to look for dormant or stored infected files. It is significantly faster than a Full Scan on larger drives. Quick scan is not configurable.

A Quick Scan runs when you click **Quick Scan for Malware**.

**Note:** Quick Scan can run only on Windows computers.

### Scan objects and sequence

The following table lists the objects scanned during each type of scan and the sequence in which they are scanned.

| Targets | Full Scan (Manual or Scheduled) | Quick Scan |
|---|---|---|
| Drivers | 1 | 1 |
| Trojan | 2 | 2 |
| Process Image | 3 | 3 |
| Memory | 4 | 4 |
| Boot Sector | 5 | - |
| Files | 6 | 5 |
| Spyware | 7 | 6 |

## Malware scan configurations

Malware scan configurations are sets of options that control the behavior of malware scans. When you configure anti-malware using a policy or for a specific computer, you select a malware scan configuration to use. You can create several malware scan configurations and use them with different policies when different groups of computers have different scan requirements.

Real-time, manual, and scheduled scans all use malware scan configurations. Deep Security provides a default malware scan configuration for each type of scan. These scan configurations are used in the default security policies. You can use the default scan configurations as-is, modify them, or create your own.

**Note:** Quick Scans are not configurable, and do not use malware scan configurations.

You can specify which files and directories are included or excluded during a scan and which actions are taken if malware is detected on a computer (for example, clean, quarantine, or delete).

For more information, see "Configure malware scans and exclusions" on page 745.

## Malware events

When Deep Security detects malware it triggers an event that appears in the event log. From there you can see information about the event, or create an exception for the file in case of false positives. You can also restore files that are actually benign.

For details, see:

- "Anti-malware events" on page 1285
- "View and restore identified malware" on page 780
- "Configure advanced exploit exceptions" on page 787

## SmartScan

Smart Scan uses threat signatures that are stored on Trend Micro servers and provides several benefits:

- Provides fast, cloud-based, real-time security status lookups
- Reduces the time required to deliver protection against emerging threats
- Reduces network bandwidth consumed during pattern updates (bulk of pattern definition updates only need to be delivered to the cloud, not to many computers)
- Reduces cost and overhead of corporate-wide pattern deployments
- Lowers kernel memory consumption on computers (consumption increases minimally over time)

When Smart Scan is enabled, Deep Security first scans locally for security risks. If Deep Security cannot assess the risk of the file during the scan, it will try to connect to a local Smart Scan server. If no local Smart Scan Server is detected, Deep Security will attempt to connect to the Trend Micro Global Smart Scan server. For more information on this feature, see "Smart Protection in Deep Security" on page 777.

## Predictive Machine Learning

Deep Security provides enhanced malware protection for unknown threats and zero-day attacks through Predictive Machine Learning. Trend Micro Predictive Machine Learning uses advanced machine learning technology to correlate threat information and perform in-depth file analysis to detect emerging security risks through digital DNA fingerprinting, API mapping, and other file features.

Predictive Machine Learning is effective in protecting against security breaches that result from targeted attacks using techniques such as phishing and spear phishing. In these cases, malware that is designed specifically to target your environment can bypass traditional malware scanning techniques.

During real-time scans, when Deep Security detects an unknown or low-prevalence file, Deep Security scans the file using the Advanced Threat Scan Engine (ATSE) to extract file features. It then sends the report to the Predictive Machine Learning engine on the Trend Micro Smart Protection Network. Through the use of malware modeling, Predictive Machine Learning compares the sample to the malware model, assigns a probability score, and determines the probable malware type that the file contains.

If the file is identified as a threat, Deep Security cleans, quarantines, or deletes the file to prevent the threat from continuing to spread across your network.

For information about using Predictive Machine Learning, see "Detect emerging threats using Predictive Machine Learning" on page 768.

## Malware types

The anti-malware module protects against many file-based threats. See also "Scan for specific types of malware" on page 747 and "Configure malware handling" on page 759

### Virus

Viruses infect files by inserting malicious code. Typically, when an infected file is opened the malicious code automatically runs and delivers a payload in addition to infecting other files. Below are some of the more common types of viruses:

- **COM and EXE infectors** infect DOS and Windows executable files, which typically have COM and EXE extensions.
- **Macro viruses** infect Microsoft Office files by inserting malicious macros.

- **Boot sector viruses** infect the section of hard disk drives that contain operating system startup instructions

The anti-malware module uses different technologies to identify and clean infected files. The most traditional method is to detect the actual malicious code that is used to infect files and strip infected files of this code. Other methods include regulating changes to infectable files or backing up such files whenever suspicious modifications are applied to them.

### Trojans

Some malware does not spread by injecting code into other files. Instead, it has other methods or effects:

- **Trojans:** Malware files that execute and infect the system when opened (like the mythological Trojan horse).
- **Backdoors:** Malicious applications that open port numbers to allow unauthorized remote users to access infected systems.
- **Worms:** Malware programs that use the network to propagate from system to system. Worms are known to propagate by taking advantage of social engineering through attractively packaged email messages, instant messages, or shared files. They are also known to copy themselves to accessible network shares and spread to other computers by exploiting vulnerabilities.
- **Network viruses:** Worms that are memory-only or packet-only programs (not file-based). Anti-malware is unable to detect or remove network viruses.
- **Rootkits:** File-based malware that manipulate calls to operating system components. Applications, including monitoring and security software, need to make such calls for very basic functions, such as listing files or identifying running processes. By manipulating these calls, rootkits are able to hide their presence or the presence of other malware.

### Packer

Packers are compressed and encrypted executable programs. To evade detection, malware authors often pack existing malware under several layers of compression and encryption. Anti-malware checks executable files for compression patterns associated with malware.

### Spyware/grayware

Spyware and grayware comprises applications and components that collect information to be transmitted to a separate system or collected by another application. Spyware/grayware detections, although exhibiting potentially malicious behavior, may include applications used for legitimate purposes such as remote monitoring. Spyware/grayware applications that are inherently malicious, including those that are distributed through known malware channels, are typically detected as other Trojans.

Spyware and grayware applications are typically categorized as:

- **Spyware:** software installed on a computer to collect and transmit personal information.
- **Dialers:** malicious dialers are designed to connect through premium-rate numbers causing unexpected charges. Some dialers also transmit personal information and download malicious software.
- **Hacking tools:** programs or sets of programs designed to assist unauthorized access to computer systems.
- **Adware (advertising-supported software):** any software package that automatically plays, displays, or downloads advertising material.
- **Cookies:** text files stored by a Web browser. Cookies contain website-related data such as authentication information and site preferences. Cookies are not executable and cannot be infected; however, they can be used as spyware. Even cookies sent from legitimate websites can be used for malicious purposes.
- **Keyloggers:** software that logs user keystrokes to steal passwords and other private information. Some keyloggers transmit logs to remote systems.

### What is grayware?

Although they exhibit what can be intrusive behavior, some spyware-like applications are considered legitimate. For example, some commercially available remote control and monitoring applications can track and collect system events and then send information about these events to another system. System administrators and other users may find themselves installing these legitimate applications. These applications are called "grayware".

To provide protection against the illegitimate use of grayware, the anti-malware module detects grayware but provides an option to "approve" detected applications and allow them to run.

### Cookie

Cookies are text files stored by a web browser, transmitted back to the web server with each HTTP request. Cookies can contain authentication information, preferences, and (in the case of stored attacks from an infected server) SQL injection and XSS exploits.

#### Other threats

Other threats includes malware not categorized under any of the malware types. This category includes joke programs, which display false notifications or manipulate screen behavior but are generally harmless.

#### Possible malware

Possible malware is a file that appears suspicious but cannot be classified as a specific malware variant. When possible malware is detected, Trend Micro recommends that you contact your support provider for assistance in further analysis of the file. By default, these detections are logged and files are sent back to Trend Micro for analysis in a protected manner.

# Set up Anti-Malware

## Enable and configure Anti-Malware

To use the Deep Security Anti-Malware module, perform the following:

1. "Enable the Anti-Malware module" below.
2. "Select the types of scans to run" on the next page.
3. "Configure scan exclusions" on the next page
4. "Configure multiple scan list exclusions and inclusion" on the next page
5. "Update Deep Security about the latest threats" on page 744
6. Review the information provided in "Configure malware scans and exclusions" on page 745 and refine the anti-malware scan behavior

Most anti-malware settings should be configured either for each individual computer or in a policy that applies to multiple computers (for example, applicable to all Windows 2008 Servers). To streamline the management, configure the settings in the policy (as opposed to individual computers) wherever possible. For more information, see "Policies, inheritance, and overrides" on page 634.

CPU usage and RAM usage varies by your anti-malware configuration. To optimize anti-malware performance on Deep Security Agent, see "Improve Anti-Malware performance" on page 763.

For for information, see "About Anti-Malware" on page 735.

### Enable the Anti-Malware module

1. Go to **Policies**.
2. Double-click the policy for which you want to enable Anti-Malware.

3. Go to **Anti-Malware > General**.
4. From **Anti-Malware State**, select **On**.
5. Click **Save**.

### Select the types of scans to run

When anti-malware is enabled, do the following to inform Deep Security about the type of scans it should run (see "Types of malware scans" on page 736):

1. Go to **Policies**.
2. Double-click the policy to configure.
3. Click **Anti-Malware > General**.
4. Enable or disable each type of scan:
   a. To perform the scan using default settings, select **Default**.
   b. To perform the scan using a malware scan configuration that you can customize, select a malware scan configuration.
   c. To disable the scan, for the malware scan configuration select **No Configuration**.
5. Click **Save**.

Trend Micro recommends that you configure Deep Security to perform weekly scheduled scans on all protected servers. You can do this using scheduled tasks. See "Schedule Deep Security to perform tasks" on page 1600.

### Configure scan exclusions

To reduce scanning time and minimize the use of computing resources, you can configure Deep Security malware scans to exclude specific folders, files, and file types from all types of scans. You can also exclude process image files from real-time malware scans that are run on Windows servers.

All of these exclusions are specified by selecting exclusion lists on the **Exclusions** tab of the **Malware Scan Configuration** editor. See "Specify the files to scan" on page 750.

If any performance-related issues are experienced when Deep Security anti-malware protection is enabled, you can use exclusions to help troubleshoot these issues by excluding specific folders or files from scanning.

### Configure multiple scan list exclusions and inclusion

After using the properties of the malware scan configuration to configure scan exclusions and inclusions for one list for a specific list type, you may choose to perform additional configurations. That is, Deep Security enables you to configure multiple scan list exclusions and inclusion at the policy level. It extends to the list specified in the malware scan configuration. Note that you must enable and configure the list for the scan list type in the malware scan configuration first before using multiple scan list.

The **All directories** setting disables the directory lists from multi-list scan inclusions. The **All files** and **File types that are identified by IntelliScan** settings disable the file extension lists from multi-list scan inclusions.

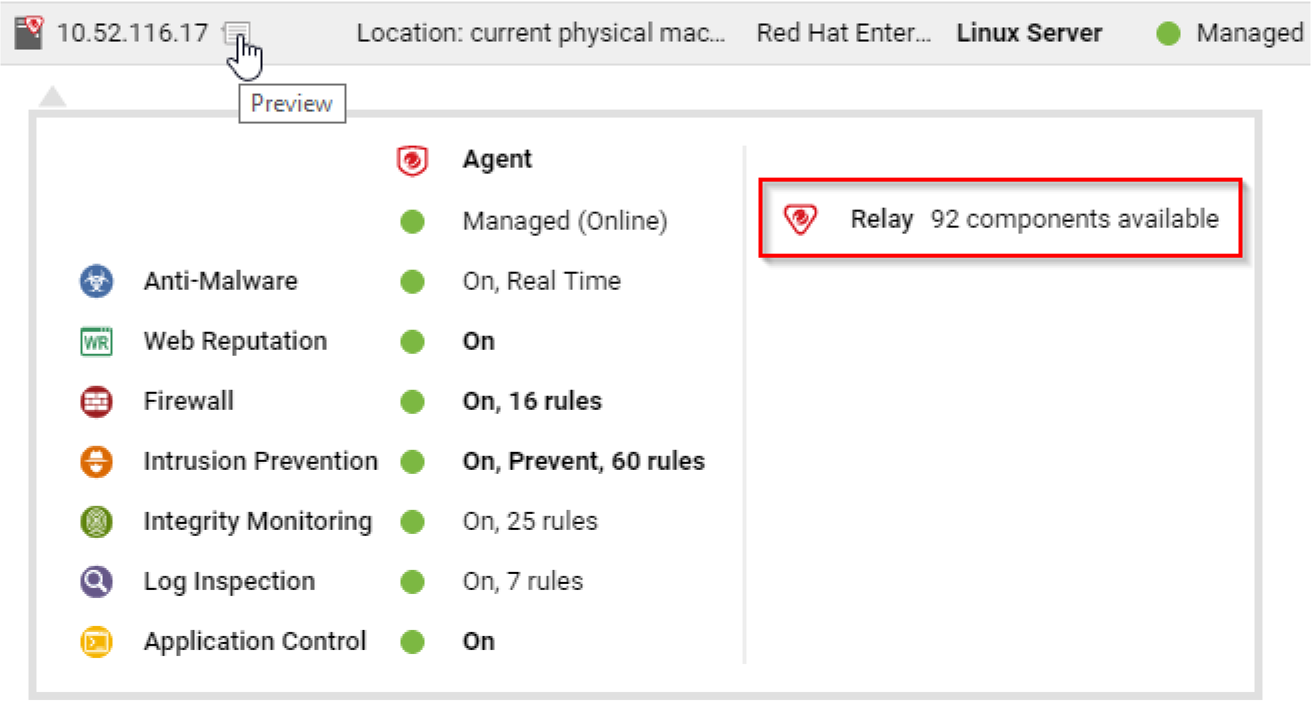
1. Go to **Policies**.
2. Double-click the policy to configure.
3. Go to **Anti-Malware > Exclusions**.
4. Select the type of scan to which you want to add the exclusions: Real-Time, Scheduled, or Manual. You can configure the following lists for these scan types:
   a. **File list**
   b. **Directory list**
   c. **File extension list**
   d. **Process image file list** (for real-time scan only)
5. To add, create, or delete lists, do the following:
   a. To add all inherited lists, select **Use inherited list**.
   b. To add non-inherited lists, select the lists and click **Add**.
   c. To create a new list, select **New**. For more information, see "Create a list of files for use in policies" on page 722.
   d. To delete a non-inherited list, select its garbage can icon. To remove inherited lists, you must deselect **Use inherited lists**.
6. Click **Save**.

When done, scan list inclusions or exclusions are combined using any added scan lists, as well as any added file lists, directory lists, and file extension lists from computers or policies. Duplicates between lists do not interfere with the behavior of inclusions and exclusions.

### Update Deep Security about the latest threats

To remain effective against new viruses and exploits, Deep Security Agents need to be able to download the latest software and security update packages from Trend Micro or indirectly, from your own Relay. These packages contain threat definitions and patterns. Relay-enabled agents, organized into relay groups (also managed and configured by the Deep Security Manager) retrieve security updates from Trend Micro, and then distribute them to other agents and appliances.

1. Go to **Administration > System Settings > Updates.**
2. Configure Deep Security's ability to retrieve security updates from Trend Micro. Make sure you have at least one relay-enabled agent, and it is assigned to the appropriate agents and appliances.
   To determine if a Deep Security Agent is a relay, next to a computer, click **Preview**.



10.52.116.17 | Location: current physical mac... | Red Hat Enter... | **Linux Server** | ● Managed

Preview

| | | |
|---|---|---|
| | | **Agent** |
| | ● | Managed (Online) |
| Anti-Malware | ● | On, Real Time |
| Web Reputation | ● | **On** |
| Firewall | ● | **On, 16 rules** |
| Intrusion Prevention | ● | **On, Prevent, 60 rules** |
| Integrity Monitoring | ● | On, 25 rules |
| Log Inspection | ● | On, 7 rules |
| Application Control | ● | **On** |

**Relay** 92 components available

3. Go to **Administration > Scheduled Tasks**.
4. Verify that there is a scheduled task to regularly download available updates for both security and software updates.

## Configure malware scans and exclusions

Malware scan configurations are reusable saved settings that you can apply when configuring anti-malware in a policy or for a computer. A malware scan configuration specifies what types of malware scanning Deep Security performs and which files it scans. Some policy properties also affect the behavior of malware scans. You can perform the following:

- "Create or modify a malware scan configuration" on the next page
- "Scan for specific types of malware" on page 747
- "Specify the files to scan" on page 750
- "Specify when real-time scans occur" on page 759

- "Configure malware handling" on page 759
- "Identify malware files by file hash digest" on page 762
- "Configure notifications on the computer" on page 762

The Deep Security Best Practice Guide also provides several recommendations for configuration of malware scans.

CPU usage and RAM usage varies by your anti-malware configuration. For information on how to optimize anti-malware performance in Deep Security Agent, see "Improve Anti-Malware performance" on page 763.

### Create or modify a malware scan configuration

You can create or modify one or more malware scan configurations to control the behavior of a real-time, manual, or scheduled scan. For more information, see "Malware scan configurations" on page 737.

- After you create a malware scan configuration, you can then associate it with a scan in a policy or computer. For more information, see "Select the types of scans to run" on page 743.
- When you edit a malware scan configuration that a policy or computer is using, the changes affect the scans that are associated with the configuration.

To create a malware scan configuration that is similar to an existing one, duplicate the existing configuration and then edit it.

You can create two types of malware scan configurations according to the type of scan it controls (see "Types of malware scans" on page 736):

- Real-time scan configuration: Controls real-time scans. Some actions such as **Deny Access** are only available for real-time scan configurations
- Manual/scheduled scan configuration: Controls manual and scheduled scans. Some options such as **CPU Usage** are only available for manual and scheduled scan configurations.

Deep Security provides a default malware scan configuration for each type of scan. You can use this configuration as follows:

1. Go to **Policies > Common Objects > Other > Malware Scan Configurations**.
2. To create a scan configuration, click **New**, click **New Real-Time Scan Configuration** or **New Manual/Scheduled Scan Configuration**, and then:

   a. Type a name to identify the scan configuration. You see the name in a list when configuring malware scans in a policy.
   b. Optionally, type a description that explains the use case for the configuration.
3. To view and edit an existing scan configuration, select it and click **Properties**.
4. To duplicate a scan configuration, select it and click **Duplicate**.

To see the policies and computers that are using a malware scan configuration, see the **Assigned To** tab of the properties.

# Test malware scans

Before continuing with Anti-Malware configuration steps, test scans to ensure they are working correctly.

To test a real-time scan:

1. Make sure the real-time scan is enabled and that a configuration is selected.
2. Go to the EICAR site and download their anti-malware test file. This standardized file tests the real-time scan's anti-virus capabilities. The file should be quarantined.
3. On Deep Security Manager, go to **Events & Reports > Anti-Malware Events** to verify the record of the EICAR file detection. If the detection is recorded, the Anti-Malware real-time scans are working correctly.

To test a manual or scheduled scan:

1. Make sure the real-time scan is disabled.
2. Go to **Administration**.
3. Click **Scheduled tasks > New**.
4. Select **Scan Computers for Malware** from the menu and select frequency. Complete the scan configuration with your desired specifications.
5. Go to the EICAR site and download their anti-malware test file. This standardized file tests the manual or scheduled scan's anti-virus capabilities.
6. Select the scheduled scan and click **Run Task Now**. The test file should be quarantined.
7. On Deep Security Manager, go to **Events & Reports > Anti-Malware Events** to verify the record of the EICAR file detection. If the detection is recorded, the Anti-Malware manual and scheduled scans are working correctly.

### Scan for specific types of malware

- "Enable Windows AMSI protection (real-time scans only)" on the next page
- "Scan for spyware and grayware" on the next page

- "Scan for compressed executable files (real-time scans only)" below
- "Scan process memory" on the next page
- "Scan compressed files" on the next page
- "Scan embedded Microsoft Office objects" on page 750

See also:

- "Enhanced anti-malware and ransomware scanning with behavior monitoring" on page 770

## Enable Windows AMSI protection (real-time scans only)

The Windows Antimalware Scan Interface (AMSI) is an interface provided by Microsoft in Windows 10 and newer. Deep Security leverages AMSI to help detect malicious scripts. By default, this option is enabled in Deep Security malware scan configurations.

1. Open the properties of the malware scan configuration.
2. On the **General** tab, select **Enable AMSI protection**.
3. Click **OK**.

## Scan for spyware and grayware

When spyware and grayware protection is enabled, the spyware scan engine quarantines suspicious files when they are detected.

1. Open the properties of the malware scan configuration.
2. On the **General** tab, select **Enable spyware/grayware protection**.
3. Click **OK**.

To identify a file that the spyware scan engine should ignore, see "Configure advanced exploit exceptions" on page 787.

## Scan for compressed executable files (real-time scans only)

Viruses often use real-time compression algorithms to attempt to circumvent virus filtering. The IntelliTrap feature blocks real-time compressed executable files and pairing them with other malware characteristics.

Because IntelliTrap identifies such files as security risks and may incorrectly block safe files, consider quarantining (not deleting or cleaning) files when you enable IntelliTrap. For more information, see "Configure malware handling" on page 759. If the exchange of real-time compressed executable files is performed regularly, disable IntelliTrap. IntelliTrap uses the virus scan engine, IntelliTrap Pattern, and IntelliTrap Exception Pattern.

1. Open the properties of the malware scan configuration.
2. On the **General** tab, select **Enable IntelliTrap**.
3. Click **OK**.

## Scan process memory

Monitor process memory and perform additional checks with the Trend Micro Smart Protection network to determine whether or not a suspicious process is known to be malicious. If the process is malicious, Deep Security terminates the process. For more information, see "Smart Protection in Deep Security" on page 777

1. Open the properties of the malware scan configuration.
2. On the **General** tab, select **Scan process memory for malware**.
3. Click **OK**.

With Deep Security Agent version 20.0.1-12510 and later, you can use **Action to take** to select the remediation action that Deep Security takes when it detects malware. The recommended value is **ActiveAction**. Or you could select **Pass**. For more information, see "ActiveAction actions" on page 761 and "Customize malware remedial actions" on page 759

## Scan compressed files

Extract compressed files and scan the contents for malware. When you enable the scan, you specify the maximum size and number of files to extract (large files can affect performance). You also specify the levels of compression to inspect so that you can scan compressed files that reside inside compressed files. Level 1 compression is a single compressed file. Compressed files inside that file are level two. You can scan a maximum of 6 compression levels, however higher levels can affect performance.

1. Open the properties of the malware scan configuration.
2. On the **Advanced** tab, select **Scan compressed files**.
3. Specify the maximum size of content files to extract, in MB, the levels of compression to scan, and the maximum number of files to extract.
4. Click **OK**.

# Scan embedded Microsoft Office objects

Certain versions of Microsoft Office use Object Linking and Embedding (OLE) to insert files and other objects into Office files. These embedded objects can contain malicious code.

After you have enabled "Scan compressed files" on the previous page, you can specify the number of OLE layers to scan to detect objects that are embedded in other objects. To reduce the impact on performance, you can scan only a few layers of embedded objects within each file.

1. Open the properties of the malware scan configuration.
2. On the **Advanced** tab, select **Scan Embedded Microsoft Office Objects**.
3. Specify the number of OLE layers to scan.
4. Click **OK**.

### Enable a manual scan for the notifier application on Windows OS

Enabling a manual scan through the Trend Micro notifier application is supported for Deep Security Agents 20.0.0-7476 and later.

This scan is disabled by default. You can enable and trigger it as follows:

1. From the **Computer** or **Policy** editor, select **Anti-Malware > General**.
2. Under **Manual Scan**, select **Allow the agent to trigger or cancel a manual scan**.

Note that agentless scans are not supported.

### Enable a manual scan on Linux OS

Enabling a manual scan is supported for Deep Security Agents 20.0.0-7476 and later.

This scan is disabled by default. You can enable it as follows:

1. From the **Computer** or **Policy** editor, select **Anti-Malware > General**.
2. Under **Manual Scan**, select **Allow the agent to trigger or cancel a manual scan**.

Note that agentless scans are not supported.

### Specify the files to scan

Identify files and directories to include in the scan and then identify any exclusions from those files and directories. You can also scan network directories.

- "Inclusions" on the next page
- "Exclusions" on the next page

- "Scan a network directory (real-time scan only)" on page 759

## Inclusions

Specify the directories to scan as well as the files inside the directories to scan.

To identify directories to scan, you can specify all directories or a list of directories. The directory list uses patterns with a specific syntax to identify the directories to scan. For more information, see "Syntax for directory lists" on page 753.

To identify the files to scan, use one of the following options:

- All files
- File types that are identified by IntelliScan. IntelliScan only scans file types that are vulnerable to infection, such as `.zip` or `.exe`. IntelliScan does not rely on file extensions to determine file type but instead reads the header and content of a file to determine whether it should be scanned. Compared to scanning all files, Intelliscan reduces the number of files to scan and improves performance.
- Files that have a file name extension that is included in a specified list: The file extension list uses patterns with a specific syntax. For more information, see "Syntax of file extension lists" on page 757.

1. Open the properties of the malware scan configuration.
2. Click the **Inclusions** tab.
3. To specify the directories to scan, select **All directories** or **Directory List**.
4. If you selected Directory List, from the drop-down menu either select an existing list or select **New** to create one.
5. To specify the files to scan, select either **All files**, **File types scanned by IntelliScan**, or **File Extension List**.
6. If you selected **File Extension List**, from the menu either select an existing list or select **New** to create one.
7. Click **OK**.

## Exclusions

Exclude directories, files, and file extensions from being scanned. For real-time scans (except when performed by Deep Security Virtual Appliance), you can also exclude process image files from being scanned.

The following are examples of files and folders to exclude:

- If you are creating a malware scan configuration for a Microsoft Exchange server, you should exclude the SMEX quarantine folder to avoid re-scanning files that have already been confirmed to be malware.
- If you choose to run malware scans on database servers used by Deep Security Manager, exclude the data directory. The Deep Security Manager captures and stores intrusion prevention data that might include viruses, which can trigger a quarantine by the Deep Security Agent, leading to database corruption.
- If you have large VMware images, exclude the directory containing these images if you experience performance issues.

You can also exclude files from Anti-Malware scanning when they are signed by a trusted digital certificate. This type of exclusion is defined in policy or computer settings. For more information, see "Exclude files signed by a trusted certificate" on page 793.

## Exclude directories, files, and process image files by creating a list of patterns to exclude

1. Open the properties of the malware scan configuration.
2. Click the **Exclusions** tab.
3. Specify the directories to exclude:
   a. Select  **Directory List**.
   b. Select a directory list or select New to create one. For more information, see "Syntax for directory lists" on the next page.
   c. If you created a directory list, select it in the directory list.
4. Similarly, specify the file list, file extension list, and process image file list to exclude. For more information, see "Syntax of file lists" on page 755, "Syntax of file extension lists" on page 757, and "Syntax of process image file lists" on page 757)
5. Click **OK**.

When Deep Security Agent cannot determine the type of a target file, the Anti-Malware scan engine loads the file to memory to identify if it was a self-extracting file. If many large files are loaded to memory, it can affect scan engine performance. To exclude files over a specific size, you can use the following Deep Security Manager command:

```
dsm_c -action changesetting -name
com.trendmicro.ds.antimalware:settings.configuration.maxSelfExtractRTScanSiz
eMB -value 512
```

In this example, the file-size limitation is set to 512 MB for loading target files. The scan engine does not add files larger than the set value to memory and instead scans them directly. Note that in order to deploy this setting, you need to send the policy to your target Deep Security Agent after running the command in Deep Security Manager.

## Test file exclusions

Before continuing with further Anti-Malware configuration steps, test file exclusions to ensure they are working correctly:

1. Make sure the real-time scan is enabled and a configuration is selected.
2. Go to **Policies > Common Objects > Other > Malware Scan Configurations**.
3. Click **New > New Real-time Scan Configuration**.
4. Go to the **Exclusions** tab, and select **New** from the directory list.
5. Name the directory list.
6. Under **Directorys** specify the path of the directory you want to exclude from the scan. For example, `c:\Test Folder\`.
7. Click **OK** .
8. Go to the **General** tab, name the manual scan, and click **OK**.
9. Go to the EICAR site and download their anti-malware test file. Save the file in the folder specified in the previous step. The file should be saved and undetected by the Anti-Malware module.

# Syntax for directory lists

Directory list items accept either forward slash or backslash to support both Windows and Linux conventions.

| Exclusion | Format | Description | Examples |
|---|---|---|---|
| Directory | DIRECTORY\ | Excludes all files in the specified directory and all files in all subdirectories. | ***C:\Program Files\***<br>Excludes all files in the `Program Files` directory and all subdirectories. |
| Directory with wildcard (*) | DIRECTORY*\ | Excludes all subdirectories except for the specified subdirectory and the files that it contains. | ***C:\abc\*\\***<br>Excludes all files in all subdirectories of `abc` but does not exclude the files in the `abc` directory.<br><br>***C:\abc\wx*z\***<br>*Matches:* |

| Exclusion | Format | Description | Examples |
|---|---|---|---|
| | | | C:\abc\wxz\<br>C:\abc\wx123z\<br>*Does not match:*<br>C:\abc\wxz<br>C:\abc\wx123z<br><br>***C:\abc\*wx\***<br>*Matches:*<br>C:\abc\wx\<br>C:\abc\123wx\<br>*Does not match:*<br>C:\abc\wx<br>C:\abc\123wx |
| Directory with wildcard (*) | DIRECTORY*\ | Excludes any subdirectories with a matching name, but does not exclude the files in that directory and any subdirectories. | ***C:\Program Files\SubDirName*\***<br>Excludes any subdirectories with a folder name that begins with `SubDirName`. Does not exclude all files under `C:\Program Files\` or any other subdirectories. |
| Environment variable | ${ENV VAR} | Excludes all files and subdirectories defined by an environment variable with the format ${ENV VAR}. Windows common environment variables, such as `windir`, `programfiles`, and so on, are supported.<br>For a Virtual Appliance and Linux, the value pairs for the environment variable must be defined in **Policy or Computer Editor > Settings > General > Environment Variable Overrides.** | ***${windir}***<br>If the variable resolves to `c:\windows`, excludes all the files in `c:\windows` and all its subdirectories. |
| Comments | DIRECTORY #Comment | Adds a comment to your exclusion definitions. | `c:\abc #Exclude the abc directory` |

## Syntax of file lists

| Exclusion | Format | Description | Example |
|---|---|---|---|
| File | FILE | Excludes all files with the specified file name regardless of its location or directory. | ***abc.doc***<br>Excludes all files named `abc.doc` in all directories. Does not exclude `abc.exe`. |
| File path | FILEPATH | Excludes the single file specified by the file path. | ***C:\Documents\abc.doc***<br>Excludes only the file named `abc.doc` in the `Documents` directory. |
| File path with wildcard (*) | FILEPATH | Excludes all the files specified by the file path. | `C:\Documents\abc.co*` (For Windows Agent platforms only) Excludes any file that has file name of `abc` and extension beginning with `.co` in the `Documents` directory. |
| Filename is a wildcard (*) | FILEPATH* | Excludes all files under the path, but does not include the files in unspecified subdirectories | ***C:\Documents\****<br>Excludes all files under the directory `C:\Documents\`<br>***C:\Documents\SubDirName*****<br>Excludes all files within subdirectories with a folder name that begins with `SubDirName`. Does not exclude all files under `C:\Documents\` or any other subdirectories.<br>***C:\Documents\*****<br>Excludes all files within all direct subdirectories under `C:\Documents`. Does not exclude files in subsequent subdirectories. |
| File with wildcard (*) | FILE* | Excludes all files with a matching pattern in the file name. | ***abc*.exe***<br>Excludes any file that has prefix of `abc` and extension of `.exe`.<br>****.db***<br>*Matches:*<br>123.db<br>abc.db<br>*Does not match:* |

| Exclusion | Format | Description | Example |
|---|---|---|---|
| | | | 123db<br>123.abd<br>cbc.dba<br><br>****db***<br>*Matches:*<br>123.db<br>123db<br>ac.db<br>acdb<br>db<br>*Does not match:*<br>db123<br><br>***wxy*.db***<br>*Matches:*<br>wxy.db<br>wxy123.db<br>*Does not match:*<br>wxydb |
| File with wildcard (*) | FILE.EXT* | Excludes all files with a matching pattern in the file extension. | ***abc.v****<br>Excludes any file that has file name of `abc` and extension beginning with `.v`.<br><br>***abc.*pp***<br>*Matches:*<br>abc.pp<br>abc.app<br>*Does not match:*<br>wxy.app<br><br>***abc.a*p***<br>*Matches:*<br>abc.ap<br>abc.a123p<br>*Does not match:*<br>abc.pp<br><br>***abc.****<br>*Matches:*<br>abc.123<br>abc.xyz<br>*Does not match:*<br>wxy.123 |
| File with wildcard (*) | FILE*.EXT* | Excludes all files with a matching pattern in the file name and in the | ***a*c.a*p***<br>*Matches:* |

| Exclusion | Format | Description | Example |
|---|---|---|---|
| | | extension. | ac.ap<br>a123c.ap<br>ac.a456p<br>a123c.a456p<br>*Does not match:*<br>ad.aa |
| Environment variable | ${ENV VAR} | Excludes files specified by an environment variable with the format ${ENV VAR}. Windows common environment variables, such as `windir`, `programfiles`, and so on, are supported.<br>For a Virtual Appliance and Linux, the value pairs for the environment variable must be defined in **Policy or Computer Editor > Settings > General > Environment Variable Overrides.** | ***${myDBFile}***<br>Excludes the file `myDBFile`. |
| Comments | FILEPATH #Comment | Adds a comment to your exclusion definitions. | `C:\Documents\abc.doc #This is a comment` |

## Syntax of file extension lists

| Exclusion | Format | Description | Example |
|---|---|---|---|
| File Extension | EXT | Matches all files with a matching file extension. | **doc**<br>Matches all files with a `.doc` extension in all directories. |
| Comments | EXT #Comment | Adds a comment to your exclusion definitions. | `doc #This a comment` |

## Syntax of process image file lists

| Exclusion | Format | Description | Example |
|---|---|---|---|
| File path | C:\DIR\FILE.EXT | Excludes the process image file specified by the file path. | **C:\abc\file.exe**<br>Excludes only the file named `file.exe` in the `abc` directory. |
| Directories with wildcard (*) | C:\DIR*\FILE.EXT | Wildcard replaces the directory name. | **C:\abc*\file.exe**<br>Matches:<br>`C:\abc\file.exe`<br>`C:\abc1\file.exe` |

| Exclusion | Format | Description | Example |
|---|---|---|---|
| | | | `C:\abc1\abc2\file.exe`<br>**C:\abc*\*\file.exe**<br>Matches:<br>`C:\abc1\abc2\file.exe`<br>Does not match:<br>`C:\abc\file.exe`<br>`C:\abc1\file.exe` |
| File names with wildcard (*) | C:\DIR\FILE*.EXT<br>C:\DIR\FILE.EXT*<br>C:\DIR\FILE*.EXT* | Wildcard replaces file names. | **C:\abc\file*.exe**<br>Matches:<br>`C:\abc\file.exe`<br>`C:\abc\file123.exe`<br>Does not match:<br>`C:\abc\file.exe123`<br>`C:\abc\file123.exe123`<br>**C:\abc\file.exe***<br>Matches:<br>`C:\abc\file.exe`<br>`C:\abc\file.exe123`<br>Does not match:<br>`C:\abc\file123.exe`<br>`C:\abc\file123.exe123`<br>**C:\abc\file*.exe***<br>Matches:<br>`C:\abc\file.exe`<br>`C:\abc\file.exe123`<br>`C:\abc\file123.exe`<br>`C:\abc\file123.exe123` |
| Drive name with wildcard ( * ) | *:\DIR\FILE.EXT | Wildcard replaces the drive name. | ***:\abc\file.exe**<br>Matches:<br>`C:\abc\file.exe` |
| Special character with wildcard ( * ) | C:\DIR\FILE*EXT<br>C:\DIR\DIR2*FILE.EXT | Wildcard replaces special characters, such as colon ( `:` ), back slash ( `\` ), forward slash ( `/` ), period ( `.` ), and so on. | **C:\abc\file*exe**<br>Matches:<br>`C:\abc\file.exe`<br>Does not match:<br>`C:\abc\abc2\file.exe`<br>`C:\abc\abc2\abc3\file.exe`<br>**C:\abc\abc2*file.exe**<br>Matches:<br>`C:\abc\abc2\file.exe` |

| Exclusion | Format | Description | Example |
|---|---|---|---|
| | | | `C:\abc\abc2\abc3\file.exe`<br>Does not match:<br>`C:\abc\file.exe` |

## Scan a network directory (real-time scan only)

If you want to scan files and folders in network shares and mapped network drives that reside in a Network File System (NFS), Server Message Block (SMB) or Common Internet File System (CIFS), select **Enable Network Directory Scan**. This option is available only for real-time scans.

Resources accessed in "`~/.gvfs`" via GVFS, a virtual file system available for the GNOME desktop, are treated as local resources, as opposed to network drives.

If a virus is detected when scanning a network folder on Windows, the agent may display some clean failed (delete failed) events.

### Specify when real-time scans occur

Choose between scanning files when they are opened for reading, when they are written to, or both.

1. Open the properties of the malware scan configuration.
2. On the **Advanced** tab, select one of the options for the **Real-Time Scan** property.
3. Click **OK**.

### Configure malware handling

Configure how Deep Security behaves when malware is detected:

- "Customize malware remedial actions" below
- "Generate alerts for malware detection" on page 762

## Customize malware remedial actions

When Deep Security detects malware, it performs a remedial action to handle the file. There are five possible actions that Deep Security can take when it encounters malware:

- Pass: Allows full access to the infected file without doing anything to the file. An Anti-Malware Event is still recorded. The remedial action **Pass** should never be used for a possible virus.

- Clean: Cleans an infected file before allowing full access to it. If the file cannot be cleaned, it is quarantined.
- Delete: On Linux, the infected file is deleted without a backup. On Windows, the infected file is backed up and then deleted. Windows backup files can be viewed and restored in **Events & Reports > Events > Anti-Malware Events > Identified Files**.
- Deny Access: This scan action can only be performed during real-time scans. When Deep Security detects an attempt to open or execute an infected file, it immediately blocks the operation. The infected file is left unchanged. When the Access Denied action is triggered, the infected files stay in their original location. Do not use the remedial action **Deny Access** when **Real-Time Scan** is set to **During Write**. When **During Write** is selected, files are scanned when they are written and the action **Deny Access** has no effect.
- Quarantine: Moves the infected file to the quarantine directory on the computer or Virtual Appliance. The quarantined file can be viewed and restored in **Events & Reports > Events > Anti-Malware Events > Identified Files**.

  Malware marked as **Quarantined** on Linux might be marked as **Deleted** on Windows, despite the malware being identical on both operating systems. In either case, the file can be viewed and restored in **Events & Reports > Events > Anti-Malware Events > Identified Files**.

  On Windows, infected non-compressed files (for example, .txt files) are quarantined, while infected compressed files (for example, .zip files) are deleted. On Windows, both quarantined or deleted files have a backup that can be viewed and restored in **Events & Reports > Events > Anti-Malware Events > Identified Files**. On Linux, all infected files (compressed or non-compressed) are quarantined, and can be viewed and restored in **Events & Reports > Events > Anti-Malware Events > Identified Files**.

The default remediation actions in the malware scan configurations are appropriate for most circumstances. However, you can customize the actions to take when Deep Security detects malware. You can either use the action that ActiveAction determines, or specify the action for each type of vulnerability.

ActiveAction is a predefined group of cleanup actions that are optimized for each malware category. Trend Micro continually adjusts the actions in ActiveAction to ensure that individual detections are handled properly. See "ActiveAction actions" on the next page.

1. Open the properties of the malware scan configuration.
2. On the **Advanced** tab, for **Remediation Actions** select Custom.

3. Specify the action to take:
   a. To let ActiveAction decide which action to take, select **Use action recommended by ActiveAction**.
   b. To specify an action for each type of vulnerability, select **Use custom actions**, and then select the actions to use.
4. Specify the action to take for Possible Malware.
5. Click **OK**.

## ActiveAction actions

The following table lists the actions that ActiveAction takes:

| Malware Type | Action |
|---|---|
| "Virus" on page 739 | Clean. If a virus cannot be cleaned, it is deleted (Windows) or quarantined (Linux or Solaris). There is an exception to this behavior: On a Linux or Solaris agent, if a virus of type Test Virus is found, access is denied to the infected file. |
| "Trojans" on page 740 | Quarantine |
| "Packer" on page 740 | Quarantine |
| "Spyware/grayware" on page 740 | Quarantine |
| "Cookie" on page 741 | Delete<br>Does not apply to real-time scans |
| "Other threats" on page 742 | Clean<br>If a threat cannot be cleaned, it is handled as follows:<br>• on Windows, the infected file is deleted but can be viewed and restored, if needed<br>• on Linux or Solaris, access is denied to the infected file<br>Also, on a Linux or Solaris agent, if a virus of type 'Joke' is found, it is quarantined immediately. No attempt is made to clean it. |
| "Possible malware" on page 742 | ActiveAction |

When the agent downloads virus pattern updates from an ActiveUpdate server or relay, it may change its ActiveAction scan actions.

# Generate alerts for malware detection

When Deep Security detects malware, you can generate an alert:

1. Open the properties of the malware scan configuration.
2. On the **General** tab, for **Alert** select **Alert when this Malware Scan Configuration logs an event**.
3. Click **OK**.

### Identify malware files by file hash digest

Deep Security can calculate the hash value of a malware file and display it on the **Events & Reports > Events > Anti-Malware Events** page. Because a particular piece of malware can go by several different names, the hash value is useful because it uniquely identifies the malware. You can use the hash value when looking up information about the malware from other sources.

1. Open the policy or computer editor that you want to configure.
2. Click **Anti-Malware > Advanced**.
3. Under **File Hash Calculation**, clear the **Default** or **Inherited** check box. **Default** is displayed for a root policy and **Inherited** is displayed for child policies.

   When **Inherited** is selected, the file hash settings are inherited from the current policy's parent policy.

   When **Default** is selected, Deep Security does not calculate any hash values.
4. Select the **Calculate hash values of all anti-malware events**.
5. By default, Deep Security will produce SHA-1 hash values. If you want to produce additional hash values, you can select one or both of **MD5** and **SHA256**.
6. You can also change the maximum size of malware files that will have hash values calculated. The default is to skip files that are larger than 128MB, but you can change the value to anything between 64 and 512 MB.

### Configure notifications on the computer

On Windows-based agents, you might occasionally see onscreen notification messages alerting you of Deep Security actions you must take that are related to the anti-malware and web reputation modules. For example, you might see the message, `A reboot is required for Anti-Malware cleanup task`. You must click **OK** on the dialog box to dismiss it.

If you do not want these notifications to appear:

1. Go to the **Computer or Policy editor**[1].
2. Click **Settings** on the left.
3. Under the **General** tab, scroll to the **Notifications** section.
4. Set **Suppress all pop-up notifications on host** to **Yes**. The messages still appear as alerts or events in Deep Security Manager. For more information about the notifier, see "Deep Security notifier" on page 1405.

## Improve Anti-Malware performance

To improve utilization of system resources by Deep Security Agent, you can optimize performance-related settings according to best practices.

See also:

- "Configure advanced exploit exceptions" on page 787
- "Identify malware files by file hash digest" on the previous page

### Minimize disk usage

Reserve an appropriate amount of disk space for storing identified malware files. The space that you reserve applies globally to all computers: physical machines, virtual machines, and Deep Security Virtual Appliances. The setting can be overridden at the policy level and at the computer level.

1. Open the policy or computer editor that you want to configure.
2. Click **Anti-Malware > Advanced**.
3. Under **Identified Files**, clear **Default**.
4. In the **Maximum disk space used to store identified files** field, specify the disk space to use.
5. Click **Save**.

Alerts are raised when there is not enough disk space to store an identified file.

### Optimize CPU usage

- Exclude files from real-time scans if they are usually safe, but have high I/O, such as databases, Microsoft Exchange quarantines, and network shares (on Windows, you can

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

use procmon to find files with high I/O). See "Exclusions" on page 751.

- Do not scan network directories. See "Scan a network directory (real-time scan only)" on page 759.
- Do not use Smart Scan if the computer does not have reliable network connectivity to the Trend Micro Smart Protection Network or your Smart Protection Server. See "Smart Protection in Deep Security" on page 777.
- Reduce the CPU impact of malware scans by setting **CPU Usage** to **Medium** (recommended; pauses between scanning files) or **Low** (pauses between scanning files for a longer interval than the medium setting):
  a. Open the properties of the malware scan configuration.
  b. On the **Advanced** tab, select the **CPU Usage** during which scans run.
  c. Click **OK**.
- Create a scheduled task to run scans at a time when CPU resources are more readily available. See "Schedule Deep Security to perform tasks" on page 1600.
- Reduce or keep small default values for the maximum file size to scan, maximum levels of compression from which to extract files, maximum size of individual extracted files, maximum number of files to extract, and OLE Layers to scan. See "Scan for specific types of malware" on page 747.

  > **Warning:** Most malware is small, and nested compression indicates malware. But if you do not scan large files, there is a risk that anti-malware does not detect some malware. You can mitigate this risk by using other features, such as integrity monitoring. See "Set up Integrity Monitoring" on page 901

## Enable multi-threaded processing

You can enable multi-threaded processing for manual and scheduled scans. Real-time scans use multi-threaded processing by default. Multi-threaded processing is effective only on systems that support this capability. To apply the setting, enable it and then restart the computer.

Do not enable multi-threaded processing if resources are limited (for example, CPU-bound tasks) or if resources have to be held by only one operator at a time (for example, IO-bound tasks).

Enabling multi-threaded processing may impact CPU usage in the following ways:

- It may reduce the number of CPU cores available to the computer's other processes.
- On Linux, when **Resource Allocation for Malware Scans** is enabled, the CPU usage setting is ignored even if set to **Medium** or **Low**.

To enable multi-threaded processing:

1. Select **Policies**.
2. Double-click to open the policy where you want to enable multi-threaded processing.
3. Go to **Anti-Malware > Advanced**.
4. In the **Resource Allocation for Malware Scans** section, select **Yes** for **Use multithreaded processing for Malware scans**, and then click **Save**.

   On Linux, this setting takes effect without requiring a restart. On platforms other than Linux, a restart is required.

5. If you are using a non-Linux platform, restart the solution platform service by doing one of the following:
   - In the `services.msc` window, select the Trend Micro Solution Platform service and click **Restart**.
   - In the command prompt, enter the following commands:

     ```
     sc stop amsp
     ```

     ```
     sc start amsp
     ```

   - Restart the computers on which you enabled multi-threaded processing for the setting to take effect.

#### Optimize RAM usage

- Reduce or keep small default values for the maximum file size to scan, maximum levels of compression from which to extract files, maximum size of individual extracted files, maximum number of files to extract, and OLE Layers to scan. See "Scan for specific types of malware" on page 747.

  > **Warning:** Most malware is small, and nested compression indicates malware. But if you do not scan large files, there is a risk that anti-malware does not detect some malware. You can mitigate this risk by using other features, such as integrity monitoring. See "Set up Integrity Monitoring" on page 901

## Coexistence of Deep Security Agent with Microsoft Defender Antivirus

Microsoft Defender Antivirus is automatically installed on Microsoft Windows Server 2016 and later, as well as Windows 10 and later. Deep Security Agent (DSA) can coexist with Microsoft Defender Antivirus in its passive mode, for all operating system levels protected by Trend Micro Deep Security. The following are compatible versions of Microsoft Defender Antivirus, Windows Server and desktop, as well as of DSA:

- Microsoft Defender Antivirus product and engine versions:
  - AMProductVersion: 4.18.2202.4
  - AMEngineVersion: 1.1.18900.3
- Windows Server and desktop versions:
  - Windows Server 2016 or later
  - Windows 10 x64 RS5 or later
- Deep Security Agent:
  - Deep Security Agent 20.0.0-4416 (20 LTS Update 2022-04-28) or later

When you install Deep Security with anti-malware enabled on a Windows 10 or Windows 11 desktop, Microsoft Defender Antivirus is automatically set to passive mode. On a Windows Server, you need to re-enable the Anti-Malware policy to let Microsoft Defender Antivirus enter passive mode.

The following table summarizes these events.

| Platform | Action | Description |
|---|---|---|
| Windows 10 and 11 Desktop | Deep Security with Anti-Malware enabled | Windows automatically sets Microsoft Defender Antivirus to passive mode after Deep Security Agent Anti-Malware is enabled. |
| Windows Server 2016 and later | Re-enable Anti-Malware policy | Deep Security Agent automatically configures Microsoft Defender Antivirus to passive mode. |

If you disable the DSA anti-malware, either by deactivating or uninstalling it, you remove both the DisableAntiSpyware and ForceDefenderPassiveMode registry in Microsoft Defender Antivirus:

- The DisableAntiSpyware registry key specifies whether or not to disable Microsoft Defender Antivirus. By removing DisableAntiSpyware, you remove the disable key and enable

Microsoft Defender Antivirus. You may have to manually enable Microsoft Defender Antivirus to ensure it is in active mode.

- The ForceDefenderPassiveMode registry key sets Microsoft Defender Antivirus to passive mode. By removing the key, Microsoft Defender Antivirus is set to active mode.

When you enable Deep Security Agent anti-malware on a Windows Server, the Windows Security virus and threat protection service may display a message "No active antivirus provider. Your device is vulnerable". Trend Micro tested this case and confirmed that such a message appears when Microsoft Defender Antivirus is disabled. This is a Windows Server behavior (as opposed to Deep Security).

There is a confirmed performance impact when both Microsoft Defender Antivirus and Deep Security Agent Anti-Malware are enabled, therefore it is recommended to have Microsoft Defender Antivirus in passive mode. The fallback approach is to have exclusion lists when passive mode is not possible, with the understanding that exclusion lists can mitigate but may not completely eliminate the impact on performance.

### Microsoft Defender Antivirus application files for exclusion list for DSA

If Microsoft Defender Antivirus cannot switch to passive mode, you must add Microsoft Defender Antivirus for Endpoint to the exclusion list for Deep Security Agent to mitigate the impact on performance. For more information, see Make the switch from non-Microsoft endpoint protection to Microsoft Defender Antivirus for Endpoint.

The following are locations of Microsoft Defender Antivirus executable files:

- `%Program Files%\Windows Defender\`
- `%ProgramData%\Microsoft\Windows Defender\Platform\4.18.2201.10-0*\`

### DSA folders and processes for Microsoft Defender Antivirus exclusion list

You need to add Deep Security agent folders and processes to your Microsoft Defender Antivirus exclusion list.

Folder:

- `C:\Program Files\Trend Micro\AMSP`
- `C:\Program Files\Trend Micro\Deep Security Agent`

Process:

- `C:\Program Files\Trend Micro\AMSP\coreServiceShell.exe`
- `C:\Program Files\Trend Micro\AMSP\coreFrameworkHost.exe`
- `C:\Program Files\Trend Micro\Deep Security Agent\dsa.exe`
- `C:\Program Files\Trend Micro\Deep Security Agent\Notifier.exe`

#### Tamper protection

Activating tamper protection of Microsoft Defender Antivirus safeguards against diverting this particular antivirus to passive mode. If multiple antivirus products have been deployed, it would be reasonable to retain only one antimalware component of one antivirus product.

For details on the supported environments, see Microsoft Defender Antivirus compatibility with other security products.

#### Microsoft Defender Antivirus Endpoint Detection and Response (EDR) in block mode for endpoint

Do not enable Microsoft Defender Antivirus' EDR in block mode for endpoint. This recommendation is based on the results of testing that discovered compatibility issues when EDR in block mode is enabled.

## Detect emerging threats using Predictive Machine Learning

> **Note:** Predictive Machine Learning is supported with Deep Security Agent 11.0 +. For details on which platforms support this feature, see "Supported features by platform" on page 425.

Use Predictive Machine Learning to detect unknown or low-prevalence malware. (For more information, see "Predictive Machine Learning" on page 739.)

Predictive Machine Learning uses the Advanced Threat Scan Engine (ATSE) to extract file features and sends the report to the Predictive Machine Learning engine on the Trend Micro Smart Protection Network. To enable Predictive Machine Learning, perform the following:

1. "Ensure Internet connectivity" on the next page
2. "Enable Predictive Machine Learning" on the next page

As with all detected malware, Predictive Machine Learning logs an event when it detects malware. (See "About Deep Security event logging" on page 1046.) You can also create an exception for any false positives. (See "Configure advanced exploit exceptions" on page 787.)

## Ensure Internet connectivity

Predictive Machine Learning requires access to the Global Census Service, Good File Reputation Service, and Predictive Machine Learning Service. These services are hosted in the Trend Micro Smart Protection Network. If your Deep Security Agents or Virtual Appliance cannot access the Internet directly, see "Configure agents that have no internet access" on page 1379 for workarounds.

## Enable Predictive Machine Learning

Predictive Machine Learning is configured as part of a real-time scan configuration that is applied to a policy or individual computer. (See "Configure malware scans and exclusions" on page 745.) After you configure the scan configuration, apply it to a policy or computer.

> **Note:** Predictive Machine Learning protects only the files and directories that real-time scan is configured to scan. See "Specify the files to scan" on page 750.

These settings can only be applied to real-time scan configurations.

1. Go to **Policies > Common Objects > Other > Malware Scan Configurations**.
2. Select the real-time scan configuration to configure and click **Details**.

   You can also create a new real-time scan configuration if desired.

3. On the **General** tab, under **Predictive Machine Learning**, select **Enable Predictive Machine Learning**. In the **Action to take** list, choose the remediation action that you want Deep Security to take when it detects malware:
   - **Quarantine (recommended):** Moves the infected file to the quarantine directory on the protected computer. The quarantined file can be viewed and restored in **Events & Reports > Events > Anti-Malware Events > Identified Files**.
   - **Pass:** Allows full access to the infected file without doing anything to the file. (An Anti-Malware Event is still recorded.)
   - **Delete:** On Linux, the infected file is deleted without a backup. On Windows, the infected file is backed up and then deleted. Windows backup files can be viewed and restored in **Events & Reports > Events > Anti-Malware Events > Identified Files**.
4. Click **OK**.
5. Open the policy or computer editor to which you want to apply the scan configuration and go to **Anti-Malware > General**.
6. Ensure that **Anti-Malware State** is **On** or **Inherited (On)**.

7. In the **Real-Time Scan** section, select the malware scan configuration.
8. Click **Save**.

## Enhanced anti-malware and ransomware scanning with behavior monitoring

Deep Security provides security settings that you can apply to Windows and Linux machines protected by a Deep Security Agent to enhance your malware and ransomware detection and clean rate. These settings enable you to go beyond malware pattern matching and identify suspicious files that could potentially contain emerging malware that has not yet been added to the anti-malware patterns (known as a zero-day attack).

On this page:

- "Enhanced scanning protection" below
- "Enable enhanced scanning" on the next page
- "Address problems found by enhanced scanning" on page 772
- "What if my agents cannot connect to the Internet directly?" on page 777

For an overview of the anti-malware module, see "About Anti-Malware" on page 735.

### Enhanced scanning protection

**Threat detection**: To avoid detection, some types of malware attempt to modify system files or files related to known installed software. These types of changes often go unnoticed because the malware takes the place of legitimate files. Deep Security can monitor system files and installed software for unauthorized changes to detect and prevent these changes from occurring.

**Anti-exploit**: Malware creators can use malicious code to hook in to user mode processes in order to gain privileged access to trusted processes and to hide the malicious activity. Malware creators inject code into user processes through DLL injection, which calls an API with escalated privilege. They can also trigger an attack on a software exploit by feeding a malicious payload to trigger code execution in memory. In Deep Security, the anti-exploit functionality monitors for processes that may be performing actions that are not typically performed by a given process. Using a number of mechanisms, including Data Execution Prevention (DEP), Structured Exception Handling Overwrite Protection (SEHOP), and heap spray prevention, Deep Security can determine whether a process has been compromised and then terminate the process to prevent further infection.

**Extended ransomware protection**: Ransomware has become more sophisticated and targeted. Most organizations have a security policy that includes anti-malware protection on their endpoints, which offers a level of protection against known ransomware variants. However, it may not be sufficient to detect and prevent an outbreak for new variants. The ransomware protection offered by Deep Security can protect documents against unauthorized encryption or modification. Deep Security has also incorporated a data recovery engine that can optionally create copies of files being encrypted to offer users an added chance of recovering files that may have been encrypted by a ransomware process.

## Enable enhanced scanning

Enhanced scanning is configured as part of the anti-malware settings applied to a policy or individual computer. For information on configuring anti-malware protection, see "Enable and configure Anti-Malware" on page 742.

These settings can only be applied to Windows and Linux machines that are protected by a Deep Security Agent.

> **Note:** Enhanced scanning may have a performance impact on agent computers running applications with heavy loads. Review "Improve Anti-Malware performance" on page 763 before deploying Deep Security Agents with enhanced scanning enabled.

The first step is to enable enhanced scanning in a real-time malware scan configuration:

1. In Deep Security Manager, go to **Policies > Common Objects > Other > Malware Scan Configurations**.
2. Double-click an existing real-time scan configuration to edit it. For details on malware scan configurations, see "Configure malware scans and exclusions" on page 745.
3. On the **General** tab, under **Behavior Monitoring**, select **Enable Behavior Monitoring**.
4. Use **Action to take** to select the remediation action that you want Deep Security to take when it detects malware:
   - **ActiveAction (recommended)**: Use the action that ActiveAction determines. ActiveAction is a predefined group of cleanup actions that are optimized for each malware category. Trend Micro continually adjusts the actions in ActiveAction to ensure that individual detections are handled properly. For more information, see "ActiveAction actions" on page 761.
   - **Pass**: Allow full access to the infected file without doing anything to the file. An Anti-Malware Event is still recorded.

5. Optionally, select **Back up and restore ransomware-encrypted files**. When this option is selected, Deep Security creates backup copies of files that are being encrypted, in case they are being encrypted by a ransomware process. This option applies only to computers running Windows.
6. Click **OK**.

By default, real-time scans are set to scan all directories. If you change the scan settings to scan a directory list, the enhanced scanning may not work as expected. For example, if you set **Directories to scan** to scan Folder1 and ransomware occurs in Folder1, it may not be detected if the encryption associated with the ransomware happens to files outside of Folder1.

Next, apply the malware scan configuration to a policy or an individual computer:

1. In the **Computer or Policy editor**[1], go to **Anti-Malware > General**.
2. Ensure that **Anti-Malware State** is set to **On** or **Inherited (On)**.
3. The **General** tab contains sections for **Real-Time Scan**, **Manual Scan**, and **Scheduled Scan**. In the appropriate sections, use **Malware Scan Configuration** to select the scan configuration that you created.
4. Click **Save**.

## Address problems found by enhanced scanning

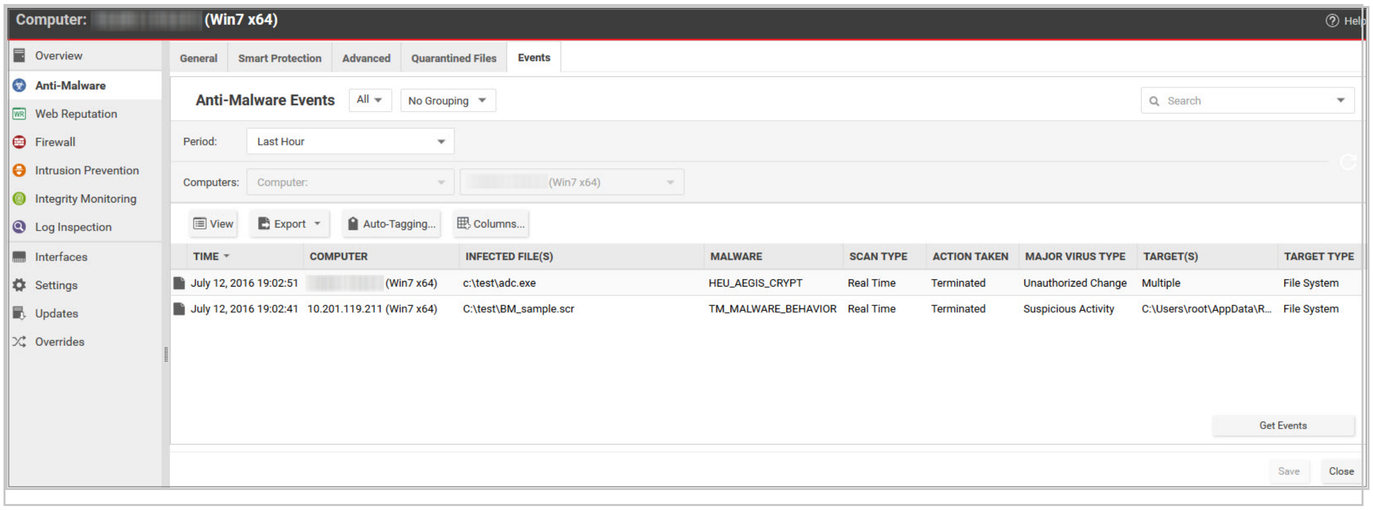
When Deep Security discovers activity or files that match the enhanced scan settings you have enabled, it logs an event that you can view by navigating to **Events & Reports > Events > Anti-Malware Events** to see a list of events. The event is identified as Suspicious activity or Unauthorized change in the **Major Virus Type** column, with details displayed in the **Target(s)** and **TargetType** columns.

Deep Security performs many types of checks related to the enhanced scan settings, and the actions that it takes depend on the type of check that finds an issue. Deep Security may Deny Access, Terminate, or Clean a suspicious object. These actions are determined by Deep Security and are not configurable, with the exception of the Clean action:

- **Deny Access**: When Deep Security detects an attempt to open or execute a suspicious file, it immediately blocks the operation and records an anti-malware event.
- **Terminate**: Deep Security terminates the process that performed the suspicious operation and records an anti-malware event.

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

- **Clean**: Deep Security checks the Malware Scan Configuration and performs the action specified for Trojans on the **Actions** tab. One or more additional events will be generated relating to the action performed on the Trojan files.



Computer: [redacted] (Win7 x64)

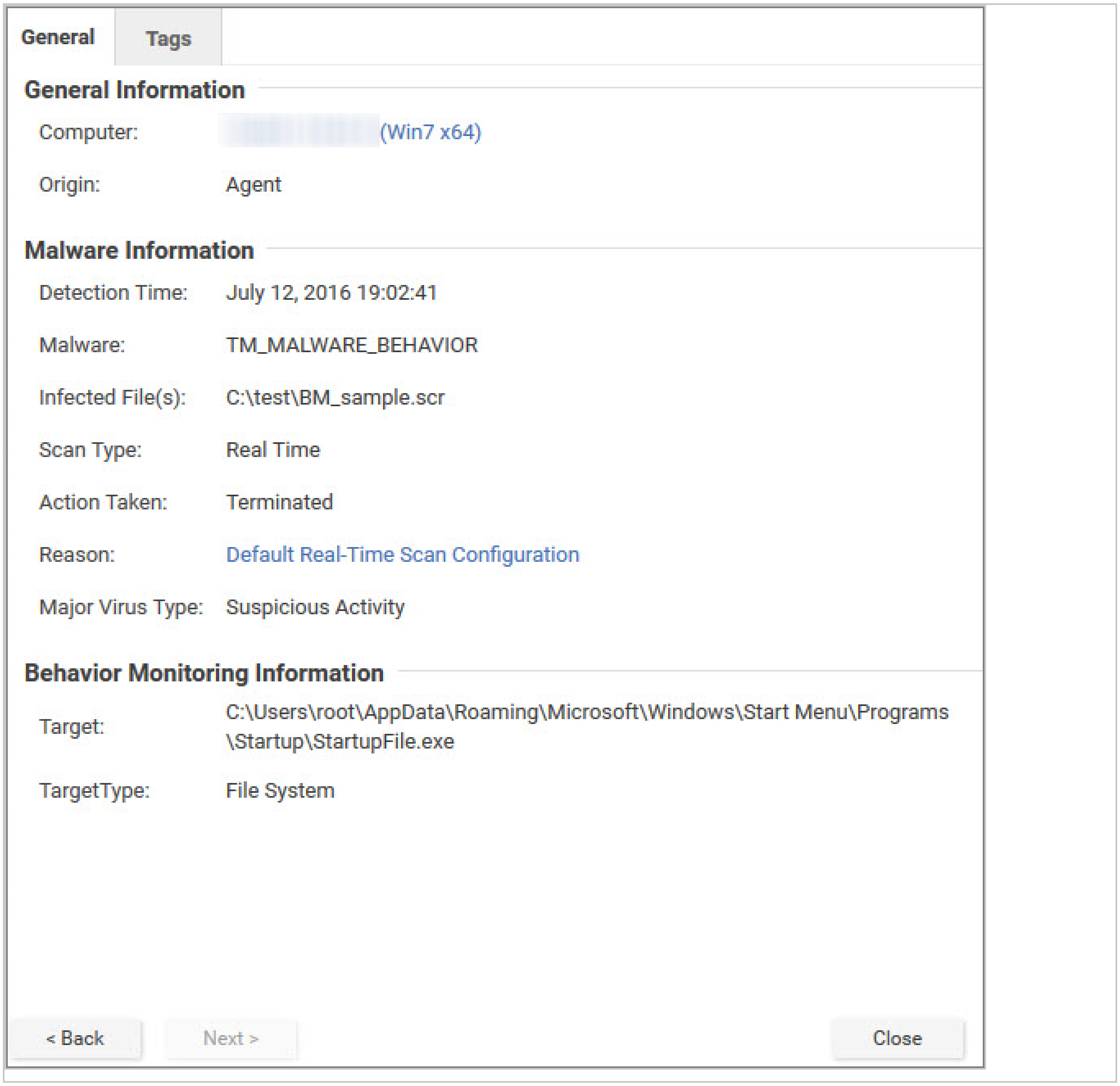
Anti-Malware Events

Period: Last Hour

Computers: Computer: [redacted] (Win7 x64)

| TIME | COMPUTER | INFECTED FILE(S) | MALWARE | SCAN TYPE | ACTION TAKEN | MAJOR VIRUS TYPE | TARGET(S) | TARGET TYPE |
|---|---|---|---|---|---|---|---|---|
| July 12, 2016 19:02:51 | [redacted] (Win7 x64) | c:\test\adc.exe | HEU_AEGIS_CRYPT | Real Time | Terminated | Unauthorized Change | Multiple | File System |
| July 12, 2016 19:02:41 | 10.201.119.211 (Win7 x64) | C:\test\BM_sample.scr | TM_MALWARE_BEHAVIOR | Real Time | Terminated | Suspicious Activity | C:\Users\root\AppData\R... | File System |

Double-click an event to see details:



**General Information**

Computer: [redacted] (Win7 x64)

Origin: Agent

**Malware Information**

Detection Time: July 12, 2016 19:02:41

Malware: TM_MALWARE_BEHAVIOR

Infected File(s): C:\test\BM_sample.scr

Scan Type: Real Time

Action Taken: Terminated

Reason: Default Real-Time Scan Configuration

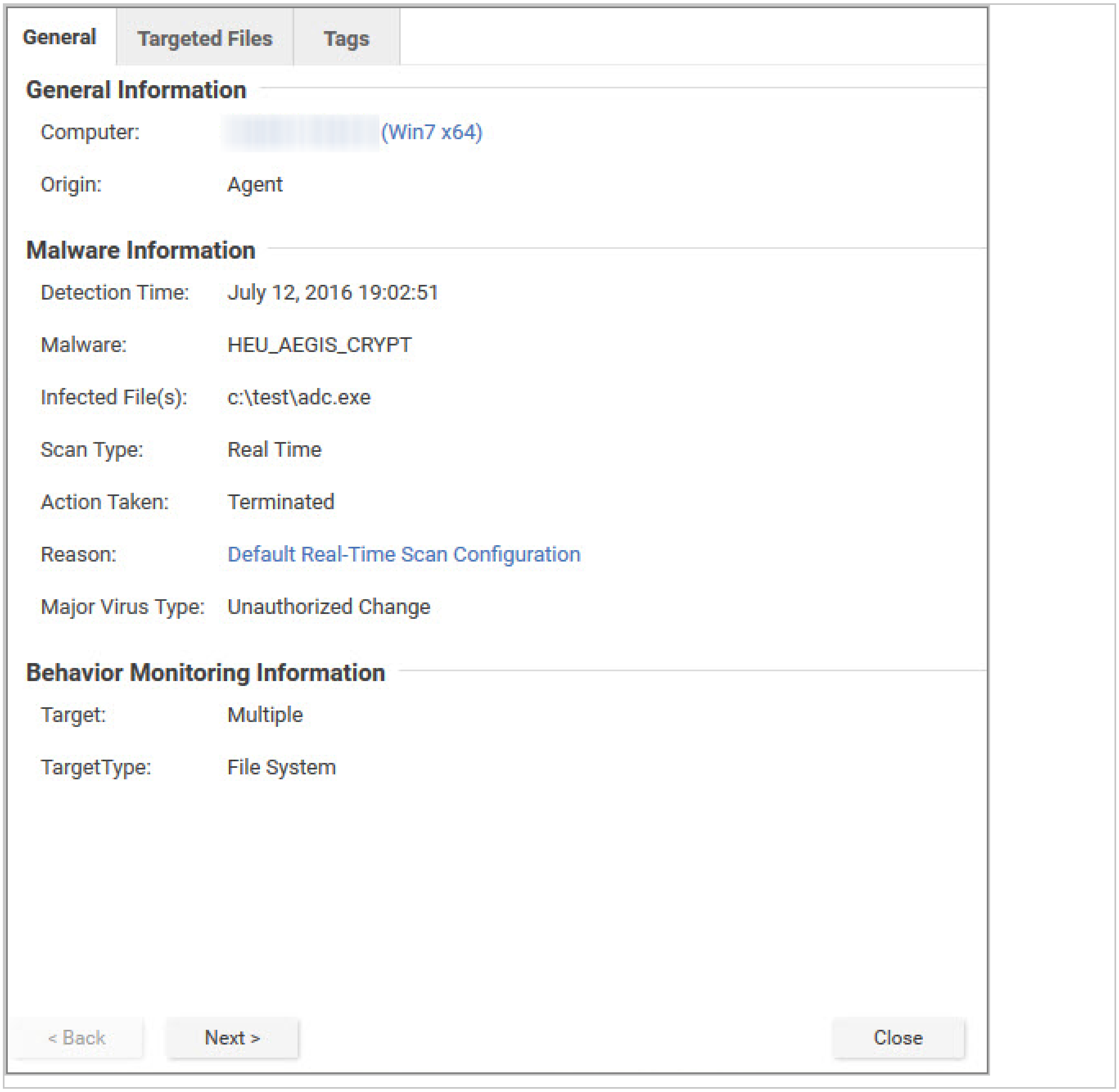
Major Virus Type: Suspicious Activity

**Behavior Monitoring Information**

Target: C:\Users\root\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\StartupFile.exe

TargetType: File System

Events related to ransomware have an additional **Targeted Files** tab:



General Information

Computer: [redacted] (Win7 x64)

Origin: Agent

Malware Information

Detection Time: July 12, 2016 19:02:51

Malware: HEU_AEGIS_CRYPT

Infected File(s): c:\test\adc.exe

Scan Type: Real Time

Action Taken: Terminated

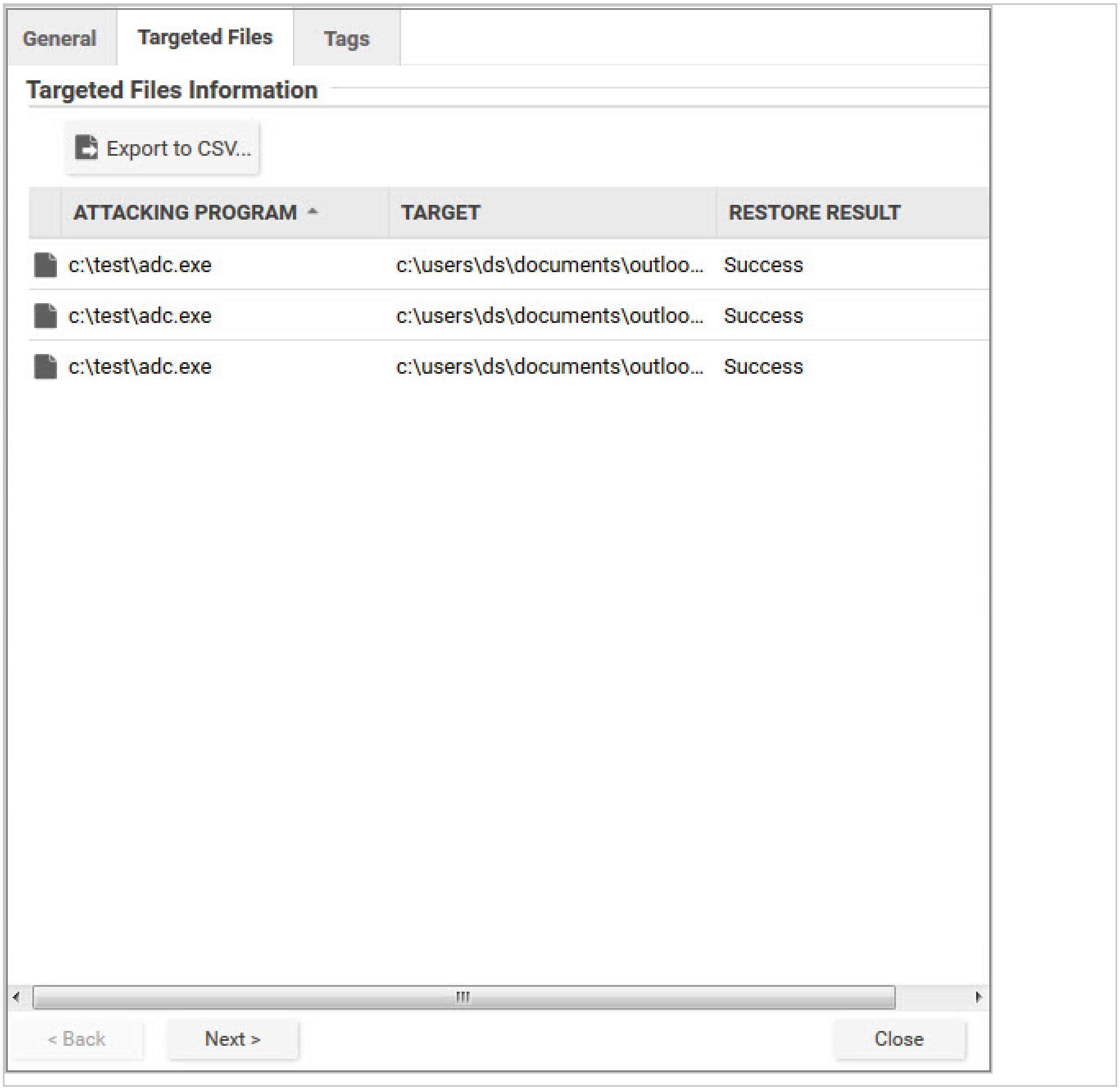
Reason: Default Real-Time Scan Configuration

Major Virus Type: Unauthorized Change

Behavior Monitoring Information

Target: Multiple

TargetType: File System



Targeted Files Information

| ATTACKING PROGRAM | TARGET | RESTORE RESULT |
|---|---|---|
| c:\test\adc.exe | c:\users\ds\documents\outloo... | Success |
| c:\test\adc.exe | c:\users\ds\documents\outloo... | Success |
| c:\test\adc.exe | c:\users\ds\documents\outloo... | Success |

If you investigate and find that an identified file is not harmful, you can right-click the event and click **Allow** to add the file to a scan exclusion list for the computer or policy. You can check the scan exclusion list in the policy or computer editor, under **Anti-Malware > Advanced > Behavior Monitoring Protection Exceptions**.

### What if my agents cannot connect to the Internet directly?

The enhanced scanning features described in this article require Internet access to check files against the Global Census Server and Good File Reputation Service. If your Deep Security Agents cannot access the Internet directly, see "Configure agents that have no internet access" on page 1379 for workarounds.

## Smart Protection in Deep Security

Smart Protection Network integration is available for your computers and workloads through Anti-Malware and Web Reputation modules. Smart Feedback, which is set at the system level, allows you to provide continuous feedback to the Smart Protection Network.

For more about Trend Micro's Smart Protection Network, see Smart Protection Network.

In this topic:

- "Anti-Malware and Smart Protection" below
- "Web Reputation and Smart Protection" on page 779
- "Smart Feedback" on page 779

See also Smart Protection Server documentation for instructions on how to manually deploy the server.

### Anti-Malware and Smart Protection

- Benefits of Smart Scan
- "Enable Smart Scan" on the next page
- "Smart Protection Server for File Reputation Service" on the next page

#### Benefits of Smart Scan

Smart Scan provides the following features and benefits:

- Provides fast, real-time security status lookup capabilities in the cloud.
- Reduces the overall time it takes to deliver protection against emerging threats.
- Reduces network bandwidth consumed during pattern updates. The bulk of pattern definition updates only needs to be delivered to the cloud, not to many endpoints.
- Reduces the cost and overhead associated with corporate-wide pattern deployments.

### Enable Smart Scan

Smart Scan is available in the Anti-Malware module. It uses Trend Micro's Smart Protection Network to allow local pattern files to be small and reduces the size and number of updates required by agents and appliances. When Smart Scan is enabled, the agent downloads a small version of the malware pattern from a Trend Micro Update Server. This smaller pattern can quickly identify files as either *confirmed safe* or *possibly dangerous*. Possibly dangerous files are compared against the larger complete pattern files stored on Trend Micro Smart Protection Servers to determine with certainty whether they pose a danger or not.

Without Smart Scan enabled, relay agents must download the full malware pattern from a Trend Micro Update Server to be used locally on the agent. The pattern will only be updated as scheduled security updates are processed. The pattern is typically updated once per day for your agents to download and is around 120 MB.

You should verify that the computer can reliably connect to the global Trend Micro Smart Protection Network URLs. For details, see "Port numbers, URLs, and IP addresses" on page 478. If connectivity is blocked by a firewall, proxy, or AWS security group, or if the connection is unreliable, anti-malware performance is reduced.

1. Go to **Policies**.
2. Double-click a policy.
3. Go to **Anti-Malware** > **Smart Protection**.
4. In the **Smart Scan** section, either:
   - Select **Inherited** (if the parent policy has Smart Scan enabled).
   - Deselect **Inherited**, and then select either **On** or **On for Deep Security Agent, Off for Virtual Appliance**.
5. Click **Save**.

**Note:** A computer that is configured to use Smart Scan does not download full anti-malware patterns locally. Therefore, if your anti-malware license expires while a computer is configured to use Smart Scan, switching Smart Scan off does not result in local patterns being used to scan for malware since no anti-malware patterns is present locally.

#### Smart Protection Server for File Reputation Service

Smart Protection Server for File Reputation Service is available in the Anti-Malware module. It supplies file reputation information required by Smart Scan.

You edit Smart Protection Server for File Reputation Service as follows:

1. Go to **Computers** or **Policies > Anti-Malware > Smart Protection**.
2. Select to connect directly to Trend Micro's Smart Protection Server or to connect to one or more locally installed Smart Protection Servers.
3. If you want to use a proxy for communication between agents and the Smart Protection Network, you should create a proxy server specifically for the Smart Protection Network. You can view and edit the list of available proxies on the **Proxies** tab on the **Administration > System Settings** page. For information on proxy protocols, see "Supported proxy protocols" on page 1336.
4. Select the **When off domain, connect to global Smart Protection Service (Windows only)** option to use the global Smart Protection Service if the computer is off domain. The computer is considered to be off domain if it cannot connect to its domain controller (this option is for Windows agents only).
5. Set **Smart Protection Server Connection Warning** to generate error events and alerts when a computer loses its connection to the Smart Protection Server.

## Web Reputation and Smart Protection

Smart Protection Server for Web Reputation supplies web reputation information required by the Web Reputation module.

You edit Smart Protection Server for Web Reputation Service as follows:

1. Go to **Computers** or **Policies > Web Reputation > Smart Protection**.
2. Select to connect directly to Trend Micro's Smart Protection Server or to connect to one or more locally installed Smart Protection Servers.
3. If you want to use a proxy for communication between agents and the Smart Protection Network, you should create a proxy server specifically for the Smart Protection Network. You can view and edit the list of available proxies on the **Proxies** tab on the **Administration > System Settings** page. For information on proxy protocols, see "Supported proxy protocols" on page 1336.
4. Select **When off domain, connect to global Smart Protection Service (Windows only)** to use the global Smart Protection Service if the computer is off domain. The computer is considered to be off domain if it cannot connect to its domain controller (this option is for Windows agents only).
5. Set **Smart Protection Server Connection Warning** to generate error events and alerts when a computer loses its connection to the Smart Protection Server.

## Smart Feedback

Trend Micro Smart Feedback provides continuous communication between Trend Micro products and the company's 24/7 threat research centers and technologies. With Smart Feedback, products become an active part of the Trend Micro Smart Protection Network, where large amounts of threat data is shared and analyzed in real time. This interconnection enables never before possible rates of analysis, identification, and prevention of new threats-a level of responsiveness that addresses the thousands of new threats and threat variants released daily.

Trend Micro Smart Feedback is a system setting in the Deep Security Manager. When enabled, Smart Feedback shares protected threat information with the Smart Protection Network, allowing Trend Micro to rapidly identify and address new threats. By default, Smart Feedback is enabled. You can disable it or adjust its settings by going to **Administration > System Settings > Smart Feedback**.

Smart Feedback uses **Update Source Proxy** in the **Relay Group Properties** area via **Administration > Updates > Relay Management**. For details, see Connect to the Primary Security Update Source via proxy.

## Handle malware

### View and restore identified malware

An identified file is a file that has been found to be or to contain malware and has therefore been encrypted and moved to a special folder on the protected computer. Whether or not an infected file can be viewed and restored depends on the anti-malware configuration and the operating system on which the file was found:

- On Windows agents, you can view and restore "Customize malware remedial actions" on page 759 files.
- On Linux agents, you can view and restore only quarantined files.

Topics on this page:

- "See a list of identified files" on the next page
- "Working with identified files" on the next page
- "Search for an identified file" on page 783
- "Restore identified files " on page 784
- "Manually restore identified files" on page 787

For information about events that are generated when malware is encountered, see "Anti-malware events" on page 1285.

### See a list of identified files

The Events and Reports page provides a list of identified files. From there you can see the details for any of those files:

1. Click **Events and Reports** > **Events** > **Anti-Malware Events** > **Identified Files**.
2. To see the details of a file, select the file and click **View**.

The list of identified files includes the following columns of information:

- **Infected File:** Shows the name of the infected file and the specific security risk.
- **Malware:** Names the malware infection.
- **Computer:** Indicates the name of the computer with the suspected infection.
- **File Status**: Indicates whether or not a file is ready for download.

The Details window provides the following information:

- **Detection Time:** The date and time on the infected computer that the infection was detected.
- **Infected File(s):** The name of the infected file.
- **File SHA-1:** The SHA-1 hash of the file.
- **Malware:** The name of the malware that was found.
- **Scan Type:** Indicates whether the malware was detected by a Real-time, Scheduled, or Manual scan.
- **Action Taken:** The result of the action taken by Deep Security when the malware was detected.
- **Computer:** The computer on which this file was found. (If the computer has been removed, this entry will read "Unknown Computer".)
- **Container Name:** Name of the Docker container where the malware was found.
- **Container ID:** ID of the Docker container where the malware was found.
- **Container Image Name:** Image name of the Docker container where the malware was found.

### Working with identified files

The **Identified Files** page allows you to manage tasks related to identified files. Using the menu bar or the context menu, you can do the following:

- **Restore** identified files back to their original location and condition. Note that you cannot perform this action if your host uses the **Agent/Appliance Initiated** communication.
- **Download** identified files from the computer or Virtual Appliance to a location of your choice. To download files:
  a. Select the files you want to download.
  b. Go to **Download > Request download**. The **File Status** column indicates that the download is pending.
  c. Once the file is ready for download, the **File Status** column changes to **Ready for download** and the system event **Identified file is ready for download** appears.
  d. Select the identified files that are ready to be downloaded.
  e. Go to **Download > Download**.

  Once a file is ready for download, you have 24 hours to download the file to your location of choice.

- **Analyze** identified files from the computer or Virtual Appliance.
- **Delete** one or more identified files from the computer or Virtual Appliance. Note that you cannot perform this action if your host uses the **Agent/Appliance Initiated** communication.
- **Export** information about the identified files (not the file itself) to a CSV file.
- **View** the details of an identified file.
- **Computer Details** displays the screen of the computer on which the malware was detected.
- **View Anti-Malware Event** displays the anti-malware event associated with this identified file.
- **Add or Remove Columns** by clicking **Add/Remove.**
- **Search** for a particular identified file.

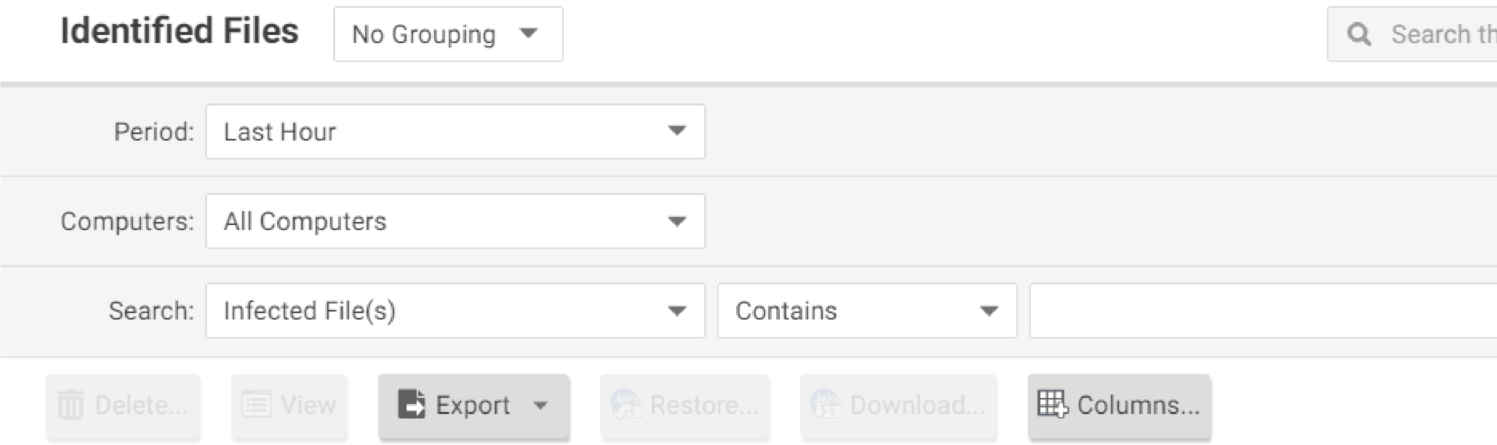
Identified files are automatically deleted from a Deep Security Virtual Appliance when the following occurs:

- A VM is moved to another ESXi host by vMotion. Identified files associated with that VM are deleted from the virtual appliance.

- A VM is deactivated from the Deep Security Manager. Identified files associated with that VM are deleted from the virtual appliance.
- Deep Security Virtual Appliance is deactivated from the Deep Security Manager. All the identified files stored on that virtual appliance are deleted.
- Deep Security Virtual Appliance is deleted from the vCenter. All identified files stored on that virtual appliance are deleted.

### Search for an identified file

- Use the **Period** drop-down menu to see only the files that were identified within a specific time frame.
- Use the **Computers** drop-down menu to organize files by Computer Groups or Computer Policies.
- Click **Search this page > Open Advanced Search** to toggle the display of the advanced search options:


Identified Files

Period: Last Hour

Computers: All Computers

Search: Infected File(s) Contains

Advanced searches include one or more search criteria for filtering identified files. Each criterion is a logical statement comprised of the following items:

- The characteristic of the identified file to filter on, such as the type of file (infected file or malware) or the computer that was affected.
- An operator:
  - **Contains:** The entry in the selected column contains the search string.
  - **Does Not Contain:** The entry in the selected column does not contain the search string.
  - **Equals:** The entry in the selected column exactly matches the search string.

  - **Does Not Equal:** The entry in the selected column does not exactly match the search string.
  - **In:** The entry in the selected column exactly matches one of the comma-separated search string entries.
  - **Not In:** The entry in the selected column does not exactly match any of the comma-separated search string entries.
- A value.

To add a criterion, click the "plus" button (+) to the right of the topmost criterion.To search, click the Search button (the circular arrow).

> **Note:** Searches are not case-sensitive.

**Restore identified files**

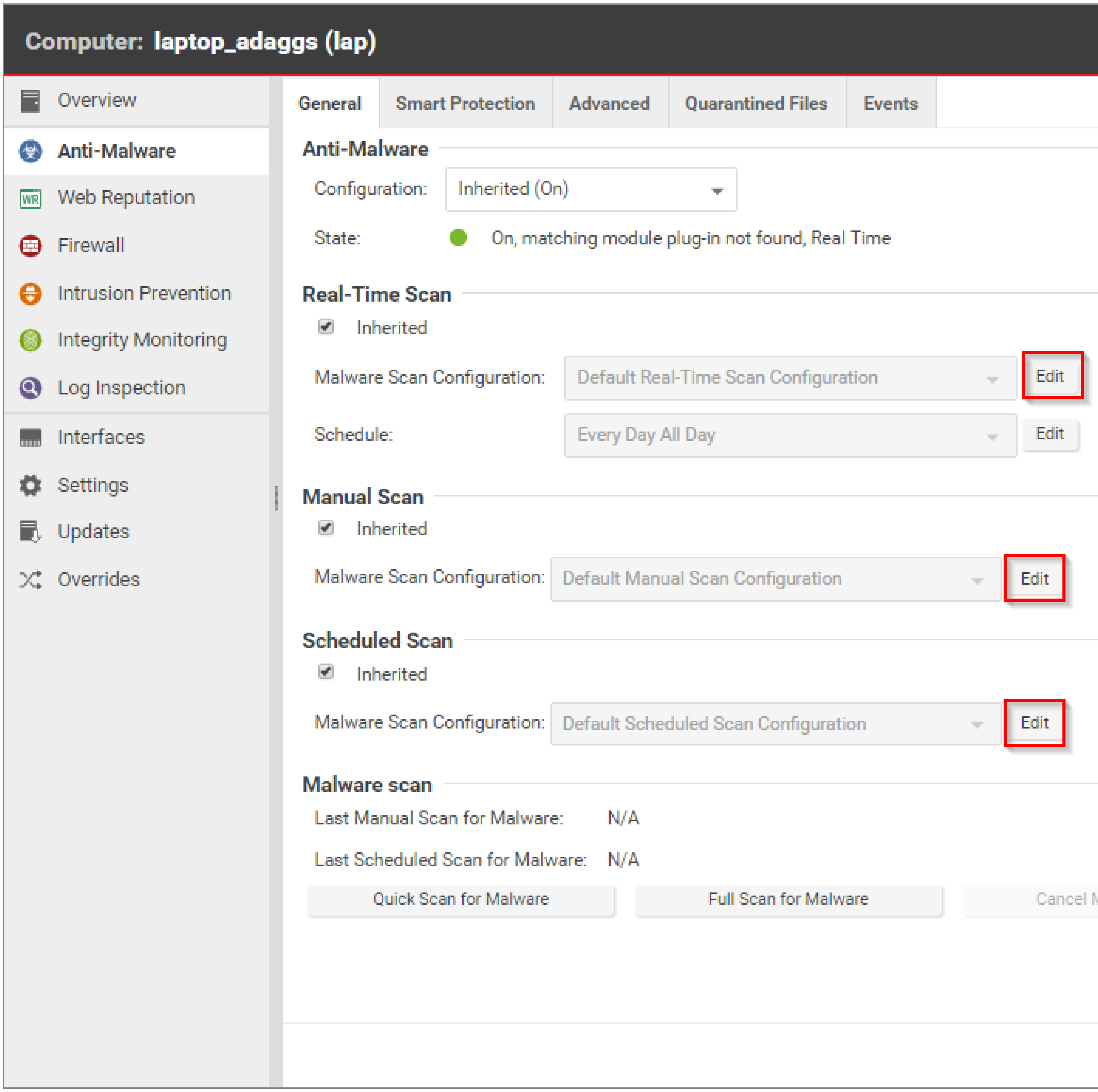
## Create a scan exclusion for the file

Before you can restore a file to its original location, you have to create a scan exclusion so that Deep Security doesn't immediately re-identify the file when it reappears on the computer.

> **Note:** The following instructions describe how to create an exclusion for the file on an individual computer but you can make the same configuration changes at the policy level.

1. Open the Computers page and go to **Anti-Malware > Identified Files** and double click the identified file to view its properties.
2. Note the file's exact name and original location.
3. Still in the Computers page, go to **Anti-Malware > General** and click the Edit button next to each Malware Scan that's in effect to open the Malware Scan Configuration properties

window.



Computer: laptop_adaggs (lap)

Anti-Malware

Configuration: Inherited (On)

State: ● On, matching module plug-in not found, Real Time

Real-Time Scan

☑ Inherited

Malware Scan Configuration: Default Real-Time Scan Configuration

Schedule: Every Day All Day

Manual Scan

☑ Inherited

Malware Scan Configuration: Default Manual Scan Configuration

Scheduled Scan

☑ Inherited

Malware Scan Configuration: Default Scheduled Scan Configuration

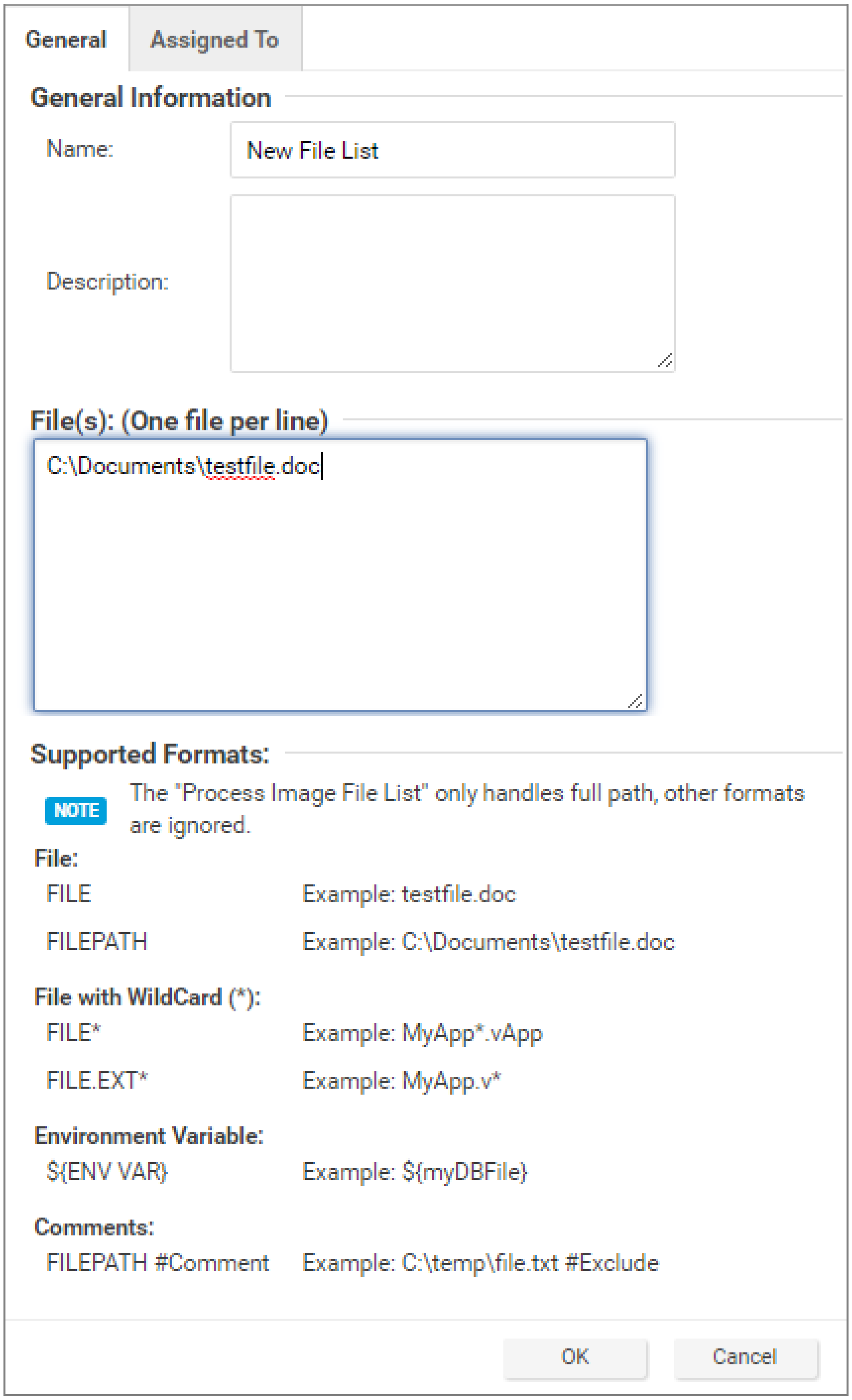
Malware scan

Last Manual Scan for Malware: N/A

Last Scheduled Scan for Malware: N/A

4. In the **Malware Scan Configuration** properties window, click on the **Exclusions** tab.
5. In the **Scan Exclusions** area, select **File List** and then either press edit if a file list is already selected, or select **New** from the menu to create a new File List.

6. In the **File List** properties window, enter the file path and name of the file to be restored. Click **OK** to close the File List properties window.



**General Information**

Name: New File List

Description:

**File(s): (One file per line)**

C:\Documents\testfile.doc

**Supported Formats:**

NOTE The "Process Image File List" only handles full path, other formats are ignored.

**File:**

| | |
|---|---|
| FILE | Example: testfile.doc |
| FILEPATH | Example: C:\Documents\testfile.doc |

**File with WildCard (*):**

| | |
|---|---|
| FILE* | Example: MyApp*.vApp |
| FILE.EXT* | Example: MyApp.v* |

**Environment Variable:**

| | |
|---|---|
| ${ENV VAR} | Example: ${myDBFile} |

**Comments:**

| | |
|---|---|
| FILEPATH #Comment | Example: C:\temp\file.txt #Exclude |

7. Close the **Malware Scan Configuration** properties window by clicking **OK**.
8. When you've edited all the **Malware Scan Configurations**, click **Save** in the Computers page to save your changes. You're now ready to restore your file.

# Restore the file

1. Still in the Computers page, go to the **Anti-Malware > Identified Files** tab.
2. Right-click the identified file and select **Actions > Restore** and follow the steps in the wizard.

Your file is restored to its original location.

### Manually restore identified files

To manually restore an identified file, download the file to your computer. The **Identified File** wizard will display a link to an **Administration Utility** which you can use to decrypt, examine, or restore the file. Use the quarantined file decryption utility to decrypt the file and then move it back to its original location.

The decryption utility is in a zip file, **QFAdminUtil_win32.zip**, located in the "util" folder under the Deep Security Manager root directory. The zipped file contains two utilities which perform the same function: **QDecrypt.exe** and **QDecrypt.com**. Running **QDecrypt.exe** invokes an open file dialog that lets you select the file for decryption. **QDecrypt.com** is a command-line utility with the following options:

- **/h, --help**: show this help message
- **--verbose**: generate verbose log messages
- **/i, --in=<str>**: quarantined file to be decrypted, where **<str>** is the name of the quarantined file
- **/o, --out=<str>**: decrypted file output, where **<str>** is the name given to the resulting decrypted file

**Note:** This utility is supported on Windows 32-bit systems and Windows 64-bit systems.

## Configure advanced exploit exceptions

Files that are not malicious can be falsely identified as malware if they share certain characteristics with malware. If a file is known to be benign and is identified as malware, you can create an exception for that file. When an exception is created, the file does not trigger an event when Deep Security scans the file.

For an overview of the anti-malware module, see "About Anti-Malware" on page 735.

You can also exclude files from real-time, manual, and scheduled scans. For more information, see "Specify the files to scan" on page 750.

Exceptions can be created for the following types of malware and malware scans:

- Predictive Machine Learning scans. For more information, see "Detect emerging threats using Predictive Machine Learning" on page 768.
- Scans for spyware and grayware. For more information, see "Scan for spyware and grayware" on page 748.
- Behavior monitoring protection. For more information, see "Enhanced anti-malware and ransomware scanning with behavior monitoring" on page 770.

You can also exclude files from Anti-Malware scanning if they are signed by a trusted certificate. This feature is supported with Deep Security Agent 20.0.0-3445+ on Windows. For details, see "Exclude files signed by a trusted certificate" on page 793.

Deep Security maintains a list of exceptions for each type of malware scan in policy and computer properties.

1. To see the lists of exceptions, open the policy or computer editor.
2. Click **Anti-Malware > Advanced**.
   The exceptions are listed in the **Allowed Spyware/Grayware**, **Document Exploit Protection Rule Exceptions**, **Predictive Machine Learning Detection Exceptions**, **Behavior Monitoring Protection Exceptions**, and **Trusted Certificates Detection Exceptions** sections.

See also "Scan exclusion recommendations" on page 792.

### Create an exception from an anti-malware event

When a file is identified as malware, Deep Security generates an anti-malware event. If you know that the file is benign, you can create an exception for the file from the event report, as follows:

1. Click **Events & Reports > Events > Anti-Malware Events** and locate the malware detection event.
2. Right-click the event.
3. Select **Allow**.

### Manually create an anti-malware exception

You can manually create anti-malware exceptions for spyware or grayware, document exploit protection rules, predictive machine learning, and behavior monitoring exceptions. To add the exception, you need specific information from the anti-malware event that the scan generated. The type of malware or scan determines the information that you need:

- **Spyware or grayware:** The value in the MALWARE field, for example `SPY_CCFR_CPP_TEST.A`
- **Document exploit protection rules:** The value in the MALWARE field, for example `HEUR_OLEP.EXE`
- **Predictive machine learning:** The SHA1 digest of the file from the FILE SHA-1 field, for example `3395856CE81F2B7382DEE72602F798B642F14140`
- **Behavior monitoring:** The process image path, for example `C:\test.exe`

1. Click **Events & Reports > Events > Anti-Malware Events** and copy the field value that is required to identify the malware.
2. Open the policy or computer editor where you want to create the exception.
3. Click **Anti-Malware > Advanced**.
4. In the **Allowed Spyware/Grayware**, **Document Exploit Protection Rule Exceptions**, **Predictive Machine Learning Detection Exceptions**, or **Behavior Monitoring Protection Exceptions** section, enter the information from the event in the text box.
5. Click **Add**.

# Exception List Wildcard Support

The **Behavior Monitoring Protection Exceptions** list supports the use of wildcard characters when defining file path, file name, and file extension exception types. Use the following table to properly format your exception lists to ensure that Deep Security excludes the correct files and folders from scanning.

Supported wildcard characters:

- Asterisk (*): Represents any character or string of characters

Note that the Behavior Monitoring Protection Exceptions list does not support the use of wildcard characters to replace system drive designations or within Universal Naming Convention (UNC) addresses.

| Exception Type | Wildcard Usage | Matched | Not Matched |
|---|---|---|---|
| Directories | `C:\*`<br>Excludes all files and folders on the specified drive | • `C:\sample.exe`<br>• `C:\folder\test.doc` | • `D:\sample.exe`<br>• `E:\folder\test.doc` |

| Exception Type | Wildcard Usage | Matched | Not Matched |
|---|---|---|---|
| Specific files under a specific folder level | `C:\*\Sample.exe`<br>Excludes the `Sample.exe` file only if the file is located in any subfolder of the `C:\` directory | - `C:\files\Sample.exe`<br>- `C:\temp\files\Sample.exe` | - `C:\sample.exe` |
| Universal Naming Convention (UNC) paths | `\\<UNC path>\*\Sample.exe`<br>Excludes the `Sample.exe` file only if the file is located in any subfolder of the specified UNC path | - `\\<UNC path>\files\Sample.exe`<br>- `\\<UNC path>\temp\files\Sample.exe` | - `R:\files\Sample.exe`<br>Reason: Mapped drives are not supported.<br>- `\\<UNC path>\Sample.exe`<br>Reason: The file does not exist within a subfolder of the UNC path. |
| File names and extensions | `C:\*.*`<br>Excludes all files with extensions in all folders and subfolders of the `C:\` directory | - `C:\Sample.exe`<br>- `C:\temp\Sample.exe`<br>- `C:\test.doc` | - `D:\sample.exe`<br>- `C:\Sample`<br>**Note:** Because `C:\Sample` does not have a file extension, it is not a match for the exception. |

| Exception Type | Wildcard Usage | Matched | Not Matched |
|---|---|---|---|
| File names | `C:\*.exe`<br>Excludes all files with the `.exe` extension in all folders and subfolders of the `C:\` directory | - `C:\Sample.exe`<br>- `C:\temp\test.exe` | - `C:\Sample.doc`<br>- `C:\temp\test.bat`<br>- `C:\Sample`<br>**Note:** Because `C:\Sample` does not have a file extension, it is not a match for the exception. |
| File extensions | `C:\Sample.*`<br>Excludes all files with the name `Sample` and any extension in the `C:\` directory | - `C:\Sample.exe` | - `C:\Sample1.doc`<br>- `C:\temp\Sample.bat`<br>- `C:\Sample`<br>**Note:** Because `C:\Sample` does not have a file extension, it is not a match for the exception. |
| Files in specific directory structures | `C:\*\*\Sample.exe`<br>Excludes all files located within the second subfolder level or any subsequent subfolders of the `C:\` directory with | - `C:\files\temp\Sample.exe`<br>- `C:\files\temp\test\Sample.exe` | - `C:\Sample.exe`<br>- `C:\temp\Sample.exe`<br>- `C:\files\temp\Sample.doc` |

| Exception Type | Wildcard Usage | Matched | Not Matched |
|---|---|---|---|
| | the file name and extension `Sample.exe` | | |

### Exception strategies for spyware and grayware

When spyware is detected, the malware can be immediately cleaned, quarantined, or deleted, depending on the malware scan configuration that controls the scan. After you create the exception for a spyware or grayware event, you might have to restore the file. For more information, see "Restore identified files " on page 784.

Alternatively, you can temporarily scan for spyware and grayware with the action set to Pass so that all spyware and grayware detections are recorded on the Anti-Malware Events page but not cleaned, quarantined, or deleted. You can then create exceptions for the detected spyware and grayware. When your exception list is robust, you can set the action to Clean, Quarantine, or Delete modes.

For information about setting the action, see "Configure malware handling" on page 759.

### Scan exclusion recommendations

The best and most comprehensive source for scan exclusions is from the software vendor. The following are some high-level scan exclusion recommendations:

- Quarantine folders (such as `SMEX` on Microsoft Windows Exchange Server) should be excluded to avoid rescanning files that have already been confirmed to be malware.
- Large databases and database files (for example, dsm.mdf and dsm.ldf) should be excluded because scanning could impact database performance. If it is necessary to scan database files, you can create a scheduled task to scan the database during off-peak hours. Since Microsoft SQL Server databases are dynamic, exclude the directory and backup folders from the scan list:

  For Windows:

  ```
  ${ProgramFiles}\Microsoft SQL Server\MSSQL\Data\
  ```

  ```
  ${Windir}\WINNT\Cluster\ # if using SQL Clustering
  ```

  ```
  Q:\ # if using SQL Clustering
  ```

For Linux:

```
/var/lib/mysql/ # if path is set to this Data Location of MySQL in the machine.
```

```
/mnt/volume-mysql/ # if path is set to this Data Location of MySQL in the machine.
```

For a list of recommended scan exclusions, see the Trend Micro recommended scan exclusion list. Microsoft also maintains an Anti-Virus Exclusion List that you can use as a reference for excluding files from scanning on Windows servers.

#### Exclude files signed by a trusted certificate

If you have signed applications and want to exclude all activities of those processes from real-time Anti-Malware scanning (including file scans, behavior monitoring, and predictive machine learning), you can add the digital certificate to your trusted certificate list in Deep Security Manager, as follows:

1. In the policy or computer editor, go to **Anti-Malware > Advanced**.
2. In the **Trusted Certificates Detection Exemptions** section, set **Exclude files with trusted certificate** to "Yes" or "Inherited (Yes)".
3. Select **Manage Certificate List**.
4. The Trusted Certificates window displays any certificates you have imported. Select **Import From File** to add another one for scan exclusions.
5. Choose the certificate file and then select **Next**.
6. Review the certificate summary that's displayed and set **Trust this certificate for** to **Scan Exclusions**. Select **Next**.
7. The Summary page indicates whether the import was successful. Select **Close**.

Note: This type of exclusion is supported with Deep Security Agent 20.0.0-3445+ on Windows.

The imported certificate appears in the Trusted Certificates list with the **Purpose** listed as **Exception**.

Tip: Deep Security checks the exemption list when a process starts. If a process is running before the exemption is configured, the process will not be added to the exemption list until it is restarted.

### Increase debug logging for anti-malware in protected Linux instances

You can increase or decrease verbosity of the anti-malware (AM) debug logging used to diagnose any issue related to AM when running on a Linux operating system.

Anti-malware debug logs are automatically included when you create a diagnostic package for technical support.

For information on creating a diagnostic package, see "Create a diagnostic package" on page 1723.

To increase the anti-malware debug log level, enter the following command in a shell on the Linux instance as a superuser:

```
killall -USR1 ds_am
```

This command will increase the level one unit. By default the level is 6 and the maximum is 8.

To decrease the anti-malware debug log level, enter the following command in a shell on the Linux instance as a superuser:

```
killall -USR2 ds_am
```

This command decreases the level by one unit. The minimum level is 0.

> **Note:** If your Linux distribution doesn't use `killall` you can substitute it with the `pkill` command.

## Configure Web Reputation

The Web Reputation module protects against web threats by blocking access to malicious URLs. Deep Security uses Trend Micro's web security databases from Smart Protection Network sources to check the reputation of websites that users are attempting to access. The website's reputation is correlated with the specific web reputation policy enforced on the computer. Depending on the security level being enforced, Deep Security either blocks or allows access to the URL.

For a list of operating systems where Web Reputation is supported, see "Supported features by platform" on page 425.

The Web Reputation module supports HTTPS traffic. For more information, see Inspect TLS Traffic.

You can enable and configure Web Reputation by performing the following steps:

1. "Enable the Web Reputation module" below
2. "Enable the Trend Micro Toolbar" below
3. "Switch between inline and tap mode" on the next page
4. "Enforce the security level" on the next page
5. "Create exceptions" on page 797
6. "Configure the Smart Protection Server" on page 798
7. "Edit advanced settings" on page 799
8. "Test Web Reputation" on page 800

For information on how to suppress messages that appear to users of agent computers, see "Configure notifications on the computer" on page 762

## Enable the Web Reputation module

1. Go to **Policies**.
2. Double-click the policy for which you want to enable web reputation.
3. Click **Web Reputation > General**.
4. For **Web Reputation State**, select **On**.
5. Click **Save**.

## Enable the Trend Micro Toolbar

After you enable the Trend Micro Toolbar, if you use your web browser to visit a dangerous, highly suspicious, or suspicious website, you will see a blocking page in the main window of your web browser and a message in the Windows notification area. In addition, attempts to access a URL rated as dangerous, highly suspicious, or suspicious are logged in Workload Security's **Web Reputation Events** tab.

When the Trend Micro Toolbar is included in your browser extensions, a small Trend Micro logo appears in your browser: in Chrome and Firefox, the logo appears to the right of the website address field.

### Install the toolbar for Windows

The **Trend Micro Toolbar** extension for Windows is supported only on certain Windows platforms. It is currently supported with Chrome and Microsoft Edge browsers. See the "Supported features by platform" on page 425 tables for more details.

The **Trend Micro Toolbar** for Windows is downloaded automatically when the Web Reputation module is enabled. The browser is installed the next time the web browser is restarted.

## Switch between inline and tap mode

Web reputation uses the Deep Security Network Engine which can operate in one of two modes:

- **Inline:** Packet streams pass directly through the Deep Security network engine. All rules are applied to the network traffic before they proceed up the protocol stack.
- **Tap mode:** Packet streams are not modified. The traffic is still processed by Web Reputation, if it's enabled. However any issues detected do not result in packet or connection drops. When in Tap mode, Deep Security offers no protection beyond providing a record of events.

In tap mode, the live stream is not modified. All operations are performed on the replicated stream. When in tap mode, Deep Security offers no protection beyond providing a record of events.

To switch between inline and tap mode, open the **Computer or Policy editor**[1] and go to **Settings > Advanced > Network Engine Mode**.

For more on the network engine, see "Test Firewall rules before deploying them" on page 852.

## Enforce the security level

Web addresses that are known to be or are suspected of being malicious are assigned a **risk level** of:

- **Dangerous**: Verified to be fraudulent or known sources of threats
- **Highly suspicious**: Suspected to be fraudulent or possible sources of threats
- **Suspicious**: Associated with spam or possibly compromised

Security levels determine whether Deep Security allows or blocks access to a URL, based on the associated risk level. For example, if you set the security level to low, Deep Security will only block URLs that are known to be web threats. As you set the security level higher, the web threat detection rate improves but the possibility of false positives also increases.

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

### To configure the security level:

1. Go to **Policies**.
2. Double-click the policy that you want to edit.
3. Click **Web Reputation > General**.
4. Select one of the following security levels:
   - **High**: Blocks pages that are:
     - Dangerous
     - Highly suspicious
     - Suspicious
   - **Medium**: Blocks pages that are:
     - Dangerous
     - Highly Suspicious
   - **Low**: Blocks pages that are:
     - Dangerous
5. Click **Save**.

## Create exceptions

You can override the block and allow behavior dictated by the Smart Protection Network's assessments with your lists of URLs that you want to block or allow.

> **Note:** The **Allowed** list takes precedence over the **Blocked** list. URLs that match entries in the **Allowed** list are not checked against the **Blocked** list.

### To create URL exceptions:

1. Go to **Policies**.
2. Double-click the policy that you want to edit.
3. Click **Web Reputation > Exceptions**.
4. To allow URLs:
   a. Go to the **Allowed** section.
   b. In the blank under **URLs to be added to the Allowed list (one per line)**, enter your desired URL. Multiple URLs can be added at once but they must be separated by a line break.

c. Select one of the following:
   - **Allow URLs from the domain**: All pages from the specified domain are allowed. Subdomains are supported. Only include the domain (and optionally subdomain) in the entry. For example, "testdomain.com" and "another.testdomain.com" are valid entries.
   - **Allow the URL**: Specified URL is allowed. Wildcards are supported. For example, "testdomain.com/shopping/coats.html", and "testdomain.com/shopping/*" are valid entries.

d. Click **Add**.

To block URLs:

a. Go to the **Blocked** section

b. In the blank under **URLs to be added to the Blocked list (one per line)**, enter your desired URL. Multiple URLs or keywords can be added at once but they must be separated by a line break.

c. Select one of the following:
   - **Block URLs from the domain**: All pages from the specified domain are blocked. Subdomains are supported. Only include the domain (and optionally subdomain) in the entry. For example, "testdomain.com" and "another.testdomain.com" are valid entries.
   - **Block the URL**: Specified URL is blocked. Wildcards are supported. For example, "testdomain.com/shopping/coats.html" and "testdomain.com/shopping/*" are valid entries. If the URL contains a question mark ( ? ), you need to prepend it with a back slash ( \ ). For example, "testdomain.com/shopping.com/?testQuery=test" should be entered as "testdomain.com/shopping/\?testQuery=test".
   - **Block URLs containing this keyword**: Any URL containing the specified keyword is blocked.

d. Click **Add**.

5. Click **Save**.

## Configure the Smart Protection Server

Smart Protection Service for web reputation supplies web information required by the web reputation module. For more information, see Smart Protection Network - Global Threat Intelligence.

To configure Smart Protection Server:

1. Go to **Policies**.
2. Double-click the policy you'd like to edit.
3. Click **Web Reputation > Smart Protection**.
4. Select whether to connect directly to Trend Micro's Smart Protection service:
   a. Select **Connect directly to Global Smart Protection Service**.
   b. Optionally select **When accessing Global Smart Protection Service, use proxy**. Select **New** and enter your desired proxy.

   Or to connect to one or more locally-installed Smart Protection Servers:

   a. Select **Use locally-installed Smart Protection Server. For example, "http://[server]:5274"**.
   b. Enter the Smart Protection Server URL into the field and click **Add**. To find the Smart Protection Server URL, log in to the Smart Protection Server, and in the main pane, look under **Real Time Status**. The Smart Protection Server's HTTP and HTTPS URLs are listed in the **Web Reputation** row. The HTTPS URL is only supported with Deep Security Agents version 11.0 or later. If you have version 10.3 or earlier agents, use the HTTP URL.
   c. Optionally, for Windows only, select **When off domain, connect to global Smart Protection Service.**.
5. Click **Save**.

### Smart Protection Server Connection Warning

This option determines whether or not error events are generated and alerts are raised if a computer loses its connection to the Smart Protection Server. Select either **Yes** or **No** and click **Save**.

If you have a locally installed Smart Protection Server, this option should be set to **Yes** on at least one computer so that you are notified if there is a problem with the Smart Protection Server itself.

## Edit advanced settings

### Blocking Page

When users attempt to access a blocked URL, they are redirected to a blocking page. In the blank for **Link**, provide a link that users can use to request access to the blocked URL.

### Alert

Decide to raise an alert when a web reputation event is logged by selecting either **Yes** or **No**.

### Ports

Select specific ports to monitor for potentially harmful web pages from the drop down list next to **Ports to monitor for potentially harmful web pages**.

## Test Web Reputation

Before continuing, test that the Web Reputation is working correctly:

1. Ensure Web Reputation is enabled.
2. Go to the **Computer or Policy editor > Web Reputation > Exceptions**.
3. Under **Blocked**, enter *http://www.speedtest.net* and click **Add**.
4. Click **Save**.
5. Open a browser and attempt to access the website. A message denying the access should appear.
6. Go to **Events & Reports > Web Reputation** to verify the record of the denied web access. If the detection is recorded, the Web Reputation module is working correctly.

# Configure Intrusion Prevention (IPS)

## About Intrusion Prevention

The Intrusion Prevention module protects your computers from known and zero-day vulnerability attacks as well as against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities.

When patches are not available for known vulnerabilities in applications or operating systems, Intrusion Prevention rules can intercept traffic that is trying to exploit the vulnerability. It identifies malicious software that is accessing the network and it increases visibility into, or control over, applications that are accessing the network. Therefore your computers are protected until patches that fix the vulnerability are released, tested, and deployed.

Protection is available for file sharing and messaging software such as Skype, but also web applications with vulnerabilities such as SQL injection and cross-site scripting (XSS). In this way, Intrusion Prevention can also be used as a lightweight web application firewall (WAF).

To enable and configure Intrusion Prevention, see "Set up Intrusion Prevention" on page 804.

## Intrusion Prevention rules

Intrusion Prevention rules define a set of conditions that are compared to the payload session and application layers of network packets (such as DNS, HTTP, SSL, and SMTP), as well as the sequence of those packets according to those higher-layer protocols.

> Tip: Firewall rules examine the network and transport layers of a packet (IP, TCP, and UDP, for example).

When Deep Security Agents scan network traffic and the traffic meets a rule's match conditions, the agent handles it as a possible or confirmed attack and performs one of the following actions, depending on the rule:

- Completely drop packets
- Reset the connection

Intrusion Prevention rules are assigned to policies and computers. Therefore you can enforce sets of rules on groups of computers based on the policy that they use, and override policies as required. (See "Policies, inheritance, and overrides" on page 634.)

For information about how you can affect the functionality of rules, see "Configure intrusion prevention rules" on page 811.

### Application types

Application types organize rules by the application that they are associated with. Application types can also store property values that rules can reference as required, such as protocols used for communications, and port numbers. Some application types have configurable properties. For example, the Database Microsoft SQL application type contains rules that are associated with Microsoft SQL Server. You can configure this application type to specify the ports used to connect to the database.

For more information, see "Application types" on page 831.

### Rule updates

Trend Micro creates Intrusion Prevention rules for application vulnerabilities as they are discovered. Security updates can include new or updated rules and application types. When a rule is already assigned to a policy, and an update includes rules upon which the assigned rule depends, you can choose to automatically assign the updated rules.

**Tip:** Intrusion Prevention rules from Trend Micro include information about the vulnerability against which it protects.

Intrusion Prevention rules from Trend Micro are not directly editable through Deep Security Manager. However some rules are configurable, and some rules require configuration. (See "Setting configuration options (Trend Micro rules only)" on page 817.)

### Recommendation scans

You can use recommendation scans to discover the Intrusion Prevention rules that you should assign to your policies and computers. (See "Manage and run recommendation scans" on page 639.)

## Use behavior modes to test rules

Intrusion Prevention works in either Detect or Prevent mode:

- **Detect**: Intrusion Prevention uses rules to detect matching traffic and generate events, but does not block traffic. Detect mode is useful to test that Intrusion Prevention rules do not interfere with legitimate traffic.
- **Prevent**: Intrusion Prevention uses rules to detect matching traffic, generate events, and block traffic to prevent attacks.

When you first apply new Intrusion Prevention rules, use Detect mode to verify that they don't accidentally block normal traffic (false positives). When you are satisfied that no false positives occur, you can use Prevent mode to enforce the rules and block attacks. (See "Enable Intrusion Prevention in Detect mode" on page 805 and "Switch to Prevent mode" on page 810.)

**Tip:** Similar to using Intrusion Prevention in Detect mode, the Deep Security network engine can run in tap mode for testing purposes. In tap mode, Intrusion Prevention detects rule-matching traffic and generates events, but doesn't block traffic. Also, tap mode affects the Firewall and Web Reputation modules. You can use Detect mode to test Intrusion Prevention rules separately.

You use tap mode with Intrusion Prevention in the same way that tap mode is used for testing Firewall rules. See "Test Firewall rules before deploying them" on page 852.

#### Override the behavior mode for rules

By selecting Detect mode for individual rules, you can selectively override Prevent mode behavior set at the computer or policy level. This is useful for testing new Intrusion Prevention rules that are applied to a policy or computer. For example, when a policy is configured such that Intrusion Prevention works in Prevent mode, you can bypass the Prevent mode behavior for an individual rule by setting that rule to Detect mode. For that rule only, Intrusion Prevention merely logs the traffic, and enforces other rules that do not override the policy's behavior mode. (See "Override the behavior mode for a rule" on page 819.)

**Note:** While Prevent mode at the computer or policy level can be overridden by contradictory rule settings, Detect mode cannot. Selecting Detect mode at the computer or policy level enforces Detect mode behavior regardless of rule settings.

Some rules issued by Trend Micro use Detect mode by default. For example, mail client rules generally use Detect mode because in Prevent mode they block the downloading of all mail. Some rules trigger an alert only when a condition occurs a large number times, or a certain number of times within a certain period of time. These types of rules apply to traffic that constitutes suspicious behavior only when a condition recurs, and a single occurrence of the condition is considered normal.

**Warning:**
To prevent blocking legitimate traffic and interrupting network services, when a rule requires configuration, keep it in Detect mode until you've configured the rule. Switch a rule to Prevent mode only after configuration and testing.

## Intrusion Prevention events

By default, the Deep Security Manager collects Firewall and Intrusion Prevention event logs from the Deep Security **Agents and Appliances**[1] at every heartbeat. Once collected by the Deep Security Manager, event logs are kept for a period of time which can be configured. The default setting is one week. (See "Log and event storage best practices" on page 1050.) You can configure event logging for individual rules as required. (See "Configure event logging for rules" on page 815.)

[1] The Deep Securty Agent and Deep Security Virtual Appliance are the components that enforce the Deep Security policies that you have defined. Agents are deployed directly on a computer. Appliances are used in VMware vSphere environments to provide agentless protection. They are not available with Deep Security as a Service.

Event tagging can help you to sort events. You can manually apply tags to events or automatically tag them. You can also use the auto-tagging feature to group and label multiple events. For more information on event tagging, see "Apply tags to identify and group events" on page 1057.

### Support for secure connections

The Intrusion Prevention module supports inspecting packets over secure connections. See "Inspect TLS traffic" on page 832.

### Contexts

Contexts are a powerful way of implementing different security policies depending on the computer's network environment. You typically use contexts to create policies that apply different Firewall and Intrusion Prevention rules to computers (usually mobile laptops) depending on whether that computer is in the office or away.

To determine a computer's location, contexts examine the nature of the computer's connection to its domain controller. For more information, see "Define contexts for use in policies" on page 728.

### Interface tagging

You can use interface types when you need to assign Firewall or Intrusion Prevention rules to a specific interface when a machine has multiple network interfaces. By default, Firewall and Intrusion Prevention rules are assigned to all interfaces on a computer. For example, to apply special rules only to the wireless network interface, use interface types to accomplish this. For more information, see "Configure a policy for multiple interfaces" on page 650.

## Set up Intrusion Prevention

Enable the Intrusion Prevention module and monitor network traffic for exploits using Detect mode. When you are satisfied with how your Intrusion Prevention rules are assigned, switch to Prevent mode.

1. "Enable Intrusion Prevention in Detect mode" on the next page
2. "Test Intrusion Prevention" on page 807
3. "Apply recommended rules" on page 808
4. "Monitor your system" on page 809
5. "Enable 'fail open' for packet or system failures" on page 810
6. "Switch to Prevent mode" on page 810
7. "Implement best practices for specific rules" on page 810

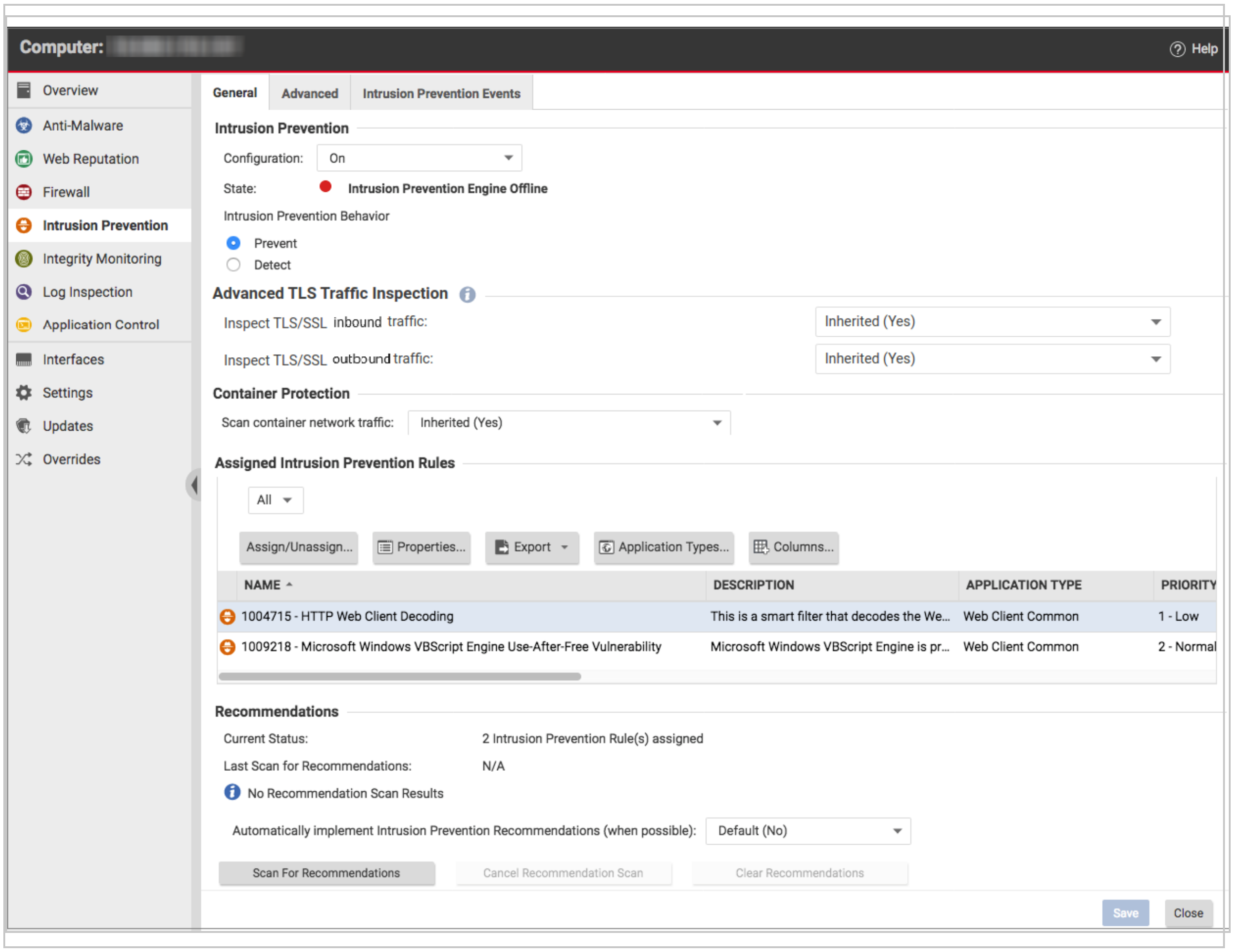
**Note:** CPU usage and RAM usage varies by your IPS configuration. To optimize IPS performance on Deep Security Agent, see "Performance tips for intrusion prevention" on page 848.

For an overview of the Intrusion Prevention module, see "About Intrusion Prevention" on page 800.

## Enable Intrusion Prevention in Detect mode

Enable Intrusion Prevention and use Detect mode for monitoring. Configure Intrusion Prevention using the appropriate policies to affect the targeted computers. You can also configure individual computers:

1. Go to **Computer or Policy editor**[1] > **Intrusion Prevention** > **General**.
2. For **Configuration**, select either **On** or **Inherited (On)**.



Computer: [redacted]

Intrusion Prevention

Configuration: On

State: ● Intrusion Prevention Engine Offline

Intrusion Prevention Behavior

● Prevent
○ Detect

Advanced TLS Traffic Inspection

Inspect TLS/SSL inbound traffic: Inherited (Yes)

Inspect TLS/SSL outbound traffic: Inherited (Yes)

Container Protection

Scan container network traffic: Inherited (Yes)

Assigned Intrusion Prevention Rules

| NAME | DESCRIPTION | APPLICATION TYPE | PRIORITY |
|---|---|---|---|
| 1004715 - HTTP Web Client Decoding | This is a smart filter that decodes the We... | Web Client Common | 1 - Low |
| 1009218 - Microsoft Windows VBScript Engine Use-After-Free Vulnerability | Microsoft Windows VBScript Engine is pr... | Web Client Common | 2 - Normal |

Recommendations

Current Status: 2 Intrusion Prevention Rule(s) assigned

Last Scan for Recommendations: N/A

No Recommendation Scan Results

Automatically implement Intrusion Prevention Recommendations (when possible): Default (No)

3. For **Intrusion Prevention Behavior**, select **Detect**.
4. With Deep Security Agent 11.1 and earlier, the Intrusion Prevention module inspects traffic that passes through the host computer's network interface to containers. With Deep Security Agent 11.2 or later, it can also inspect traffic between containers. When the **Scan container network traffic** setting is set to **Yes**, Deep Security scans the traffic that goes through both containers and hosts. When it is set to **No**, Deep Security scans only the traffic that goes through the host network interface.
5. Click **Save**.

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

Tip: If the behavior settings are not available, **Network Engine Mode** may be set to **Tap**. (See "Test Firewall rules before deploying them" on page 852.)

For more fine-grained control, when you assign Intrusion Prevention rules, you can override the global behavior mode and configure specific rules to either prevent or detect (see "Override the behavior mode for a rule" on page 819).

## Test Intrusion Prevention

Before continuing, you should perform the following steps to verify that the Intrusion Prevention module is working properly:

1. If you have an agent-based deployment, make sure you have a computer that has an agent running. For an agentless deployment, make sure your Deep Security Virtual Appliance is running normally.
2. Disable the Web Reputation module. In Deep Security Manager, click **Computers**, then double-click the computer where you will test Intrusion Prevention. In the computer's dialog, click **Web Reputation**, and select **Off**. Web Reputation is now disabled and won't interfere with the Intrusion Prevention functionality.
3. Make sure bad traffic is blocked. Still in the computer's dialog, click **Intrusion Prevention**, and under the **General** tab, select **Prevent**. (If it is shaded, set the **Configuration** drop-down list to **Inherited (On)**.)
4. Assign the EICAR test policy. Still in the computer's dialog, click **Intrusion Prevention**. Click **Assign/Unassign**. Search for `1005924`. The **1005924 - Restrict Download of EICAR Test File Over HTTP** policy appears. Select it and click **OK**. The policy is now assigned to the computer.
5. Try to download the EICAR file (you cannot, if Intrusion Prevention is running properly). On Windows, go to this link: http://files.trendmicro.com/products/eicar-file/eicar.com. On Linux, enter this command: `curl -O http://files.trendmicro.com/products/eicar-file/eicar.com`
6. Check the Intrusion Prevention events for the computer. Still in the computer's dialog box, click **Intrusion Prevention > Intrusion Prevention Events**. Click **Get Events** to see events that have occurred since the last heartbeat. An event appears with a **Reason** of **1005924 - Restrict Download of EICAR Test File Over HTTP**. The presence of this event indicates that Intrusion Prevention is working.
7. Revert your changes to return your system to its previous state. Turn on the Web Reputation module (if you turned it off), reset the **Prevent** or **Detect** option, and remove the EICAR policy from the computer.

## Apply recommended rules

To maximize performance, only assign the Intrusion Prevention rules that are required by your policies and computers. You can use a recommendation scan to obtain a list of rules that are appropriate.

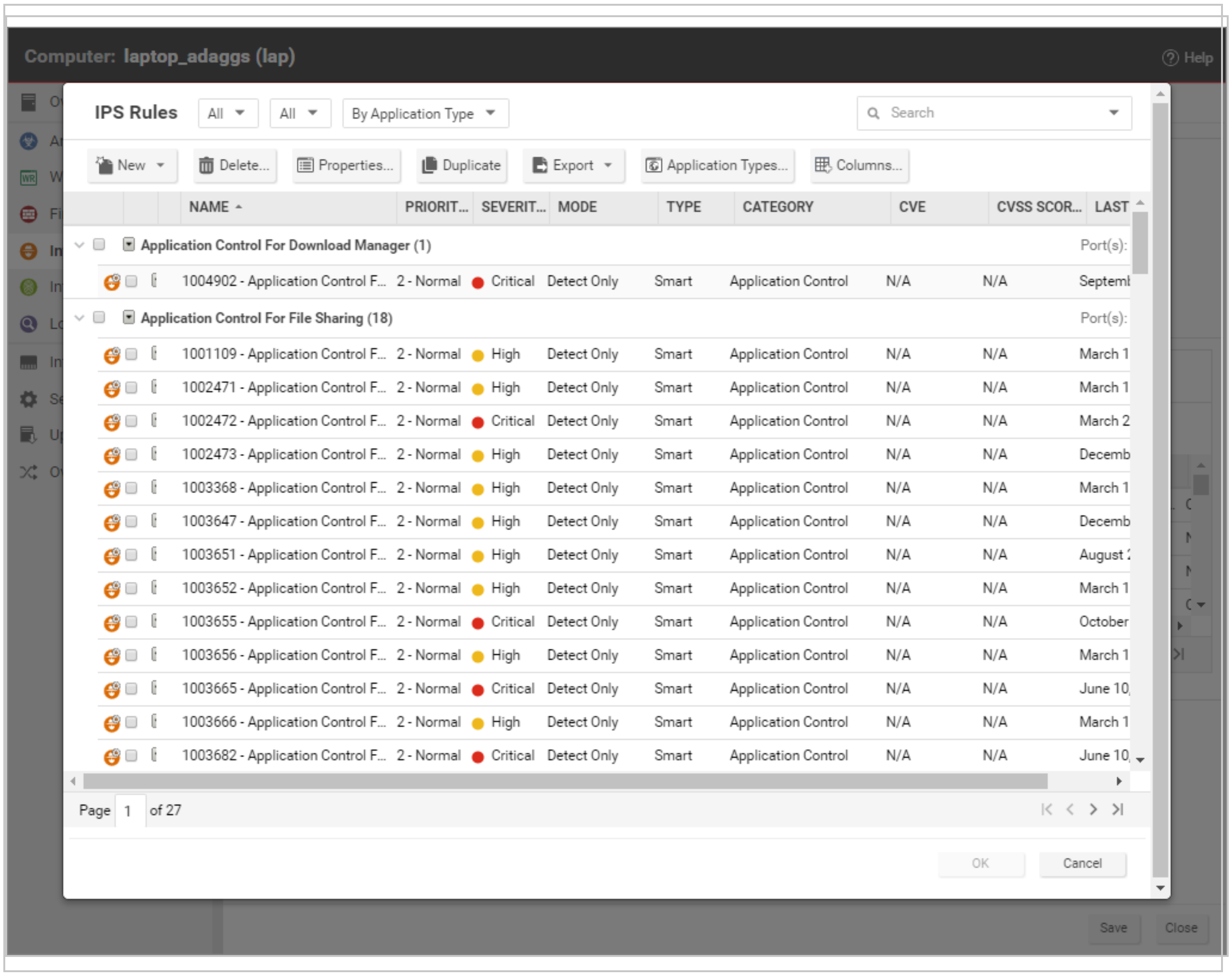
Although recommendation scans are performed for a specific computer, you can assign the recommendations to a policy that the computer uses.

For more information, see "Manage and run recommendation scans" on page 639.

1. Open the properties for the computer to scan. Run the recommendation scan as described in "Manually run a recommendation scan" on page 644.

   > **Note:** You can configure Deep Security to "Automatically implement recommendations" on page 645 scan results when it is appropriate to do so.

2. Open the policy to which you want to assign the rules, and complete the rule assignments as described in "Check scan results and manually assign rules" on page 646.



| NAME | PRIORIT... | SEVERIT... | MODE | TYPE | CATEGORY | CVE | CVSS SCOR... | LAST |
|---|---|---|---|---|---|---|---|---|
| Application Control For Download Manager (1) | | | | | | | | Port(s): |
| 1004902 - Application Control F... | 2 - Normal | ● Critical | Detect Only | Smart | Application Control | N/A | N/A | Septemb |
| Application Control For File Sharing (18) | | | | | | | | Port(s): |
| 1001109 - Application Control F... | 2 - Normal | ● High | Detect Only | Smart | Application Control | N/A | N/A | March 1 |
| 1002471 - Application Control F... | 2 - Normal | ● High | Detect Only | Smart | Application Control | N/A | N/A | March 1 |
| 1002472 - Application Control F... | 2 - Normal | ● Critical | Detect Only | Smart | Application Control | N/A | N/A | March 2 |
| 1002473 - Application Control F... | 2 - Normal | ● High | Detect Only | Smart | Application Control | N/A | N/A | Decemb |
| 1003368 - Application Control F... | 2 - Normal | ● High | Detect Only | Smart | Application Control | N/A | N/A | March 1 |
| 1003647 - Application Control F... | 2 - Normal | ● High | Detect Only | Smart | Application Control | N/A | N/A | Decemb |
| 1003651 - Application Control F... | 2 - Normal | ● High | Detect Only | Smart | Application Control | N/A | N/A | August 2 |
| 1003652 - Application Control F... | 2 - Normal | ● High | Detect Only | Smart | Application Control | N/A | N/A | March 1 |
| 1003655 - Application Control F... | 2 - Normal | ● Critical | Detect Only | Smart | Application Control | N/A | N/A | October |
| 1003656 - Application Control F... | 2 - Normal | ● High | Detect Only | Smart | Application Control | N/A | N/A | March 1 |
| 1003665 - Application Control F... | 2 - Normal | ● Critical | Detect Only | Smart | Application Control | N/A | N/A | June 10, |
| 1003666 - Application Control F... | 2 - Normal | ● High | Detect Only | Smart | Application Control | N/A | N/A | March 1 |
| 1003682 - Application Control F... | 2 - Normal | ● Critical | Detect Only | Smart | Application Control | N/A | N/A | June 10, |

Tip: To automatically and periodically fine tune your assigned Intrusion Prevention rules, you can schedule recommendation scans. See "Schedule Deep Security to perform tasks" on page 1600.

## Monitor your system

After you apply Intrusion Prevention rules, monitor system performance and Intrusion Prevention event logs.

### Monitor system performance

Monitor CPU, RAM, and network usage to verify that system performance is still acceptable. If not, you can modify some settings and deployment aspects to improve performance (see

"Performance tips for intrusion prevention" on page 848).

### Check Intrusion Prevention events

Monitor Intrusion Prevention events to ensure that rules are not matching legitimate network traffic. If a rule is causing false positives you can unassign the rule. (See "Assign and unassign rules" on page 814.)

To see Intrusion Prevention events, click **Events & Reports** > **Intrusion Prevention Events**.

## Enable 'fail open' for packet or system failures

The Intrusion Prevention module includes a network engine that might block packets before Intrusion Prevention rules can be applied. This might lead to downtime or performance issues with your services and applications. You can change this behavior so that packets are allowed through when system or internal packet failures occur. For details, see "Enable 'fail open' behavior" on page 854.

## Switch to Prevent mode

When you are satisfied that Intrusion Prevention is not finding false positives, configure your policy to use Intrusion Prevention in Prevent mode so that rules are enforced and related events are logged, as follows:

1. Go to **Computer or Policy editor**[1] **> Intrusion Prevention > General**.
2. For **Intrusion Prevention Behavior**, select **Prevent**.
3. Click **Save**.

## Implement best practices for specific rules

### HTTP Protocol Decoding rule

The HTTP Protocol Decoding rule is the most important rule in the Web Server Common application type. This rule decodes the HTTP traffic before the other rules inspect it. This rule also allows you to control various components of the decoding process.

This rule is required when you use any of the Web Application Common or Web Server Common rules that require it. Deep Security Manager automatically assigns this rule when it is required by other rules. As each web application is different, the policy that uses this rule should run in Detect

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

mode for a period of time before switching to Prevent mode to determine if any configuration changes are required.

Changes to the list of illegal characters are often required.

For more information, see the following:

- HTTP protocol decoding in Deep Security
- Modifying the list of URI characters that Deep Security Agent considers illegal
- Illegal character in URI error appears in Deep Security

#### Cross-site scripting and generic SQL injection rules

Two of the most common application-layer attacks are SQL injection and cross-site scripting (XSS). Cross-site scripting and SQL injection rules intercept the majority of attacks by default, but you may need to adjust the drop score for specific resources if they cause false positives.

Both rules are smart filters that need custom configuration for web servers. If you have output from a Web Application Vulnerability Scanner, you should leverage that information when applying protection. For example, if the user name field on the login.asp page is vulnerable to SQL injection, ensure that the SQL injection rule is configured to monitor that parameter with a low threshold to drop on.

For more information, see Understanding the Generic SQL Injection Prevention rule.

Apply NSX security tags

## Configure intrusion prevention rules

Perform the following tasks to configure and work with intrusion prevention rules:

- "See the list of intrusion prevention rules" on the next page
- "See information about an intrusion prevention rule" on the next page
- "See information about the associated vulnerability (Trend Micro rules only)" on page 814
- "Assign and unassign rules" on page 814
- "Automatically assign updated required rules" on page 815
- "Configure event logging for rules" on page 815
- "Generate alerts" on page 816
- "Setting configuration options (Trend Micro rules only)" on page 817

- "Schedule active times" on page 817
- "Exclude from recommendations" on page 818
- "Set the context for a rule" on page 818
- "Override the behavior mode for a rule" on page 819
- "Override rule and application type configurations" on page 819
- "Export and import rules" on page 820
- "Configure an SQL injection prevention rule" on page 820

For an overview of the intrusion prevention module, see "About Intrusion Prevention" on page 800.

## See the list of intrusion prevention rules

The Policies page provides a list of intrusion prevention rules. You can search for intrusion prevention rules, and open and edit rule properties. In the list, rules are grouped by application type, and some rule properties appear in different columns.

> Tip: The "TippingPoint" column contains the equivalent Trend Micro TippingPoint rule ID. In the Advanced Search for intrusion prevention, you can search on the TippingPoint rule ID. You can also see the TippingPoint rule ID in the list of assigned intrusion prevention rules in the policy and computer editor.

To see the list, click **Policies**, and then below **Common Objects/Rules** click **Intrusion Prevention Rules**.

## See information about an intrusion prevention rule

The properties of intrusion prevention rules include information about the rule and the exploit against which it protects.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.

### General Information

- **Name:** The name of the intrusion prevention rule.
- **Description:** The description of the intrusion prevention rule.

- **Minimum Agent/Appliance Version:** The minimum version of the Deep Security Agent or Appliance[1] required to support this intrusion prevention rule.

**Details**

Clicking **New** () or **Properties** () displays the **Intrusion Prevention Rule Properties** window.

**Note:** Note the **Configuration** tab. Intrusion Prevention Rules from Trend Micro are not directly editable through Deep Security Manager. Instead, if the Intrusion Prevention Rule requires (or allows) configuration, those configuration options will be available on the **Configuration** tab. Custom Intrusion Prevention Rules that you write yourself will be editable, in which case the **Rules** tab will be visible.

## See the list of intrusion prevention rules

The Policies page provides a list of intrusion prevention rules. You can search for intrusion prevention rules, and open and edit rule properties. In the list, rules are grouped by application type, and some rule properties appear in different columns.

**Tip:** The "TippingPoint" column contains the equivalent Trend Micro TippingPoint rule ID. In the Advanced Search for intrusion prevention, you can search on the TippingPoint rule ID. You can also see the TippingPoint rule ID in the list of assigned intrusion prevention rules in the policy and computer editor.

To see the list, click **Policies**, and then below **Common Objects/Rules** click **Intrusion Prevention Rules**.

## General Information

- **Application Type:** The application type under which this intrusion prevention rule is grouped.

[1] The Deep Securty Agent and Deep Security Virtual Appliance are the components that enforce the Deep Security policies that you have defined. Agents are deployed directly on a computer. Appliances are used in VMware vSphere environments to provide agentless protection. They are not available with Deep Security as a Service.

> Tip: You can edit application types from this panel. When you edit an application type from here, the changes are applied to all security elements that use it.

- **Priority:** The priority level of the rule. Higher priority rules are applied before lower priority rules.
- **Severity:** Setting the severity of a rule has no effect on how the rule is implemented or applied. Severity levels can be useful as sorting criteria when viewing a list of intrusion prevention rules. More importantly, each severity level is associated with a severity value; this value is multiplied by a computer's Asset Value to determine the Ranking of an Event. (See **Administration > System Settings > Ranking**.)
- **CVSS Score:** A measure of the severity of the vulnerability according the National Vulnerability Database.

#### Identification (Trend Micro rules only)

- **Type:** Can be either Smart (one or more known and unknown (zero day) vulnerabilities), Exploit (a specific exploit, usually signature based), or Vulnerability (a specific vulnerability for which one or more exploits may exist).
- **Issued:** The date the rule was released. This does not indicate when the rule was downloaded.
- **Last Updated:** The last time the rule was modified either locally or during Security Update download.
- **Identifier:** The rule's unique identification tag.

## See information about the associated vulnerability (Trend Micro rules only)

Rules that Trend Micro provides can include information about the vulnerability against which the rule protects. When applicable, the Common Vulnerability Scoring System (CVSS) is displayed. (For information on this scoring system, see the CVSS page at the National Vulnerability Database.)

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Click the **Vulnerabilities** tab.

## Assign and unassign rules

To apply intrusion prevention rules during agent scans, you assign them to the appropriate policies and computers. When the rule is no longer necessary because the vulnerability has been patched you can unassign the rule.

If you cannot unassign intrusion prevention rules from a **Computer editor**[1], it is likely because the rules are currently assigned in a policy. Rules assigned at the policy level must be removed using the **Policy editor**[2] and cannot be removed at the computer level.

When you make a change to a policy, it affects all computers using the policy. For example, when you unassign a rule from a policy you remove the rule from all computers that are protected by that policy. To continue to apply the rule to other computers, create a new policy for that group of computers. (See "Policies, inheritance, and overrides" on page 634.)

Tip: To see the policies and computers to which a rule is assigned, see the Assigned To tab of the rule properties.

1. Go to the **Policies** page, right-click the policy to configure and click **Details**.
2. Click **Intrusion Prevention > General**.
   The list of rules that are assigned to the policy appear in the **Assigned Intrusion Prevention Rules** list.
3. Under **Assigned Intrusion Prevention Rules**, click **Assign/Unassign**.
4. To assign a rule, select the check box next to the rule.
5. To unassign a rule, deselect the check box next to the rule.
6. Click **OK**.

## Automatically assign updated required rules

Security updates can include new or updated application types and intrusion prevention rules which require the assignment of secondary intrusion prevention rules. Deep Security can automatically assign these rules if they are required. You enable these automatic assignments in the the policy or computer properties.

1. Go to the **Policies** page, right-click the policy to configure and click **Details**.
2. Click **Intrusion Prevention > Advanced**.
3. To enable the automatic assignments, in the **Rule Updates** area, select **Yes**.
4. Click **OK**.

## Configure event logging for rules

Configure whether events are logged for a rule, and whether to include packet data in the log.

[1] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2] To open the Policy editor, go to the Policies page and double-click the policy that you want to edit (or select the policy and click Details).

**Note:** Deep Security can display X-Forwarded-For headers in intrusion prevention events when they are available in the packet data. This information can be useful when the Deep Security Agent is behind a load balancer or proxy. The X-Forwarded-For header data appears in the event's Properties window. To include the header data, include packet data in the log. In addition, rule 1006540 " Enable X-Forwarded-For HTTP Header Logging" must be assigned.

Because it would be impractical to record all packet data every time a rule triggers an event, Deep Security records the data only the first time the event occurs within a specified period of time. The default time is five minutes, however you can change the time period using the "Period for Log only one packet within period" property of a policy's Advanced Network Engine settings. (See Advanced Network Engine Options.)

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" on page 819.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. On the General tab, go to the Events area and select the desired options:
   - To disable logging for the rule, select **Disable Event Logging**.
   - To log an event when a packet is dropped or blocked, select **Generate Event on Packet Drop**.
   - To include the packet data in the log entry, select **Always Include Packet Data**.
   - To log several packets that precede and follow the packet that the rule detected, select **Enable Debug Mode**.Use debug mode only when your support provider instructs you to do so.

Additionally, to include packet data in the log, the policy to which the rule is assigned must allow rules to capture packet data:

1. On the Policies page, open the policy that is assigned the rule.
2. Click **Intrusion Prevention > Advanced**.
3. In the **Event Data** area, select **Yes**.

## Generate alerts

Generate an alert when an intrusion prevention rule triggers an event.

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" on page 819.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Click the Options tab, and in the **Alert** area select **On**.
4. Click **OK**.

## Setting configuration options (Trend Micro rules only)

Some intrusion prevention rules that Trend Micro provides have one or more configuration options such as header length, allowed extensions for HTTP, or cookie length. Some options require you to configure them. If you assign a rule without setting a required option, an alert is generated that informs you about the required option. (This also applies to any rules that are downloaded and automatically applied by way of a Security Update.)

Intrusion prevention rules that have configuration options appear in the Intrusion Prevention Rules list with a small gear over their icon .

**Note:** Custom intrusion prevention rules that you write yourself include a **Rules** tab where you can edit the rules.

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" on page 819.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Click the **Configuration** tab.
4. Configure the properties and then click **OK**.

## Schedule active times

Schedule a time during which an intrusion prevention rule is active. Intrusion prevention rules that are active only at scheduled times appear in the Intrusion Prevention Rules page with a small clock over their icon .

**Note:** With Agent-based protection, schedules use the same time zone as the endpoint operating system. With Agentless protection, schedules use the same time zone as the Deep Security Virtual Appliance.

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" on the next page.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Click the **Options** tab.
4. In the **Schedule** area, select **New** or select a frequency.
5. Edit the schedule as required.
6. Click **OK**.

## Exclude from recommendations

Exclude intrusion prevention rules from rule recommendations of recommendation scans.

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" on the next page.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Click the **Options**tab.
4. In the **Recommendations Options** area, select **Exclude from Recommendations**.
5. Click **OK**.

## Set the context for a rule

Set the context in which the rule is applied.

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" on the next page.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Click the **Options** tab.
4. In the **Context** area, select **New** or select a context.

5. Edit the context as required.
6. Click **OK**.

## Override the behavior mode for a rule

Set the behavior mode of an intrusion prevention rule to Detect when testing new rules. In Detect mode, the rule creates a log entry prefaced with the words "detect only:" and does not interfere with traffic. Some intrusion prevention rules are designed to operate only in Detect mode. For these rules, you cannot change the behavior mode.

> **Note:** If you disable logging for the rule, the rule activity is not logged regardless of the behavior mode.

For more information about behavior modes, see "Use behavior modes to test rules" on page 802.

The configuration performed in the following procedure affects all policies. For information about configuring a rule for one policy, see "Override rule and application type configurations" below.

1. Click **Policies > Intrusion Prevention Rules**.
2. Select a rule and click **Properties**.
3. Select **Detect Only**.

## Override rule and application type configurations

From a **Computer or Policy editor**[1] , you can edit an intrusion prevention rule so that your changes apply only in the context of the policy or computer. You can also edit the rule so that the changes apply globally so that the changes affect other policies and computers that are assigned the rule. Similarly, you can configure application types for a single policy or computer, or globally.

1. Go to the **Policies** page, right-click the policy to configure and click **Details**.
2. Click **Intrusion Prevention**.
3. To edit a rule, right-click the rule and select one of the following commands:
   - **Properties**: Edit the rule only for the policy.
   - **Properties (Global)**: Edit the rule globally, for all policies and computers.
4. To edit the application type of a rule, right-click the rule and select one of the following commands:

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

- **Application Type Properties**: Edit the application type only for the policy.
- **Application Type Properties (Global)**: Edit the application type globally, for all policies and computers.

5. Click **OK**.

Tip: When you select the rule and click Properties, you are editing the rule only for the policy that you are editing.

Note: You cannot assign one port to more than eight application types. If they are, the rules will not function on that port.

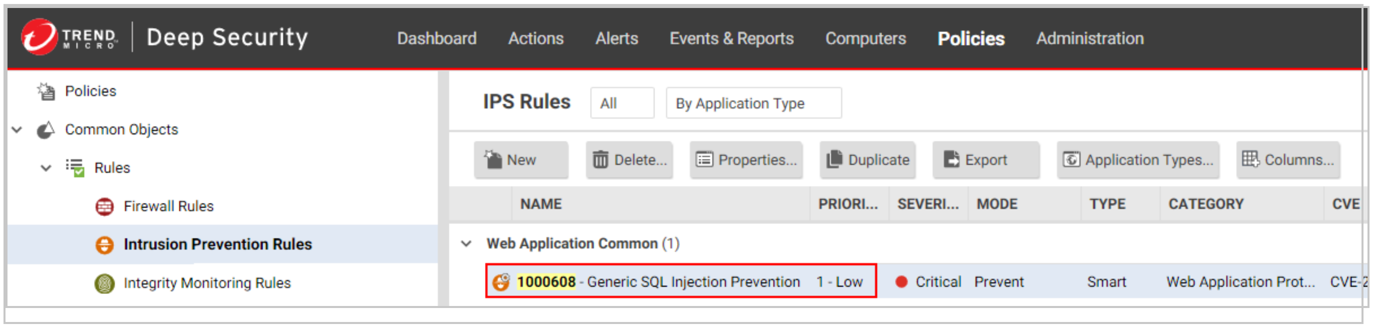
### Export and import rules

You can export one or more intrusion prevention rules to an XML or CSV file, and import rules from an XML file.

1. Click **Policies > Intrusion Prevention Rules**.
2. To export one or more rules, select them and click **Export > Export Selected to CSV** or **Export > Export Selected to XML**.
3. To export all rules, click **Export > Export to CSV** or **Export > Export to XML**.
4. To import rules, click **New > Import From File** and follow the instructions on the wizard.

## Configure an SQL injection prevention rule

Deep Security's intrusion prevention module includes a built-in rule that detects SQL injection attacks and drops the connection or logs it depending on its characteristics. The rule is called **1000608 - Generic SQL Injection Prevention** and can be configured to suit your organization's needs. For example, you can change the sensitivity of the rule by modifying the drop threshold.



| NAME | PRIORI... | SEVERI... | MODE | TYPE | CATEGORY | CVE |
|---|---|---|---|---|---|---|
| Web Application Common (1) | | | | | | |
| 1000608 - Generic SQL Injection Prevention | 1 - Low | ● Critical | Prevent | Smart | Web Application Prot... | CVE-2 |

Topics in this article:

## What is an SQL injection attack?

An SQL injection attack, or SQL phishing attack, is a method of attacking data-driven applications wherein an attacker includes portions of SQL statements in an entry field. The newly-formed rogue SQL command is passed by the website to your database where it is executed. The command can result in the attacker being able to read, add, delete, or change information in the database.

## What are common characters and strings used in SQL injection attacks?

Here are some commonly used characters and strings. The list is not exhaustive.

- ('
- %27
- \x22
- %22
- char
- ;
- ascii
- %3B
- %2B
- --
- %2D%2D
- /*
- %2F%2A
- */
- %2A%2F
- substring

- drop table
- drop+table
- insert into
- insert+into
- version(
- values
- group by
- group+by
- create table
- create+table
- delete
- update
- bulk insert
- bulk+insert
- load_file
- shutdown
- union
- having
- select
- declare
- exec
- and
- or
- like
- @@hostname
- @@tmpdir
- is null
- is+null
- is not null
- is+not+null
- %3D

- CONCAT
- %40%40basedir
- version%28,user(
- user%28,system_user(
- (,%28,)
- %29
- @
- %40
- cast

## How does the Generic SQL Injection Prevention rule work?

To detect SQL injection attacks, the Generic SQL Injection Prevention rule uses a scoring system. It works like this:

1. Packets from your application arrive at the Deep Security Agent for analysis.
2. The Generic SQL Injection Prevention rule looks at the packets and determines whether any of the strings shown in the table below are present. Notice that the strings are separated by commas and divided into ten groups.
3. If strings are found, a score is calculated as follows:
   - If a single string is found, then the score associated with its group constitutes the total score.
   - If multiple strings are found in *different* groups, then the scores of those groups are added together.
   - If multiple strings are found in the *same* group, then the score of that group is counted only once.
     See "Examples of the rule and scoring system in action" on the next page for clarification.
4. Using the total score, Deep Security determines whether to drop the connection or log it. If the total score exceeds the **Drop Threshold** score, then the connection is dropped, and if it exceeds the **Log Threshold** score, then it is logged.

**Note:** Trend Micro frequently updates its rules, so the strings in the table below might not match exactly the ones in Deep Security Manager.

**Note:** The use of '`\W`' in the lines below means 'followed by a non-alphanumeric character'.

| Group | Score |
|---|---|
| drop table,drop+table,insert into,insert+into,values\W,create table,create+table,delete\W,update\W,bulk insert,bulk+insert,shutdown\W,from\W | 2 |
| declare\W,select\W | 2 |
| cast\W,exec\W,load_file | 2 |
| union\W,group by,group+by,order by,order+by,having\W | 2 |
| and\W,or\W,like\W,is null,is+null,is not null,is+not+null,where\W | 1 |
| --,%2D%2D,/*,%2F%2A,*/,%2A%2F | 1 |
| ',%27,\x22,%22,char\W | 1 |
| ;,%3B | 1 |
| %2B,CONCAT\W | 1 |
| %3D | 1 |
| (,%28,),%29,@,%40 | 1 |
| ascii,substring | 1 |
| version(,version%28,user(,user%28,system_user(,system_user%28,database(,database%28,@@hostname,%40%40hostname,@@basedir,%40%40basedir,@@tmpdir,%40%40tmpdir,<br>@@datadir,%40%40datadir | 2 |

## Examples of the rule and scoring system in action

Below are some examples of how the scores are tallied and what actions are undertaken in each scenario.

### Example 1: Logged and dropped traffic

Let's assume you are using this rule configuration (where the score for the group comes after the colon (":")):

```
drop table,drop+table,insert into,insert+into,values\W,create
table,create+table,delete\W,update\W,bulk
insert,bulk+insert,shutdown\W,from\W:2
declare\W,select\W:2
cast\W,exec\W,load_file:2
union\W,group by,group+by,order by,order+by,having\W:2
and\W,or\W,like\W,is null,is+null,is not null,is+not+null,where\W:1
--,%2D%2D,/*,%2F%2A,*/,%2A%2F:1
',%27,\x22,%22,char\W:1
;,%3B:1
%2B,CONCAT\W:1
%3D:1
(,%28,),%29,@,%40:1
ascii,substring:1
version(,version%28,user(,user%28,system_user(,system_user%28,databas
(,database%28,@@hostname,%40%40hostname,@@basedir,%40%40basedir,@@tmpdir,%40
%40tmpdir,@@datadir,
%40%40datadir:2

Log Threshold: 3
Drop Threshold: 4
```

And this attack string is encountered:

`productID=BB10735166+UNION/**/+SELECT+FROM+user`

Then the total score is 5 (2+1+0+2) because:

- The string `UNION/` matches the fourth group for a score of 2.
- The string `/*` matches the sixth group for a score of 1.
- The string `*/` matches the sixth group for a score of 0 (because the score of the sixth group has already been counted).
- The string `SELECT+` matches the second group for a score of 2.

With a total score of 5, a log is generated and the traffic is dropped.

#### Example 2: No logged or dropped traffic

Let's assume you are using this rule configuration (where the `select\W` string has been moved to the same line as `union\W`):

```
drop table,drop+table,insert into,insert+into,values\W,create
table,create+table,delete\W,update\W,bulk
insert,bulk+insert,shutdown\W,from\W:2
declare\W:2
cast\W,exec\W,load_file:2
union\W,select\W,group by,group+by,order by,order+by,having\W:2
and\W,or\W,like\W,is null,is+null,is not null,is+not+null,where\W:1
--,%2D%2D,/*,%2F%2A,*/,%2A%2F:1
',%27,\x22,%22,char\W:1
;,%3B:1
%2B,CONCAT\W:1
%3D:1
(,%28,),%29,@,%40:1
ascii,substring:1
version(,version%28,user(,user%28,system_user(,system_user%28,databas
(,database%28,@@hostname,%40%40hostname,@@basedir,%40%40basedir,@@tmpdir,
%40%40tmpdir,@@datadir,%40%40datadir:2

Log Threshold: 3
Drop Threshold: 4
```

And this attack string is encountered:

`productID=BB10735166+UNION/**/+SELECT+FROM+user`

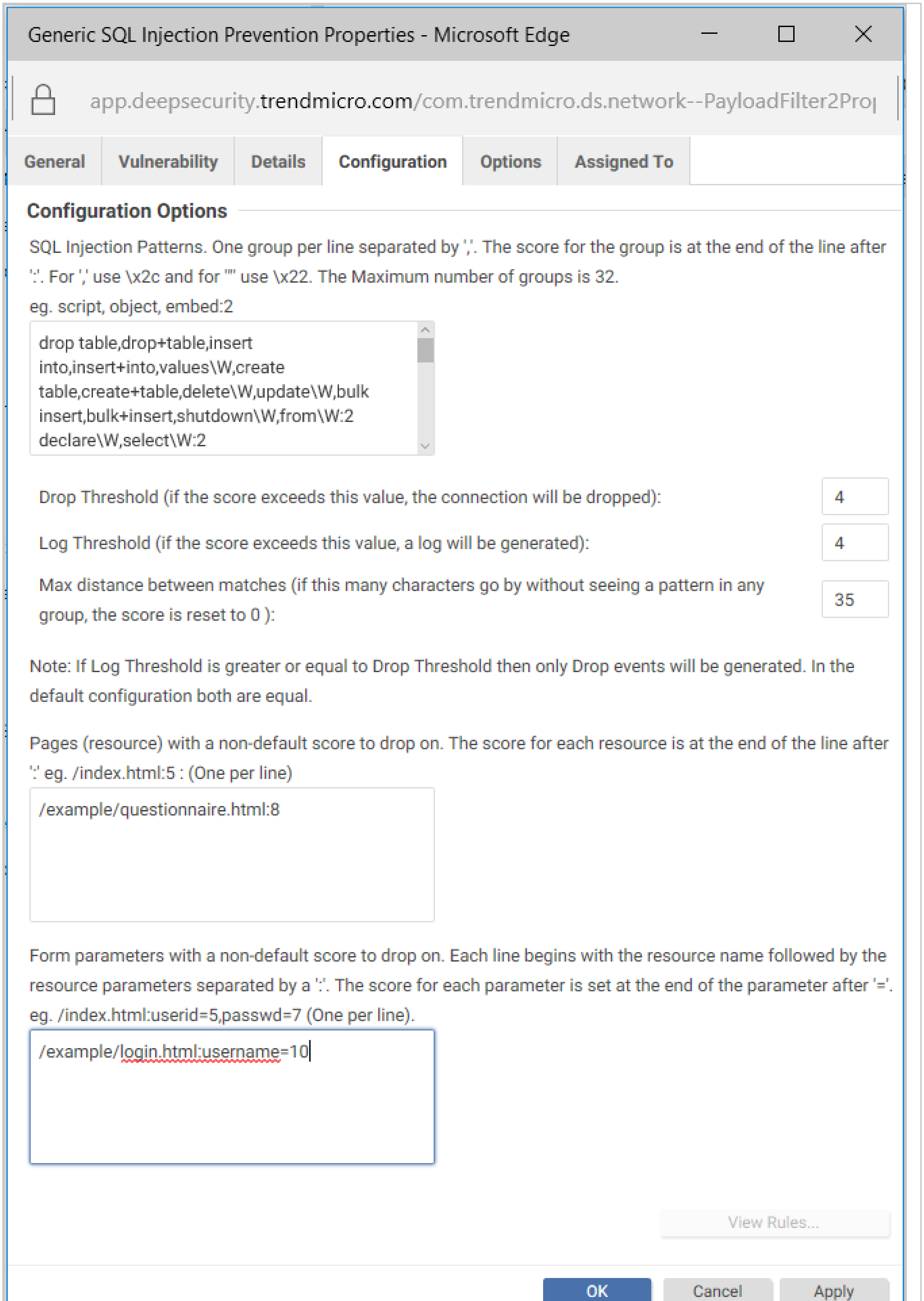
Then the total score is 3 (2+1+0+0) because:

- The string `UNION/` matches the fourth group for a score of 2.
- The string `/*` matches the sixth group for a score of 1.
- The string `*/` matches the sixth group for a score of 0 (because the score of the sixth group has already been counted).
- The string `SELECT+` matches the fourth group for a score of 0 (because the score of the fourth group has already been counted).

With a total score of 3, no log is generated and no traffic is dropped. The score must *exceed* the thresholds for them to take effect.

## Configure the Generic SQL Injection Prevention rule

You can configure the Generic SQL Injection Prevention rule to suit your organization's needs. The configurable options are shown in the image below.



Generic SQL Injection Prevention Properties - Microsoft Edge
app.deepsecurity.trendmicro.com/com.trendmicro.ds.network--PayloadFilter2Pro
General
Vulnerability
Details
Configuration
Options
Assigned To

Configuration Options

SQL Injection Patterns. One group per line separated by ','. The score for the group is at the end of the line after ':'. For ',' use \x2c and for '"' use \x22. The Maximum number of groups is 32.

eg. script, object, embed:2

```
drop table,drop+table,insert
into,insert+into,values\W,create
table,create+table,delete\W,update\W,bulk
insert,bulk+insert,shutdown\W,from\W:2
declare\W,select\W:2
```

Drop Threshold (if the score exceeds this value, the connection will be dropped): 4

Log Threshold (if the score exceeds this value, a log will be generated): 4

Max distance between matches (if this many characters go by without seeing a pattern in any group, the score is reset to 0 ): 35

Note: If Log Threshold is greater or equal to Drop Threshold then only Drop events will be generated. In the default configuration both are equal.

Pages (resource) with a non-default score to drop on. The score for each resource is at the end of the line after ':' eg. /index.html:5 : (One per line)

```
/example/questionnaire.html:8
```

Form parameters with a non-default score to drop on. Each line begins with the resource name followed by the resource parameters separated by a ':'. The score for each parameter is set at the end of the parameter after '='. eg. /index.html:userid=5,passwd=7 (One per line).

```
/example/login.html:username=10
```

To configure the rule:

1. Log in to Deep Security Manager.
2. At the top, click **Policies**.
3. In the search box on the right, enter `1000608` which is the Generic SQL Injection Prevention rule's numeric identifier. Press Enter. The rule appears in the main pane.
4. Double-click the rule.
5. Click the **Configuration** tab. You see the SQL injection pattern in the text box at the top.
6. Update the SQL injection pattern with the latest version, if you haven't customized it yet. To update to the latest pattern, go to the **Details** tab, copy the text under the **Default SQL Pattern** heading and paste it into the **SQL Injection Patterns** text box on the **Configuration** tab. You are now working with the most up-to-date pattern from Trend Micro.
7. Edit the fields as follows:
   - **SQL Injection Patterns**: This is where you to specify the list of characters and strings used in SQL injection attacks. Characters and strings are grouped and assigned a score. If you want to add or change the strings, make sure to use the proper encoding. See "Character encoding guidelines" on the next page below for details.
   - **Drop Threshold**: This is where you specify the drop score. The connection is dropped when the score exceeds this threshold. (If the score equals the drop threshold, the connection is maintained.) The default is `4`.
   - **Log Threshold**: This is where you specify the log score. The connection is logged when the score exceeds this threshold. (If the score equals the log threshold, nothing is logged.) The default is `4`.
   - **Max distance between matches**: This is where you specify the number of bytes that can pass without a match to reset the score to `0`. The default is `35`.
   - **Note:** Consider using the next two options to create overrides for pages and fields that might cause the normal thresholds to be exceeded.
   - **Pages (resource) with a non-default score to drop on**: This is where you can override the **Drop Threshold** for specific resources. For example, if your **Drop Threshold** is `4`, but you want a drop score of `8` for a questionnaire page, specify `/example/questionnaire.html:8`. With this configuration, `/example/questionnaire.html` needs to have a score *higher than* `8` in order for the connection to be dropped, while all other resources only need a score higher than `4`. Specify each resource on a separate line.
   - **Form parameters with a non-default score to drop on**: This is where you can override the thresholds defined in **Drop Threshold** or the **Pages (resources)with a non-default**

**score to drop on** fields for specific form fields. For example, if your **Drop Threshold** score is `4`, but you want a higher drop score of `10` for a username field, specify `/example/login.html:username=10`, where `/example/login.html` is replaced with the path and name of the page where the username field appears, and `username` is replaced with the username field used by your application. With this configuration, the username field needs to have a score *higher than* `10` for the connection to be dropped, while the page itself only needs a score higher than `4`. Specify each form field on a separate line.

> **Note:** The **Log Threshold** does not take effect when connections are dropped due to a match on the **Pages (resources) with a non-default score to drop on** or **Form parameters with a non-default score to drop on** fields. For example, if you set the form parameter field to `/example/login.html:username=10`, and the username field scores `11`, the connection is dropped but there is no log of this event.

8. Click **OK**.

You have now configured the Generic SQL Injection Prevention rule.

## Character encoding guidelines

If you want to change or add strings to the Generic SQL Injection Prevention rule, you must encode them properly. For example, if you want to use the quote character `'` in your pattern, you must enter `\x22`.

The table below shows characters and their encoded equivalents, as well as character classes that you can use to denote extended patterns.

| Enter this string... | To denote... |
|---|---|
| \a<br>\A | alphabetic characters, a-z A-Z<br>non-alphabetic characters<br>example: `delete\a` means "the word 'delete' followed by alphabetical characters" |
| \w<br>\W | alphanumeric characters, a-z A-Z 0-9<br>non-alphanumeric characters |

| Enter this string... | To denote... |
|---|---|
| | example: `delete\W` means "the word 'delete' followed by non-alphanumeric characters" |
| \d<br>\D | digits 0-9<br>non-digit characters<br>example: `delete\d` means "the word 'delete' followed by digits between zero and nine" |
| \s<br>\S | whitespace<br>not whitespace [\r,\n,\t,0x32]<br>example: `delete\S` means "the word 'delete' followed by non-whitespace" |
| \p<br>\P | punctuation character, printable ascii other than above<br>non-punctuation character<br>example: `delete\p` means "the word 'delete' followed by a punctuation character or printable ascii" |
| \c<br>\C | control character, below 32, or greater than or equal to 127, not including whitespace<br>non-control character<br>You can find details on control characters here. |
| \. | any |
| \xDD | hex byte 0xDD |
| \x2c | comma character (,) |
| \x22 | double-quotes character (") |
| \\ | escaped backslash (\) |

<table>
<tr><th>Enter this string...</th><th>To denote...</th></tr>
<tr><td>\|</td><td>escaped pipe (|)</td></tr>
<tr><td>|xx xx xx...|</td><td>hex pipe (byte sequence)</td></tr>
</table>

## Application types

The applications defined by Application Types are identified by the direction of traffic, the protocol being used, and the port number through which the traffic passes. Application Types are useful for grouping intrusion prevention rules.that have a common purpose. Rule groups simplify the process of selecting a set of intrusion prevention rules to assign to a computer. For example, consider the set of rules required to protect HTTP traffic to an Oracle Report Server. Simply select the rules in the "Web Server Common" and "Web Server Oracle Report Server" application types and then exclude unneeded rules, such as the rules that are specific to IIS servers.

### See a list of application types

Open the list of application types where you can see the properties of existing application types, as well as configure, export, and duplicate them. You can export to XML or CSV files. You can import XML files. You can also create and delete application types.

1. Click **Policies > Intrusion Prevention Rules**.
2. Click **Application Types**.
3. To apply a command to an application type, select the type and click the appropriate button.

Tip: Application types that have configurable properties have an icon with a gear.

See also "Override rule and application type configurations" on page 819.

### General Information

The name and description of the Application Type. "Minimum Agent/Appliance Version" tells you what version of the Deep Security **agent or appliance**[1] is required to support this Application

[1] The Deep Securty Agent and Deep Security Virtual Appliance are the components that enforce the Deep Security policies that you have defined. Agents are deployed directly on a computer. Appliances are used in VMware vSphere environments to provide agentless protection. They are not available with Deep Security as a Service.

Type.

### Connection

- **Direction:** The direction of the initiating communication. That is, the direction of the first packet that establishes a connection between two computers. For example, if you wanted to define an Application Type for Web browsers, you would select "Outgoing" because it is the Web browser that sends the first packet to a server to establish a connection (even though you may only want to examine traffic traveling from the server to the browser). The Intrusion Prevention Rules associated with a particular Application Type can be written to examine individual packets traveling in either direction.
- **Protocol:** The protocol this Application Type applies to.
- **Port:** The port(s) this Application Type monitors. (*Not* the port(s) over which traffic is exclusively allowed.)

### Configuration

The **Configuration** tab displays options that control how Intrusion Prevention Rules associated with this Application Type behave. For example, the "Web Server Common" Application Type has an option to "Monitor responses from Web Server". If this option is deselected, Intrusion Prevention Rules associated with this Application Type will not inspect response traffic.

### Options

Items in the **Options** tab control how the Deep Security Manager uses and applies the Application Type. For example, most Application Types have an option to exclude them from Recommendation Scans. This means that if the "Exclude from Recommendations" options is selected, a Recommendation Scan will not recommend this Application Type and its associated Intrusion Prevention Rules for a computer even if the application in question is detected.

### Assigned To

The **Assigned To** tab lists the Intrusion Prevention Rules associated with this Application Type.

## Inspect TLS traffic

You can enable Advanced TLS Traffic Inspection for the Intrusion Prevention module.

Note that advanced TLS Traffic Inspection and SSL Inspection do not support compressed traffic.

On this page:

- Enable Advanced TLS Traffic Inspection
- Use Advanced TLS Traffic Inspection
- "Configure SSL inspection (legacy)" on the next page
- "Change port settings" on page 835
- "Use Intrusion Prevention when traffic is encrypted with Perfect Forward Secrecy (PFS)" on page 835
- Supported cipher suites
- "Supported protocols" on page 843

## Enable Advanced TLS Traffic Inspection

Advanced TLS Traffic Inspection offers the following benefits over the legacy SSL inspection implementation:

- It removes the need to configure TLS credentials manually.
- It supports more ciphers than SSL inspection, including Perfect Forward Secrecy (PFS) ciphers. For more information, see Supported cipher suites.

With the Intrusion Prevention module enabled, Advanced TLS Traffic Inspection is applied by default to both inbound and outbound traffic:

- **Inspect Inbound TLS/SSL Traffic** is enabled by default for inbound traffic.
- **Inspect Outbound TLS/SSL Traffic** is enabled by default for outbound traffic and is supported by the Deep Security Agent release 20.0.1-12510 (20 LTS Update 2024-06-19) or later.

To verify or adjust these settings, as well as obtain guidance on the configuration steps for outbound traffic, navigate to **Policy > Intrusion Prevention > General > Advanced TLS Traffic Inspection**.

### Use Advanced TLS Traffic Inspection for inbound and outbound traffic

Advanced TLS Traffic Inspection can be enabled and used for inbound and outbound traffic on Windows and Linux platforms (see Supported features by platform).

On Windows, Advanced TLS Traffic Inspection only supports traffic using Windows-native TLS communication channels (see Secure Channel). For example, traffic produced by IIS, Microsoft Exchange, and Remote Desktop Protocol (RDP) is inspected. When Advanced TLS Traffic Inspection is enabled, a component called TMExtractor is activated to perform the necessary inspections. The TMExtractor file remains after DSA is uninstalled, but this file is automatically removed after a reboot.

On Linux, Advanced TLS Traffic Inspection only supports traffic by popular web applications: NGINX, Apache HTTP Server, HAProxy, and Tomcat server. Note that Tomcat server only supports OpenJDK 8 on Linux (64-bit) and runs without a container.

If you need to inspect TLS traffic that is not supported by Advanced TLS Traffic Inspection, or TLS traffic on other operating systems, you can configure the legacy SSL inspection instead.

## Configure SSL inspection (legacy)

You can configure SSL inspection for a given credential-port pair on one or more interfaces of your protected computer.

Credentials can be imported in PKCS#12 or PEM format. The credential file must include the private key. Windows computers can use CryptoAPI directly.

1. In Deep Security Manager, select the computer to configure and click **Details** to open the computer editor.
2. In the left pane of the computer editor, click **Intrusion Prevention > Advanced > View SSL Configurations,** and click **View SSL Configurations** to open the SSL computer Configurations window.
3. Click **New** to open the SSL Configuration wizard.
4. Specify the interface to which to apply the configuration on this computer:
   - To apply to all interfaces on this computer, select **All Interface(s)**.
   - To apply to specific interfaces, select **Specific Interface(s)**.
5. Select **Port(s)** or **Ports List** and select a list, then click **Next**.
6. On the IP Selection screen, select **All IPs** or provide a **Specific IP** on which to perform SSL inspection, then click **Next**.
7. On the Credentials screen, select how to provide the credentials:
   - **I will upload credentials now**
   - **The credentials are on the computer**

   **Note:** The credential file must include the private key.
8. If you chose the option to upload credentials now, enter their type, location, and pass phrase (if required).

   If the credentials are on the computer, provide Credential Details:

- If you are using PEM or PKCS#12 credential formats stored on the computer, identify the location of the credential file and the file's pass phrase (if required).
- If you are using Windows CryptoAPI credentials, choose the credentials from the list of credentials found on the computer.

9. Provide a name and description for this configuration.
10. Review the summary and close the SSL Configuration Wizard. Read the summary of the configuration operation and click **Finish** to close the wizard.

#### Change port settings

Change the port settings for the computer to ensure that the agent is performing the appropriate Intrusion Prevention filtering on the SSL-enabled ports. The changes you make are applied to a specific application type, such as Web Server Common, on the agent computer. The changes do not affect the application type on other computers.

1. Go to **Intrusion Prevention Rules** in the computer's Details window to see the list of Intrusion Prevention rules being applied on this computer.
2. Sort the rules by **Application Type** and locate the "Web Server Common" application type. (You can perform these changes to similar application types as well.)
3. Right-click a rule in the application type and click **Application Type Properties**.
4. Override the inherited "HTTP" Port List so that you include the port you defined during the SSL Configuration setup as well as port 80. Enter the ports as comma-separated values. For example, if you use port 9090 in the SSL configuration, enter 9090, 80.
5. To improve performance, on the **Configuration** tab, deselect **Inherited and Monitor responses from Web Server**.
6. Click **OK** to close the dialog.

### Use Intrusion Prevention when traffic is encrypted with Perfect Forward Secrecy (PFS)

Perfect Forward Secrecy (PFS) can be used to create a communication channel that cannot be decrypted if, at a later time, the server's private key is compromised. Since the intent of Perfect Forward Secrecy is to prevent decryption after the session is over, it also prevents the Intrusion Prevention module from seeing the traffic through SSL inspection.

**Note:**
Using Advanced TLS Traffic Inspection, the Intrusion Prevention module can analyze traffic encrypted with PFS ciphers without additional configuration.

To use PFS ciphers with SSL inspection instead, you can do the following:

1. Use Perfect Forward Secrecy for TLS traffic between the Internet and your load balancer or reverse proxy.
2. Terminate the Perfect Forward Secrecy session at your load balancer or reverse proxy.
3. Use a non-PFS cipher suite (see "Supported cipher suites" on the next page) for traffic between the load balancer (or reverse proxy) and the web server or application server, so that the Intrusion Prevention module on the server can decrypt the TLS sessions and inspect them.
4. Restrict traffic to the web server for application server ports that do not use Perfect Forward Secrecy.

### Special considerations for Diffie-Hellman ciphers when using SSL Inspection

Perfect Forward Secrecy relies on the Diffie-Hellman key exchange algorithm. On some web servers, Diffie-Hellman might be the default, which means that SSL inspection won't work properly. It is therefore important to check the server's configuration file and disable Diffie-Hellman ciphers for TLS traffic between the web server and load balancer (or reverse proxy). For example, to disable Diffie-Hellman on an Apache server:

1. Open the server's configuration file. The file name and location of web server configuration files vary by operating system (OS) and distribution. For example, the path could be:
   - **Default installation on RHEL4:** `/etc/httpd/conf.d/ssl.conf`
   - **Apache 2.2.2 on Red Hat Linux:** `/apache2/conf/extra/httpd-ssl.conf`
2. In the file, find the "`SSLCipherSuite`" variable.
3. Add `!DH:!EDH:!ADH:` to these fields, if this string does not already appear. (The "`!`" tells Apache to "not" use this cipher.)
4. For example, you might edit the Apache configuration file's cipher suite to look like this:

```
SSLCipherSuite
 !DH:!EDH:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
```

The preceding information only applies when using SSL Inspection instead of Advanced TLS Traffic Inspection.

For more information, see the Apache Documentation for `SSLCipherSuite`: http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite.

## Supported cipher suites

| Hex Value | OpenSSL Name | IANA Name | NSS Name | Advanced TLS Inspection | SSL inspection (legacy) |
|---|---|---|---|---|---|
| 0x00,0x04 | RC4-MD5 | TLS_RSA_WITH_RC4_128_MD5 | SSL_RSA_WITH_RC4_128_MD5 | ✓ | ✓ |
| 0x00,0x05 | RC4-SHA | TLS_RSA_WITH_RC4_128_SHA | SSL_RSA_WITH_RC4_128_SHA | ✓ | ✓ |
| 0x00,0x09 | DES-CBC-SHA | TLS_RSA_WITH_DES_CBC_SHA | SSL_RSA_WITH_DES_CBC_SHA | ✓ | ✓ |
| 0x00,0x0A | DES-CBC3-SHA | TLS_RSA_WITH_3DES_EDE_CBC_SHA | SSL_RSA_WITH_3DES_EDE_CBC_SHA | ✓ | ✓ |
| 0x00,0x2F | AES128-SHA | TLS_RSA_WITH_AES_128_CBC_SHA | TLS_RSA_WITH_AES_128_CBC_SHA | ✓ | ✓ |
| 0x00,0x33 | DHE-RSA-AES128-SHA | TLS_DHE_RSA_WITH_AES_128_CBC_SHA | TLS_DHE_RSA_WITH_AES_128_CBC_SHA | ✓ | |
| 0x00,0x35 | AES256-SHA | TLS_RSA_WITH_AES_256_CBC_SHA | TLS_RSA_WITH_AES_256_CBC_SHA | ✓ | ✓ |

| Hex Value | OpenSSL Name | IANA Name | NSS Name | Advanced TLS Inspection | SSL inspection (legacy) |
|---|---|---|---|---|---|
| 0x00,0x39 | DHE-RSA-AES256-SHA | TLS_DHE_RSA_WITH_AES_256_CBC_SHA | TLS_DHE_RSA_WITH_AES_256_CBC_SHA | ✓ | |
| 0x00,0x3C | AES128-SHA256 | TLS_RSA_WITH_AES_128_CBC_SHA256 | TLS_RSA_WITH_AES_128_CBC_SHA256 | ✓ | ✓ |
| 0x00,0x3D | AES256-SHA256 | TLS_RSA_WITH_AES_256_CBC_SHA256 | TLS_RSA_WITH_AES_256_CBC_SHA256 | ✓ | ✓ |
| 0x00,0x41 | CAMELLIA128-SHA | TLS_RSA_WITH_CAMELLIA_128_CBC_SHA | TLS_RSA_WITH_CAMELLIA_128_CBC_SHA | ✓ | ✓ |
| 0x00,0x67 | DHE-RSA-AES128-SHA256 | TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 | TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 | ✓ | |
| 0x00,0x6b | DHE-RSA-AES256-SHA256 | TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 | TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 | ✓ | |
| 0x00,0x84 | CAMELLIA256-SHA | TLS_RSA_WITH_ | TLS_RSA_WITH_ | ✓ | ✓ |

| Hex Value | OpenSSL Name | IANA Name | NSS Name | Advanced TLS Inspection | SSL inspection (legacy) |
|---|---|---|---|---|---|
| | | CAMELLIA_256_CBC_SHA | CAMELLIA_256_CBC_SHA | | |
| 0x00,0x9c | AES128-GCM-SHA256 | TLS_RSA_WITH_AES_128_GCM_SHA256 | TLS_RSA_WITH_AES_128_GCM_SHA256 | ✓ | ✓ |
| 0x00,0x9d | AES256-GCM-SHA384 | TLS_RSA_WITH_AES_256_GCM_SHA384 | TLS_RSA_WITH_AES_256_GCM_SHA384 | ✓ | ✓ |
| 0x00,0x9e | DHE-RSA-AES128-GCM-SHA256 | TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 | TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 | ✓ | |
| 0x00,0x9f | DHE-RSA-AES256-GCM-SHA384 | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 | ✓ | |
| 0x00,0xBA | CAMELLIA128-SHA256 | TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 | TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 | ✓ | ✓ |
| 0x00,0xC0 | CAMELLIA256- | TLS_RSA_ | TLS_RSA_ | ✓ | ✓ |

| Hex Value | OpenSSL Name | IANA Name | NSS Name | Advanced TLS Inspection | SSL inspection (legacy) |
|---|---|---|---|---|---|
| | SHA256 | WITH_CAMELLIA_256_CBC_SHA256 | WITH_CAMELLIA_256_CBC_SHA256 | | |
| 0xc0,0x09 | ECDHE-ECDSA-AES128-SHA | TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA | TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA | ✓ | |
| 0xC0,0x0A | ECDHE-ECDSA-AES256-SHA | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA | ✓ | |
| 0xc0,0x13 | ECDHE-RSA-AES128-SHA | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | ✓ | |
| 0xc0,0x14 | ECDHE-RSA-AES256-SHA | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA | ✓ | |
| 0xc0,0x23 | ECDHE-ECDSA-AES128-SHA256 | TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 | TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 | ✓ | |

| Hex Value | OpenSSL Name | IANA Name | NSS Name | Advanced TLS Inspection | SSL inspection (legacy) |
|---|---|---|---|---|---|
| 0xc0,0x24 | ECDHE-ECDSA-AES256-SHA384 | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 | TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 | ✓ | |
| 0xc0,0x27 | ECDHE-RSA-AES128-SHA256 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | ✓ | |
| 0xc0,0x28 | ECDHE-RSA-AES256-SHA384 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 | ✓ | |
| 0xc0,0x2b | ECDHE-ECDSA-AES128-GCM-SHA256 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 | TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 | ✓ | |
| 0xc0,0x2c | ECDHE-ECDSA-AES256-GCM-SHA384 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 | TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 | ✓ | |
| 0xc0,0x2f | ECDHE-RSA-AES128-GCM-SHA256 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ✓ | |

| Hex Value | OpenSSL Name | IANA Name | NSS Name | Advanced TLS Inspection | SSL inspection (legacy) |
|---|---|---|---|---|---|
| 0xc0,0x30 | ECDHE-RSA-AES256-GCM-SHA384 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 | ✓ | |
| 0xC0,0x9C | AES128-CCM | TLS_RSA_WITH_AES_128_CCM | TLS_RSA_WITH_AES_128_CCM | ✓ | ✓ |
| 0xC0,0x9D | AES256-CCM | TLS_RSA_WITH_AES_256_CCM | TLS_RSA_WITH_AES_256_CCM | ✓ | ✓ |
| 0xC0,0xA0 | AES128-CCM8 | TLS_RSA_WITH_AES_128_CCM_8 | TLS_RSA_WITH_AES_128_CCM_8 | ✓ | ✓ |
| 0xC0,0xA1 | AES256-CCM8 | TLS_RSA_WITH_AES_256_CCM_8 | TLS_RSA_WITH_AES_256_CCM_8 | ✓ | ✓ |
| 0xcc,0xa8 | ECDHE-RSA-CHACHA20-POLY1305 | TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 | TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 | ✓ | |
| 0xcc,0xa9 | ECDHE-ECDSA-CHACHA20-POLY1305 | TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_ | TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_ | ✓ | |

| Hex Value | OpenSSL Name | IANA Name | NSS Name | Advanced TLS Inspection | SSL inspection (legacy) |
|---|---|---|---|---|---|
| | | SHA256 | SHA256 | | |
| 0xcc,0xaa | DHE-RSA-CHACHA20-POLY1305 | TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 | TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 | ✓ | |

### Supported protocols

The following protocols are supported:

- TLS 1.0
- TLS 1.1
- TLS 1.2
- TLS 1.3 (Linux only)

SSL 3.0 inspection is **not** supported and is blocked by default.

## TLS inspection support

- Deep Security Agent 20 TLS inspection support

### Manage TLS inspection support package updates

This feature always updates the TLS inspection support package for supported platforms, but allows you to disable other unnecessary updates.

This feature requires:

- Deep Security Manager 20.0.665+
- Deep Security Agent 20.0.0.5512+ on supported platforms. It is not supported on AIX or Solaris.

For a list of supported platforms with **Advanced TLS traffic inspection** feature, see the "Supported features by platform" on page 425

#### Disable TLS inspection support package updates on a single agent

1. In Deep Security Manager, go to the **Computers** page.
2. Double-click the computer where you want to disable updates (or select the computer and then the **Details** button).
3. Select **Settings**. Change **Automatically update TLS inspection package for Advanced TLS Traffic Inspection** to **No**.
4. Save your changes.

#### Disable TLS inspection support package updates by policy

This method disables TLS inspection support package updates for all computers protected by the same policy.

1. In Deep Security Manager, go to the **Policies** page.
2. Double-click the policy where you want to disable updates (or select the policy and then the **Details** button). You can also create a new policy instead of updating an existing policy.
3. Select **Settings**. Change **Automatically update TLS inspection package for Advanced TLS Traffic Inspection** to **No**.
4. Save your changes.

## Configure anti-evasion settings

Anti-evasion settings control the network engine handling of abnormal packets that may be attempting to evade analysis. Anti evasion settings are configured in a policy or an individual computer. The Security Posture setting controls how rigorous intrusion prevention analyzes packets, and can be set to one of the following values:

- **Normal:** Prevents the evasion of intrusion prevention rules without false positives. This is the default value.
- **Strict:** Performs more stringent checking than Normal mode but can produce some false-positive results. Strict mode is useful for penetration testing but should not be enabled under normal circumstances.
- **Custom:** If you select **Custom**, additional settings are available that enable you to specify how Deep Security will handle issues with packets. For these settings (with the exception of **TCP Timestamp PAWS Window**), the options are **Allow** (Deep Security sends the packet through to the system), **Log Only** (same behavior as Allow, but an event is logged), **Deny**

(Deep Security drops the packet and logs an event), or **Deny Silent** (same behavior as Deny, but no event is logged):

> **Note:** If you changed the posture to "Custom" in Deep Security 10.1 or earlier, all default values for the anti-evasion settings were set to "Deny". This led to a dramatic increase in block events. The default custom values have changed in Deep Security 10.2, as indicated in the table below.

| Setting | Description | Normal value | Strict value | Default custom value (pre-10.2) | Default custom value (10.2 or later) |
|---|---|---|---|---|---|
| Invalid TCP Timestamps | Action to take when a TCP timestamp is too old | Ignore and Log (same function as Log Only) | Deny | Deny | Ignore and Log (same function as Log Only) |
| TCP Timestamp PAWS Window | Packets can have timestamps. When a timestamp has an earlier timestamp than the one that came before it, it can be suspicious. The tolerance for the difference in timestamps depends on the operating system. For Windows systems, select 0 (the system will only accept packets with a timestamp that is equal to or newer than the | 1 for Linux agents, otherwise 0 | 1 for Linux agents, otherwise 0 | 0 | 1 for Linux agents, otherwise 0 |

| Setting | Description | Normal value | Strict value | Default custom value (pre-10.2) | Default custom value (10.2 or later) |
|---|---|---|---|---|---|
| | previous packet). For Linux systems, select 1 (the system will accept packets with a timestamp that is a maximum of one second earlier than the previous packet). | | | | |
| Timestamp PAWS Zero Allowed | Action to take when a TCP timestamp is zero | Deny for Linux agents or NDIS5, otherwise Allow | Deny for Linux agents or NDIS5, otherwise Allow | Deny | Deny for Linux agents or NDIS5, otherwise Allow |
| Fragmented Packets | Action to take when a packet is fragmented | Allow | Allow | Deny | Allow |
| TCP Zero Flags | Action to take when a packet has zero flags set | Deny | Deny | Deny | Deny |
| TCP Congestion Flags | Action to take when a packet has congestion flags set | Allow | Allow | Deny | Allow |
| TCP Urgent Flags | Action to take when a packet has urgent flags set | Allow | Deny | Deny | Allow |
| TCP Syn Fin | Action to take | Deny | Deny | Deny | Deny |

| Setting | Description | Normal value | Strict value | Default custom value (pre-10.2) | Default custom value (10.2 or later) |
|---|---|---|---|---|---|
| Flags | when a packet has both SYN and FIN flags set | | | | |
| TCP Syn Rst Flags | Action to take when a packet has both SYN and RST flags set | Deny | Deny | Deny | Deny |
| TCP Rst Fin Flags | Action to take when a packet has both RST and FIN flags set | Deny | Deny | Deny | Deny |
| TCP Syn with Data | Action to take when a packet has a SYN flag set and also contains data | Deny | Deny | Deny | Deny |
| TCP Split Handshake | Action to take when a SYN is received instead of SYN-ACK, as a reply to a SYN. | Deny | Deny | Deny | Deny |
| RST Packet Out of Connection | Action to take for a RST packet without a known connection | Allow | Deny | Deny | Allow |
| FIN Packet Out of Connection | Action to take for a FIN packet without a known | Allow | Deny | Deny | Allow |

| Setting | Description | Normal value | Strict value | Default custom value (pre-10.2) | Default custom value (10.2 or later) |
|---|---|---|---|---|---|
| | connection | | | | |
| OUT Packet Out of Connection | Action to take for an outgoing packet without a known connection | Allow | Deny | Deny | Allow |
| Evasive Retransmit | Action to take for a packet with duplicated or overlapping data | Allow | Deny | Deny | Allow |
| TCP Checksum | Action to take for a packet with an invalid checksum | Allow | Deny | Deny | Allow |

## Performance tips for intrusion prevention

To improve system resources utilization on Deep Security Agent, optimize certain performance-related settings.

For an overview of the intrusion prevention module, see "About Intrusion Prevention" on page 800.

| System resource | Settings that impact performance |
|---|---|
| CPU usage | • Log an event when a packet is dropped or blocked. Logging packet modifications may result in a lot of log entries. (See "Configure event logging for rules" on page 815)<br>• Include packet data in the event log only during troubleshooting. (See "Configure event logging for rules" on page 815)<br>• Assign only intrusion prevention rules that apply to the computer's OS and applications. See "Manage and run recommendation scans" on |

| System resource | Settings that impact performance |
|---|---|
| | page 639 for information about using recommendation scans to discover applicable vulnerabilities and rules.<br>• Don't assign more than 300 rules. |
| Network usage or throughput | • Log an event when a packet is dropped or blocked. Logging packet modifications may result in a lot of log entries. (See "Configure event logging for rules" on page 815)<br>• Include packet data in the event log only during troubleshooting. (See "Configure event logging for rules" on page 815)<br>• Do not monitor HTTP responses from the web server, especially if the policy has many signatures applied:<br>a. Click **Policies > Intrusion Prevention Rules**.<br>b. Right-click a rule in the Web Server Common application type and click **Application Type Properties**.<br>c. On the **Configuration** tab, deselect **Inherited and Monitor responses from Web Server**. |
| Disk usage | • Include packet data in the event log only during troubleshooting. (See "Configure event logging for rules" on page 815) |

## Maximum size for configuration packages

When an agent is assigned a large number of intrusion prevention rules, the size of the configuration package can exceed the maximum allowed size. When the allowed size is exceeded, the status of the agent changes to "Agent configuration package too large" and the event message "Configuration package too large" appears.

**Note:** There is a configuration limit of 20 MB in Windows 32-bit platform because it has smaller kernel memory available. For other platforms, the limit is 32 MB.

For performance reasons, you should have less than 350 intrusion prevention rules assigned to a computer. To minimize the number of required rules, ensure all available patches are applied to the computer operation system and any third-party software that is installed.

1. Apply available patches to the computer operating system.
2. Apply available patches to any third-party software that is installed.
3. Apply only the intrusion prevention rules that a recommendation scan recommends. Remove any rules from the computer or the assigned policy that are recommended for unassignment. (See "Manage and run recommendation scans" on page 639.)
4. If you are managing intrusion prevention at the policy level and the configuration package is still too large, configure intrusion prevention in one of the following ways:
   - Make the policy more granular, so that all servers in that policy have the same operating system and applications.
   - Manage intrusion prevention at the server level so that rules are added and removed automatically for the computer.

Use the following procedure to manage intrusion prevention at the server level.

1. Open the editor for the policy that is assigned to the computer.
2. Click **Intrusion Prevention > General**.
3. In the **Recommendations** section, set **Automatically implement Intrusion Prevention Recommendations (when possible)** to **Yes**.
4. Remove any intrusion prevention rules from the policy.
5. Run a recommendation scan on the computer.

# Configure Firewall

## About Firewall

The firewall module provides bidirectional stateful inspection of incoming and outgoing traffic. Firewall rules define what actions to take on individual packets in that traffic. Packets can be filtered by IP and MAC address, port and packet flag across all IP-based protocols and frame types. The firewall module can also help prevent denial of service attacks and detect and prevent reconnaissance scans.

To enable and configure the firewall, see "Set up the Deep Security firewall" on the next page.

### Firewall rules

Firewall rules can process traffic using one of the following actions, listed in order of precedence:

- Bypass
- Log Only

- Force Allow
- Deny
- Allow

Rules also have a priority level between 4 (highest priority) to 0 (lowest priority). Within a specific priority level rules are processed in order based on the precedence of the action type of the rule as listed above. This means that unlike what you may have experienced when configuring other firewalls, the Deep Security firewall processes rules independently of their assignment order.

For more information on how rule priorities and actions determine processing order, see "Firewall rule actions and priorities" on page 871.

For more detailed information on how to create firewall rules, see "Create a firewall rule" on page 864.

**Note:** When creating your rules, make sure to test them using the Tap and Inline modes of the firewall module before deploying them. For information on how to do so, see the "Test firewall rules before deploying them" section of "Set up the Deep Security firewall" below.

## Set up the Deep Security firewall

The Deep Security Firewall is a highly flexible Firewall that you can configure to be restrictive or permissive. Like the intrusion prevention and web reputation modules, the Firewall module can also be run in two modes: inline or tap. It is recommended that you test your Firewall rules in tap mode and then switch to inline mode when everything is working correctly.

The configuration and administration of your Firewall must be performed carefully and there is no one set of rules that fits all environments. Make sure you understand the Firewall rule actions and rule priorities before creating your rules and proceed with extra caution when creating Allow rules because they implicitly deny everything else not defined.

In this article:

## Test Firewall rules before deploying them

The Firewall module (as well as the intrusion prevention and web reputation modules) includes a Deep Security network engine that decides whether to block or allow packets. For the Firewall and intrusion prevention modules, the network engine performs a packet sanity check and also makes sure each packet passes the Firewall and intrusion prevention rules. The network engine operates in one of two modes:

- **Tap mode**: Packet streams are not modified. The traffic is still processed by the Firewall and/or intrusion prevention modules, if they are enabled. However any issues detected do not result in packet or connection drops. When in Tap mode, Deep Security offers no protection beyond providing a record of events.
- **Inline mode**: Packet streams pass directly through the Deep Security network engine. All rules are applied to the network traffic before they proceed up the protocol stack.

It’s important to test your Firewall rules in either Tap mode or Inline mode with the action for the rules set to Log Only before deploying them. This allows you to preview the effect of the rules on traffic, without any action being taken. If rules aren’t properly tested before deployment, all traffic could become blocked and your computer could become inaccessible.

### Test in Tap mode

Tap mode allows you to test your Firewall rules, without disturbing the flow of traffic.

1. Go to **Computers** or **Policies** in the Deep Security Manager.
2. Right-click a computer (or policy) and select **Details** to open the **Computer or Policy editor**[1].
3. Go to **Settings > Advanced > Network Engine Mode**.
4. Select **Tap** from the list and click **Save**.
5. Create your rules and click **OK**. To check your rules, go to **Events & Reports > Events > Firewall Events.**

**Note:** It is not necessary to set the action of the rule to Log Only in Tap mode.

Once you are satisfied with your Firewall rules, go back to the **Computer or Policy editor**[2], select **Inline** from the drop-down list, and click **Save**.

### Test in Inline mode

In most situations, Tap mode is a good way to test your Firewall rules without disturbing traffic. However, you can also test your rules in Inline mode, if the action of the rule is set to Log Only. This way, the real world process of analyzing the traffic takes place without having to perform any action, such as blocking or denying packets.

1. Go to **Computers** or **Policies** in the Deep Security Manager.
2. Right-click a computer (or policy) and select **Details** to open the **Computer or Policy editor**[3].
3. Go to **Settings > Advanced > Network Engine Mode**.
4. Select **Inline** from the drop down menu and click **Save**.
5. While you're creating your rule, ensure the action is set to **Log Only.**
6. To check your rules, go to **Events & Reports > Events > Firewall Events**.

Once you are satisfied with your Firewall rules, change the action from Log Only to your desired action and click **OK**.

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[3] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

## Enable 'fail open' behavior

In some cases, the network engine blocks packets before the Firewall rules (or intrusion prevention rules) can be applied. By default, the network engine blocks packets if the:

- agent or virtual appliance has a system problem, such as if it's out of memory
- packet sanity check fails

This 'fail closed' behavior offers a high level of security: it ensures that cyber attacks cannot penetrate your network when an agent or virtual appliance is not functioning properly, and safeguards against potentially malicious packets. The disadvantage to 'fail closed' is that your services and applications might become unavailable because of problems on the agent or virtual appliance. You might also experience performance issues if a large number of packets are being dropped unnecessarily as a result of the packet sanity check (too many false-positives).

If you have concerns about service availability, consider changing the default behavior to allow packets through (or 'fail open') for system and packet check failures, as explained below.

1. Go to **Computers** or **Policies** in the Deep Security Manager.
2. Right-click a computer (or policy) and select **Details** to open the **Computer or Policy editor**[1].
3. Click **Settings** on the left.
4. Click the **Advanced** tab.
5. Under **Network Engine Settings**, set the **Failure Response** settings as follows:
6. Set **Network Engine System Failure** to **Fail open** to allow packets through if the Deep Security network engine experiences problems, such as out-of-memory failures, allocated memory failures, and network engine deep packet inspection (DPI) decoding failures. Consider using fail open here if your agent or virtual appliance frequently encounters network exceptions because of heavy loads or a lack of resources. With fail open, the network engine allows the packet through, does not perform Intrusion Prevention rules checking, and logs an event. Your services and applications remain available despite the problems on the agent or virtual appliance.
7. Set **Network Packet Sanity Check Failure** to **Fail open** to allow packets through that fail the network engine's packet sanity checks. Examples of packet sanity checks: Firewall sanity checks, network layer 2, 3, or 4 attribute checks, and TCP state checks. Consider using fail open here if you want to perform Intrusion Prevention rules checking only on

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

'good' packets that pass the sanity check. With fail open, the network engine allows the failed packet through, does not perform Intrusion Prevention rules checking on it, and logs an event.

8. Click **Save**.

You have now enabled fail open behavior for system or packet check failures.

## Turn on Firewall

To enable Firewall functionality on a computer:

1. In the **Computer or Policy editor**[1], go to **Firewall** > **General**.
2. With Deep Security Agent 11.1 and earlier, the Firewall module inspects traffic that passes through the host computer's network interface to containers. With Deep Security Agent 11.2 or later, it can also inspect traffic between containers. When the **Scan container network traffic** setting is set to **Yes**, Deep Security scans the traffic that goes through both containers and hosts. When it is set to **No**, Deep Security scans only the traffic that goes through the host network interface.
3. Select **On** and then click **Save**.

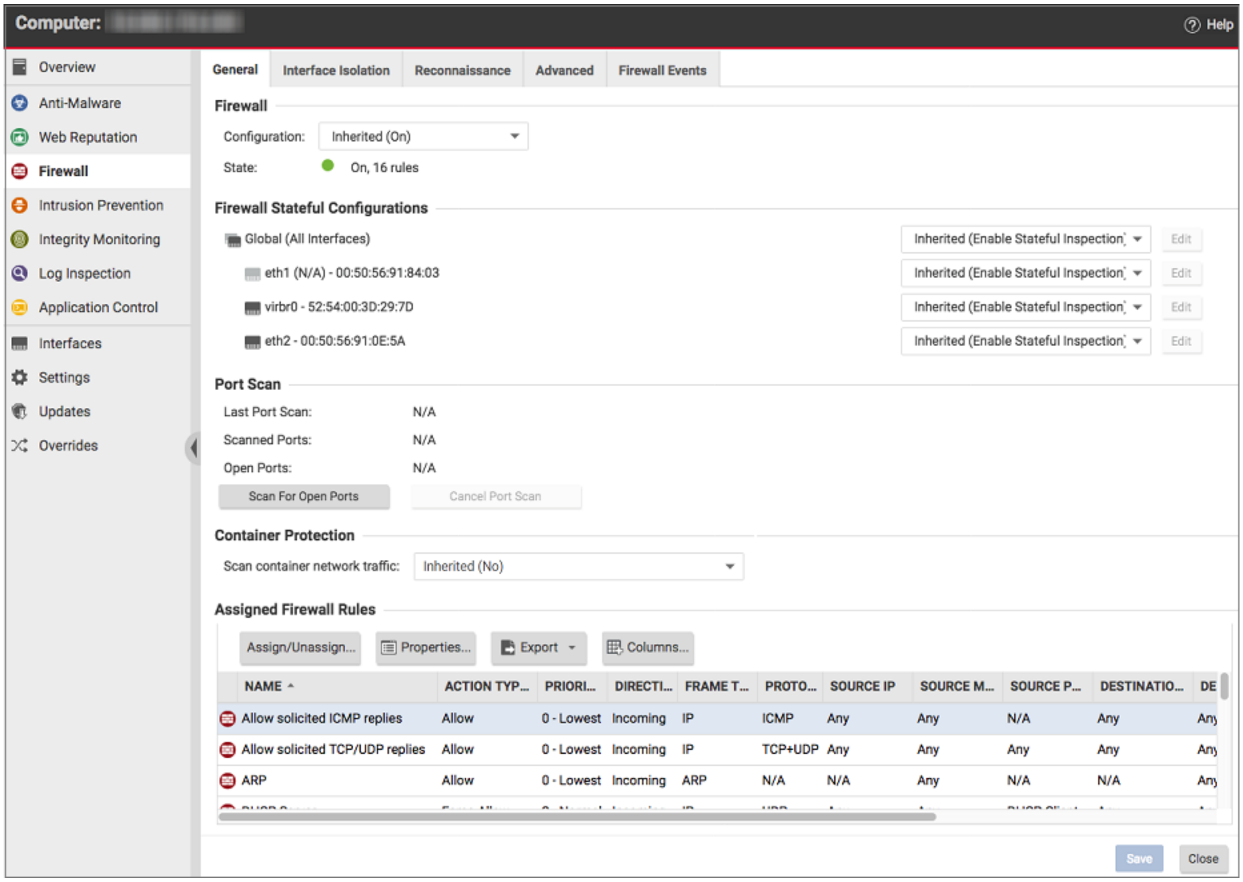
**Note:** When you enable the Deep Security Firewall with at least one firewall rule, the Agent disables the Windows Firewall automatically to prevent conflicts.

## Default Firewall rules

No outbound rules are assigned to the policies that come with Deep Security by default but several recommended inbound rules are. You can view the default inbound rules assigned to each policy by going to the **Firewall** tab in the relevant operating system policy. The example below shows the default assigned Firewall rules for the Windows 10 Desktop policy. You can configure these Firewall rules to meet the needs of your environment, but we have provided several default rules for you to get you started.

**Tip:** To minimize the impact on system performance, try not to assign more than 300 Firewall rules. It is also good practice to document all Firewall rule changes in the "Description" field of the Firewall rule. Make a note of when and why rules were created or deleted for easier Firewall maintenance.

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).



**Firewall**

Configuration: Inherited (On)

State: ● On, 16 rules

**Firewall Stateful Configurations**

Global (All Interfaces) — Inherited (Enable Stateful Inspection)

eth1 (N/A) - 00:50:56:91:84:03 — Inherited (Enable Stateful Inspection)

virbr0 - 52:54:00:3D:29:7D — Inherited (Enable Stateful Inspection)

eth2 - 00:50:56:91:0E:5A — Inherited (Enable Stateful Inspection)

**Port Scan**

Last Port Scan: N/A

Scanned Ports: N/A

Open Ports: N/A

**Container Protection**

Scan container network traffic: Inherited (No)

**Assigned Firewall Rules**

| NAME | ACTION TYP... | PRIORI... | DIRECTI... | FRAME T... | PROTO... | SOURCE IP | SOURCE M... | SOURCE P... | DESTINATIO... | DE |
|---|---|---|---|---|---|---|---|---|---|---|
| Allow solicited ICMP replies | Allow | 0 - Lowest | Incoming | IP | ICMP | Any | Any | N/A | Any | Any |
| Allow solicited TCP/UDP replies | Allow | 0 - Lowest | Incoming | IP | TCP+UDP | Any | Any | Any | Any | Any |
| ARP | Allow | 0 - Lowest | Incoming | ARP | N/A | N/A | Any | N/A | N/A | Any |

### Default Bypass rule for Deep Security Manager Traffic

The Deep Security Manager automatically implements a **Priority 4 Bypass Rule** that opens the listening port number of the agent for heartbeats on computers running Deep Security Agent. A priority of 4 ensures that this rule is applied before any Deny rule, and Bypass guarantees that the traffic is never impaired. The Bypass rule is not explicitly shown in the Firewall rule list because the rule is created internally.

This rule, however, accepts traffic from any IP address and any MAC address. To harden the Deep Security Agent's listening ports, you can create an alternative, more restrictive, Bypass rule for this port. The agent will override the default Deep Security Manager traffic rule with the new custom rule if it has these settings:

- **Priority:** 4 - Highest
- **Packet direction:** Incoming
- **Frame type:** IP

- **Protocol:** TCP
- **Packet Destination Port:** Agent's listening port for heartbeats

The custom rule must use the above parameters to replace the default rule. Ideally, the IP address or MAC address of the actual Deep Security Manager should be used as the packet source for the rule.

## Restrictive or permissive Firewall design

Typically, Firewall policies are based on one of two design strategies. Either they permit any service unless it is expressly denied or they deny all services unless expressly allowed. It is best practice to decide what type of Firewall you would like to implement. This helps reduce administrative overhead in terms of creating and maintaining the rules.

### Restrictive Firewall

A restrictive Firewall is the recommended best practice from a security perspective. All traffic is stopped by default and only traffic that has been explicitly allowed is permitted. If the primary goal of your planned Firewall is to block unauthorized access, the emphasis needs to be on restricting rather than enabling connectivity. A restrictive Firewall is easier to maintain and more secured. Allow rules are used only to permit certain traffic across the Firewall and deny everything else.

> **Note:** As soon as you assign a single outgoing Allow rule, the outgoing Firewall will operate in restrictive mode. This is also true for the inbound Firewall: as soon as you assign a single incoming Allow rule, the inbound Firewall will operate in restrictive mode.

### Permissive Firewall

A permissive Firewall permits all traffic by default and only blocks traffic known bad port/protocol based on what deny firewall rules configured. A permissive Firewall is easy to implement but it provides minimal security and requires complex rules. Deny rules are used to explicitly block traffic.

## Firewall rule actions

You can configure the Firewall to take the following actions:

> **Warning:** If you assign only incoming rules, all outgoing traffic will be allowed. If you assign a single outgoing Allow rule, the outgoing Firewall will operate in restrictive mode. There is one

exception to this: ICMPv6 traffic is always permitted unless it is specifically blocked by a Deny rule.

| | |
|---|---|
| Allow | Explicitly allows traffic that matches the rule to pass and then implicitly denies everything else.<br>**Note:** You should use an Allow action with caution because it implicitly denies everything else not defined. Be careful when creating Allow rules without defining the related rules correctly because doing so can cause all traffic to be blocked except for the traffic that the Allow rule is created for. Traffic that is not explicitly allowed by an Allow rule is dropped and gets recorded as a 'Out of "allowed" Policy' Firewall event. |
| Bypass | Allows traffic to bypass both Firewall and intrusion prevention analysis. Bypass rules should always be created in pairs (for both incoming and outgoing traffic). A Bypass rule can be based on IP, port, traffic direction, and protocol.<br>The Bypass rule is designed for media-intensive protocols or traffic originating from trusted sources. |
| Deny | Explicitly blocks traffic that matches the rule. |
| Force Allow | If a packet matches a force allow rule, it is passed but still filtered by intrusion prevention. No events are logged.<br>This type of Firewall rule action must be used for UDP and ICMP traffic. |
| Log only | Traffic will only be logged. No other action will be taken. |

For more information on how to create a Firewall rule, see "Create a firewall rule" on page 864.

## Firewall rule priorities

Rule priority determines the order in which filters are applied. This means that high priority rules get applied before low priority rules. When actions share the same priority, the orders of precedence for rules are: Bypass, Force Allow, and then Deny. However, a Deny action with a higher priority will take precedence over a Bypass action with a lower priority. For more information on how rule priorities and actions determine processing order, see "Firewall rule actions and priorities" on page 871.

To simplify the administration of Firewall rules, consider reserving certain priority levels for specific actions. For example, apply a default of priority 3 to rules that use Bypass, priority 2 for Force Allow rules, and priority 1 for Deny rules. This reduces the potential for rule conflicts.

#### Allow rules

Allow rules can only have a priority of 0. This is to ensure it is processed after all Force Allow and Deny rules at higher priorities. Keep this in mind when using Allow rules to implicitly deny traffic (any traffic not matching the Allow rules are denied). This means that when a Deny rule is assigned, it will take precedence over all of the existing assigned Allow rules.

#### Force Allow rules

Force Allow rules are recommended for traffic that must always be allowed, such as Address Resolution Protocol (ARP). The Force Allow action only acts as a trump card to a deny rule at the same or higher priority. For example, if you have a Deny rule at priority 3 that prevents access to an allowed port number from the 10.0.0.0/8 subnet, and you want to allow host 10.102.12.56 to access that, you must create a Force Allow rule at priority 3 or 4 to trump the Deny rule at priority 3. Once a packet triggers this rule, it is immediately allowed and the lower priority rules will not process it anymore.

#### Bypass rules

The Bypass rule is a special type of rule that allows a packet to bypass both the Firewall and Deep Packet Inspection (DPI) engines. This rule must be priority 4 and created in pairs, one rule for each traffic direction.

### Recommended Firewall policy rules

We recommend that you make the following rules mandatory for all of your Firewall policies:

- **ARP**: Allows incoming ARP requests so that the computer can reply to queries for its MAC address. If you do not assign this rule, no devices on the network can query the host for its MAC address and it will be inaccessible from the network.
- **Allow solicited TCP/UDP replies**: Allows the computer to receive replies to its own TCP connections and UDP messages. This works in conjunction with TCP and UDP stateful Firewall configuration.
- **Allow solicited ICMP replies**: Allows the computer to receive replies to its own ICMP messages. This works in conjunction with ICMP stateful Firewall configuration.
- **DNS Server**: Allows DNS servers to receive inbound DNS queries.

- **Remote Access RDP**: Allows the computer to accept Remote Desktop connections.
- **Remote Access SSH**: Allows the computer to accept SSH connections.

### Test Firewall rules

Before continuing with further Firewall configuration steps, test the recommended Firewall rules to ensure they're working correctly.

Test the remote access SSH rule:

1. Try to establish a SSH connection to the computer. If the Firewall is enabled and the Remote Access SSH rule is not enabled, the connection will be denied. Go to **Events & Reports > Firewall Events** to view the denied event.
2. Go to the **Computer or Policy editor**[1] **> Firewall**. Under **Assigned Firewall Rules**, click **Assign/Unassign**.
3. Search for Remote Access SSH and enable the rule. Click **OK** and **Save**.
4. Try to establish a SSH connection to the computer. The connection should be allowed.

Test the remote access RDP rule:

1. Try to establish a RDP connection to the computer. If the Firewall is enabled and the Remote Access RDP rule is not enabled, the connection will be denied. Go to **Events & Reports > Firewall** events to view the denied event.
2. Go to the **Computer or Policy editor**[2] **> Firewall**. Under **Assigned Firewall Rules**, click **Assign/Unassign**.
3. Search for Remote Access RDP and enable the rule. Click **OK** and **Save**.
4. Try to establish a RDP connection to the computer. The connection should be allowed.

## Reconnaissance scans

You can configure the Firewall to detect possible reconnaissance scans and help prevent attacks by blocking traffic from the source IPs for a period of time. Once an attack has been detected, you can instruct agents and appliances to block traffic from the source IPs for a period of time. Use

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

the Block Traffic lists on the on the **Policy or Computer Editor** > **Firewall** > **Reconnaissance** tab to set the number of minutes.

- **Computer OS Fingerprint Probe:** The agent or appliance detects an attempt to discover the computer's OS.
- **Network or Port Scan:** The agent or appliance reports a network or port scan if it detects that a remote IP is visiting an abnormal ratio of IPs to ports. Normally, an agent or appliance computer will only see traffic destined for itself, so a port scan is the most common type of probe that will be detected. The statistical analysis method used in computer or port scan detection is derived from the "TAPS" algorithm proposed in the paper "Connectionless Port Scan Detection on the Backbone" presented at IPCCC in 2006.
- **TCP Null Scan:** The agent or appliance detects packages with no flags set.
- **TCP SYNFIN Scan:** The agent or appliance detects packets with only the SYN and FIN flags set.
- **TCP Xmas Scan:** The agent or appliance detects packets with only the FIN, URG, and PSH flags set or a value of 0xFF (every possible flag set).

For each type of attack, the agent or appliance can be instructed to send the information to the Deep Security Manager where an alert will be triggered by selecting the option **Notify DSM Immediately**. For this option to work, the agents and appliances must be configured for agent or appliance-initiated or bidirectional communication in **Policy / Computer Editor > Settings > General > Communication Direction**. If enabled, the agent or appliance will initiate a heartbeat to the Deep Security Manager immediately upon detecting the attack or probe.

**Note:** If you want to enable reconnaissance protection, you must also enable the Firewall and stateful inspection on the **Policy or Computer Editor** > **Firewall** > **General** tab. You should also go to the **Policy or Computer Editor** > **Firewall** > **Advanced** tab and enable the **Generate Firewall Events** for packets that are 'Out of Allowed Policy' setting. This will generate Firewall events that are required for reconnaissance.

**Note:** The reconnaissance scans detection requires there to be at least one active Firewall rule assigned to the policy of the agent.

For information on how to handle reconnaissance warnings, see "Warning: Reconnaissance Detected" on page 1333.

## Stateful inspection

Deep Security Firewall stateful configuration mechanism should be enabled when the Firewall is on. This mechanism analyzes each packet in the context of traffic history, correctness of TCP and IP header values, and TCP connection state transitions. In the case of stateless protocols like UDP and ICMP, a pseudo-stateful mechanism is implemented based on historical traffic analysis.

Packets are handled by the stateful mechanism as follows:

1. A packet is passed to the stateful routine if it has been allowed through by the static Firewall rule conditions.
2. The packet is examined to determine whether it belongs to an existing connection.
3. The TCP header is examined for correctness (for example, sequence numbers, flag combinations, and so on).

The Deep Security Firewall stateful configuration enables protection against attacks such as denial of service, provided that a default configuration with stateful TCP, ICMP, or UDP protocol is enabled and only solicited replies are allowed. If the UDP stateful option is enabled, Force Allow must be used when running UDP servers (for example, DHCP). If there is no DNS or WINS server configured for the Deep Security Agents, a Force Allow Incoming UDP Ports 137 rule might be required for NetBIOS.

Stateful logging should be disabled unless required for ICMP or UDP protocols.

## Example

This is an example of how a simple Firewall policy can be created for a web server:

1. Enable stateful inspection for TCP, UDP, and ICMP using a global Firewall stateful configuration with these options enabled.
2. Add a Firewall rule to allow TCP and UDP replies to requests originated on the workstation. To do this create an incoming Allow rule with the protocol set to **TCP + UDP** and select **Not** and **Syn** under **Specific Flags**. At this point the policy only allows TCP and UDP packets that are replies to requests initiated by a user on the workstation. For example, in conjunction with the stateful analysis options enabled in step 1, this rule allows a user on this computer to perform DNS lookups (via UDP) and to browse the Web via HTTP (TCP).
3. Add a Firewall rule to allow ICMP replies to requests originated on the workstation. To do this, create an incoming Allow rule with the protocol set to **ICMP** and select the **Any Flags** check box. This means that a user on this computer can ping other workstations and receive a reply but other users will not be able to ping this computer.

4. Add a Firewall rule to allow incoming TCP traffic to port 80 and 443 with the **Syn** check box checked in the **Specific Flags** section. This means that external users can access a Web server on this computer.

   At this point we have a basic Firewall policy that allows solicited TCP, UDP and ICMP replies and external access to the Web server on this computer all other incoming traffic is denied.

   For an example of how Deny and Force Allow rule actions can be used to further refine this policy consider how we may want to restrict traffic from other computers in the network. For example, we may want to allow access to the Web server on this computer to internal users but deny access from any computers that are in the DMZ. This can be done by adding a Deny rule to prohibit access from servers in the DMZ IP range.

5. Add a Deny rule for incoming TCP traffic with source IP 10.0.0.0/24 which is the IP range assigned to computers in the DMZ. This rule denies any traffic from computers in the DMZ to this computer.

   We may, however, want to refine this policy further to allow incoming traffic from the mail server which resides in the DMZ.

6. Use a Force Allow for incoming TCP traffic from source IP 10.0.0.100. This Force Allow overrides the Deny rule we created in the previous step to permit traffic from this one computer in the DMZ.

## Important things to remember

- All traffic is first checked against Firewall rules before being analyzed by the stateful inspection engine. If the traffic clears the Firewall rules, the traffic is then analyzed by the stateful inspection engine (provided stateful inspection is enabled in the Firewall Stateful Configuration).
- Allow rules are prohibitive. Anything not specified in the Allow rules is automatically dropped. This includes traffic of other frame types so you need to remember to include rules to allow other types of required traffic. For example, don't forget to include a rule to allow ARP traffic if static ARP tables are not in use.
- If UDP stateful inspection is enabled a Force Allow rule must be used to allow unsolicited UDP traffic. For example, if UDP stateful inspection is enabled on a DNS server then a Force Allow for port 53 is required to allow the server to accept incoming DNS requests.

- If ICMP stateful inspection is enabled a Force Allow rule must be used to allow unsolicited ICMP traffic. For example, if you wish to allow outside ping requests a Force Allow rule for ICMP type 3 (Echo Request) is required.
- A Force Allow acts as a trump card only within the same priority context.
- If you do not have a DNS or WINS server configured (which is common in test environments) a "Force Allow incoming UDP port 137" rule may be required for NetBIOS (Windows shares).

**Note:** When troubleshooting a new Firewall policy the first thing you should do is check the Firewall rule logs on the **agent or appliance**[1]. The Firewall rule logs contain all the information you need to determine what traffic is being denied so that you can further refine your policy as required.

## Create a firewall rule

Firewall rules examine the control information in individual packets, and either block or allow them according to the criteria that you define. Firewall rules can be assigned to a policy or directly to a computer.

**Note:** This article specifically covers how to create a firewall rule. For information on how to configure the firewall module, see "Set up the Deep Security firewall" on page 851.

To create a new firewall rule, you need to:

1. "Add a new rule" on the next page.
2. "Select the behavior and protocol of the rule" on the next page.
3. "Select a Packet Source and Packet Destination" on page 867.

When you're done with your firewall rule, you can also learn how to:

- "Configure rule events and alerts" on page 869
- "Set a schedule for the rule" on page 869

[1] The Deep Securty Agent and Deep Security Virtual Appliance are the components that enforce the Deep Security policies that you have defined. Agents are deployed directly on a computer. Appliances are used in VMware vSphere environments to provide agentless protection. They are not available with Deep Security as a Service.

- "See policies and computers a rule is assigned to" on page 869
- "Assign a context to the rule " on page 869

## Add a new rule

There are three ways to add a new firewall rule on the **Policies** > **Common Objects** > **Rules** > **Firewall Rules** page. You can:

- Create a new rule. Click **New** > **New Firewall Rule**.
- Import a rule from an XML file. Click **New** > **Import From File**.
- Copy and then modify an existing rule. Right-click the rule in the Firewall Rules list and then click **Duplicate**. To edit the new rule, select it and then click **Properties**.

## Select the behavior and protocol of the rule

1. Enter a **Name** and **Description** for the rule.

   > Tip: It is good practice to document all firewall rule changes in the Description field of the firewall rule. Make a note of when and why rules were created or deleted for easier firewall maintenance.

2. Select the **Action** that the rule should perform on packets. You can select from one of the following five actions:

   > Note: Only one rule action is applied to a packet, and rules (of the same priority) are applied in the order of precedence listed below.

   - The rule can allow traffic to **bypass** the firewall. A bypass rule allows traffic to pass through the firewall and intrusion prevention engine at the fastest possible rate. Bypass rules are meant for traffic using media intensive protocols where filtering may not be desired or for traffic originating from trusted sources.

     > Tip: For an example of how to create and use a bypass rule for trusted sources in a policy, see "Allow trusted traffic to bypass the firewall" on page 870.

     > Note: Bypass rules are unidirectional. Explicit rules are required for each direction of traffic.

> **Tip:** You can achieve maximum throughput performance on a bypass rule with the following settings:
>
> - **Priority:** Highest
> - **Frame Type:** IP
> - **Protocol:** TCP, UDP, or other IP protocol. (Do not use the "Any" option.)
> - **Source and Destination IP and MAC:** all "Any"
> - If the protocol is TCP or UDP and the traffic direction is "incoming", the destination ports must be one or more specified ports (not "Any"), and the source ports must be "Any".
> - If the protocol is TCP or UDP and the traffic direction is "outgoing", the source ports must be one or more specified ports (Not "Any"), and the destination ports must be "Any".
> - **Schedule:** None.

- The rule can **log only**. This action will make entries in the logs but will not process traffic.
- The rule can **force allow** defined traffic (it will allow traffic defined by this rule without excluding any other traffic.)
- The rule can **deny** traffic (it will deny traffic defined by this rule.)
- The rule can **allow** traffic (it will exclusively allow traffic defined by this rule.)

> **Note:** If you have no allow rules in effect on a computer, all traffic is permitted unless it is specifically blocked by a deny rule. Once you create a single allow rule, all other traffic is blocked unless it meets the requirements of the allow rule. There is one exception to this: ICMPv6 traffic is always permitted unless it is specifically blocked by a deny rule.

3. Select the **Priority** of the rule. The priority determines the order in which rules are applied. If you have selected "force allow", "deny", or "bypass" as your rule action, you can set a priority of 0 (low) to 4 (highest). Setting a priority allows you to combine the actions of rules to achieve a cascading rule effect.

> **Note:** **Log only** rules can only have a priority of **4**, and **Allow** rules can only have a priority of **0**.

> **Note:** High priority rules get applied before low priority rules. For example, a port 80 incoming deny rule with a priority of 3 will drop a packet before a port 80 incoming force allow rule with a priority of 2 gets applied to it.

For detailed information on how actions and priority work together, see "Firewall rule actions and priorities" on page 871.

4. Select a **Packet Direction**. Select whether this rule will be applied to **incoming** (from the network to the computer) or **outgoing**(from the computer to the network) traffic.

   > **Note:** An individual firewall rule only apply to a single direction of traffic. You may need to create incoming and outgoing firewall rules in pairs for specific types of traffic.

5. Select an Ethernet **Frame Type**. The term "frame" refers to Ethernet frames, and the available protocols specify the data that the frame carries. If you select "Other" as the frame type, you need to specify a frame number.
6. > **Note:** **IP** covers both IPv4 and IPv6. You can also select **IPv4** or **IPv6** individually

   > **Note:** On Solaris, Deep Security Agents will only examine packets with an IP frame type, and Linux Agents will only examine packets with IP or ARP frame types. Packets with other frame types will be allowed through. Note that the Virtual Appliance does not have these restrictions and can examine all frame types, regardless of the operating system of the virtual machine it is protecting.

   If you select the Internet Protocol (IP) frame type, you need to select the transport **Protocol**. If you select "Other" as the protocol, you also need to enter a protocol number.

## Select a Packet Source and Packet Destination

Select a combination of **IP** and **MAC** addresses, and if available for the frame type, **Port** and **Specific Flags** for the Packet Source and Packet Destination.

> **Tip:** You can use a previously created IP, MAC or port list.

Support for IP-based frame types is as follows:

| | IP | MAC | Port | Flags |
|---|---|---|---|---|
| Any | ✓ | ✓ | | |
| ICMP | ✓ | ✓ | | ✓ |
| ICMPV6 | ✓ | ✓ | | ✓ |
| IGMP | ✓ | ✓ | | |
| GGP | ✓ | ✓ | | |
| TCP | ✓ | ✓ | ✓ | ✓ |
| PUP | ✓ | ✓ | | |
| UDP | ✓ | ✓ | ✓ | |
| IDP | ✓ | ✓ | | |
| ND | ✓ | ✓ | | |
| RAW | ✓ | ✓ | | |
| TCP+UDP | ✓ | ✓ | ✓ | ✓ |

**Note:** ARP and REVARP frame types only support using MAC addresses as packet sources and destinations.

You can select **Any Flags** or individually select the following flags:

- **URG**
- **ACK**
- **PSH**
- **RST**
- **SYN**
- **FIN**

## Configure rule events and alerts

When a firewall rule is triggered, it logs an event in the Deep Security Manager and records the packet data.

> Note: Note that rules using the "Allow", "Force Allow" and "Bypass" actions will not log any events.

### Alerts

You can configure rules to also trigger an alert if they log an event. To do so, open the properties for a rule, click on **Options**, and then select **Alert when this rule logs an event**.

> Note: Only firewall rules with an action set to "Deny" or "Log Only" can be configured to trigger an alert.

## Set a schedule for the rule

Select whether the firewall rule should only be active during a scheduled time.

For more information on how to do so, see "Define a schedule that you can apply to rules" on page 734.

## Assign a context to the rule

Rule contexts allow you to set firewall rules uniquely for different network environments. Contexts are commonly used to allow for different rules to be in effect for laptops when they are on and off-site.

For more information on how to create a context, see "Define contexts for use in policies" on page 728.

> Tip: For an example of a policy that implements firewall rules using contexts, look at the properties of the "Windows Mobile Laptop" Policy.

## See policies and computers a rule is assigned to

You can see which policies and computers are assigned to a firewall rule on the **Assigned To** tab. Click on a policy or computer in the list to see their properties.

### Export a rule

You can export all firewall rules to a .csv or .xml file by clicking **Export** and selecting the corresponding export action from the list. You can also export specific rules by first selecting them, clicking **Export** and then selecting the corresponding export action from the list.

### Delete a rule

To delete a rule, right-click the rule in the Firewall Rules list, click **Delete** and then click **OK**.

**Note:** Firewall Rules that are assigned to one or more computers or that are part of a policy cannot be deleted.

## Allow trusted traffic to bypass the firewall

You can set up Deep Security to allow trusted traffic to bypass the firewall.

To configure this, the basic steps are as follows:

1. "Create a new IP list of trusted traffic sources" below
2. "Create incoming and outbound firewall rules for trusted traffic using the IP list" below
3. "Assign the firewall rules to a policy used by computers that trusted traffic flows through" on the next page

After the firewall rules have been assigned to a policy, Deep Security will allow traffic from trusted sources in the IP list and will not scan the traffic for stateful issues or vulnerabilities.

### Create a new IP list of trusted traffic sources

1. Click **Policies**.
2. In the left pane, click **Lists > IP Lists**.
3. Click **New > New IP List**.
4. Enter a name for the IP list.
5. Paste the IP addresses for your trusted sources into the **IP(s)** box, one per line.
6. Click **OK**.

### Create incoming and outbound firewall rules for trusted traffic using the IP list

1. Click **Policies**.
2. In the left pane, click **Rules**.
3. Click **Firewall Rules > New > New Firewall Rule**.

4. Create a firewall rule for incoming trusted traffic using the values in the below:

| | |
|---|---|
| Name: | *source name* Traffic - Incoming |
| Action: | Bypass |
| Protocol: | Any |
| Packet Source: | IP List (select the IP list created above) |

5. Create a firewall rule for outgoing trusted traffic using the values in the below:

| | |
|---|---|
| Name: | *source name* Traffic - Outgoing |
| Action: | Bypass |
| Protocol: | Any |
| Packet Destination: | IP List (select the IP list created above) |

### Assign the firewall rules to a policy used by computers that trusted traffic flows through

1. Click **Policies**.
2. In the left pane, click **Policies**.
3. Double-click a policy to open its properties window.
4. In the left pane of the policy's properties window, click **Firewall**.
5. Click **Assign/Unassign**.
6. Ensure your view at the top left shows **All** firewall rules.
7. Use the search window to find the rules you created and select them.
8. Click **OK**.
9. Repeat the steps above for each computer that trusted traffic flows through.

## Firewall rule actions and priorities

In this article:

- "Firewall rule actions" below
- "Firewall rule sequence" on page 874
- "How firewall rules work together" on page 875
- "Rule priority" on page 877
- "Putting rule action and priority together" on page 878

### Firewall rule actions

Firewall rules can take the following actions:

- **Allow:** Explicitly allows traffic that matches the rule to pass, and then implicitly denies everything else.
- **Bypass:** Allows traffic to bypass both firewall and intrusion prevention analysis. Use this setting for media-intensive protocols or for traffic originating from trusted sources. A bypass rule can be based on IP, port, traffic direction, and protocol.
- **Deny:** Explicitly blocks traffic that matches the rule.
- **Force Allow:** Forcibly allows traffic that would otherwise be denied by other rules.

  > **Note:** Traffic permitted by a Force Allow rule will still be subject to analysis by the intrusion prevention module.

- **Log only:** Traffic will only be logged. No other action will be taken.

### More about Allow rules

Allow rules have two functions:

1. Permit traffic that is explicitly allowed.
2. Implicitly deny all other traffic.

> **Note:** Traffic that is not explicitly allowed by an Allow rule is dropped, and gets recorded as an 'Out of "Allowed" Policy' firewall event.

Commonly applied Allow rules include:

- **ARP**: Permits incoming Address Resolution Protocol (ARP) traffic .
- **Allow solicited TCP/UDP replies**: Allow the computer to receive replies to its own TCP and UDP messages. This works in conjunction with TCP and UDP stateful configuration.
- **Allow solicited ICMP replies**: Allow the computer to receive replies to its own ICMP messages. This works in conjunction with ICMP stateful configuration.

### More about Bypass rules

The Bypass rule is designed for media-intensive protocols or for traffic originating from trusted sources where filtering by the firewall or intrusion prevention modules is neither required nor desired.

A packet that matches the conditions of a Bypass rule:

- Is not subject to conditions of stateful configuration settings.
- Bypasses both firewall and Intrusion prevention analysis.

Since stateful inspection is not applied to bypassed traffic, bypassing traffic in one direction does not automatically bypass the response in the other direction. Bypass rules should always be created and applied in pairs, one rule for incoming traffic and another for outgoing.

Note: Bypass rule events are not recorded. This is not a configurable behavior.

Tip: If the Deep Security Manager uses a remote database that is protected by a Deep Security Agent, intrusion prevention-related false alarms may occur when the Deep Security Manager saves intrusion prevention rules to the database. The contents of the rules themselves could be misidentified as an attack. One of the workarounds for this is to create a bypass rule for traffic from the Deep Security Manager to the database.

## Default Bypass rule for Deep Security Manager traffic

The Deep Security Manager automatically implements a priority 4 Bypass rule that opens incoming TCP traffic on the agent's listening port for heartbeats (see "Configure the heartbeat" on page 1374) on computers running Deep Security Agent. Priority 4 ensures that this rule is applied before any Deny rules, and Bypass guarantees that the traffic is never impaired. The Bypass rule is not explicitly shown in the firewall rule list because the rule is created internally.

This rule, however, accepts traffic from any IP address and any MAC address. To harden the agent's security on this port, you can create an alternative, more restrictive bypass rule for this port. The agent will actually disable the default Deep Security Manager traffic rule in favor of the new custom rule provided it has these characteristics:

- **Priority:** 4 - Highest
- **Packet direction:** Incoming
- **Frame type:** IP
- **Protocol:** TCP
- **Packet Destination Port:** agent's listening port number for heartbeats from the Manager

The custom rule must use the above parameters to replace the default rule. Ideally, the IP address or MAC address of the actual Deep Security Manager should be used as the packet source for the rule.

#### More about Force Allow rules

The Force Allow option excludes a sub-set of traffic that could otherwise have been covered by a Deny action. Its relationship to other actions is illustrated below. Force Allow has the same effect as a Bypass rule. However, unlike Bypass, traffic that passes the firewall because of this action is still subject to inspection by the intrusion prevention module. The Force Allow action is particularly useful for making sure that essential network services are able to communicate with the DSA computer. Generally, Force Allow rules should only be used in conjunction with Allow and rules to Allow a subset of traffic that has been prohibited by the Allow and Deny rules. Force Allow rules are also required to Allow unsolicited ICMP and UDP traffic when ICMP and UDP stateful are enabled.

> **Note:** When using multiple Deep Security Managers in a multi-node arrangement, it may be useful to define an IP list for these servers, and then create a custom Deep Security Manager traffic rule with that list.

### Firewall rule sequence

Packets arriving at a computer get processed first by firewall rules, then the firewall stateful configuration conditions, and finally by the intrusion prevention rules.

This is the order in which firewall rules are applied (incoming and outgoing):

1. Firewall rules with priority **4 (highest)**
   a. **Bypass**
   b. **Log Only** (Log Only rules can only be assigned a priority of **4 (highest)**)
   c. **Force Allow**
   d. **Deny**
2. Firewall rules with priority **3 (high)**
   a. **Bypass**
   b. **Force Allow**
   c. **Deny**
3. Firewall rules with priority **2 (normal)**
   a. **Bypass**
   b. **Force Allow**
   c. **Deny**
4. Firewall rules with priority **1 (low)**
   a. **Bypass**
   b. **Force Allow**
   c. **Deny**

5. Firewall rules with priority **0 (lowest)**
    1. **Bypass**
    2. **Force Allow**
    3. **Deny**
    4. **Allow**(Note that an Allow rule can only be assigned a priority of **0 (lowest)**)

> **Note:** If you have no Allow rules in effect on a computer, all traffic is permitted unless it is specifically blocked by a Deny rule. Once you create a single Allow rule, all other traffic is blocked unless it meets the conditions of the Allow rule. There is one exception to this: ICMPv6 traffic is always permitted unless it is specifically blocked by a Deny rule.

Within the same priority context, a Deny rule will override an Allow rule, and a Force Allow rule will override a Deny rule. By using the rule priorities system, a higher priority Deny rule can be made to override a lower priority Force Allow rule.

Consider the example of a DNS server policy that makes use of a Force Allow rule to Allow all incoming DNS queries. Creating a Deny rule with a higher priority than the Force Allow rule lets you specify a particular range of IP addresses that must be prohibited from accessing the same public server.

Priority-based rule sets allow you set the order in which the rules are applied. If a Deny rule is set with the highest priority, and there are no Force Allow rules with the same priority, then any packet matching the Deny rule is automatically dropped and the remaining rules are ignored. Conversely, if a Force Allow rule with the highest priority flag set exists, any incoming packets matching the Force Allow rule will be automatically allowed through without being checked against any other rules.

### A note on logging

Bypass rules will never generate an event. This is not configurable.

Log Only rules will only generate an event if the packet in question is not subsequently stopped by either:

- a Deny rule, or
- an Allow rule that excludes it.

If the packet is stopped by one of those two rules, those rules will generate the Event and not the Log Only rule. If no subsequent rules stop the packet, the Log Only rule will generate an event.

## How firewall rules work together

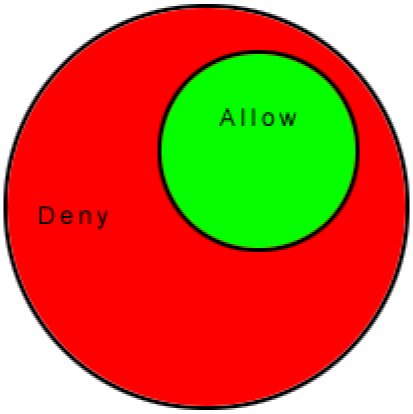
Deep Security firewall rules have both a rule action and a rule priority. Used in conjunction, these two properties allow you to create very flexible and powerful rule-sets. Unlike rule-sets used by other firewalls, which may require that the rules be defined in the order in which they should be run, Deep Security Firewall rules are run in a deterministic order based on the rule action and the rule priority, which is independent of the order in which they are defined or assigned.

### Rule Action

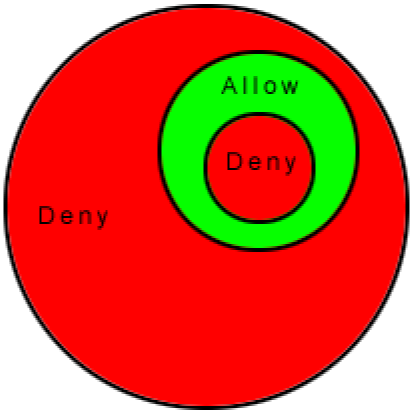
Each rule can have one of four actions.

1. **Bypass:** if a packet matches a Bypass rule, it is passed through both the firewall *and the Intrusion Prevention Engine* regardless of any other rule (at the same priority level).
2. **Log Only:** if a packet matches a Log Only rule it is passed and the event is logged.
3. **Force Allow:** if a packet matches a Force Allow rule it is passed regardless of any other rules (at the same priority level).
4. **Deny:** if a packet matches a Deny rule it is dropped.
5. **Allow:** if a packet matches an Allow rule, it is passed. Any traffic not matching one of the Allow rules is denied.

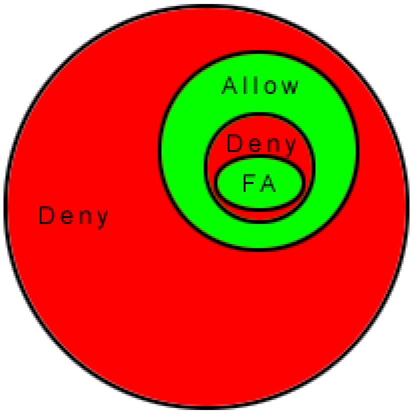
Implementing an Allow rule will cause all other traffic not specifically covered by the Allow rule to be denied:



A Deny rule can be implemented over an Allow to block specific types of traffic:



A Force Allow rule can be placed over the denied traffic to Allow certain exceptions to pass through:



## Rule priority

Rule actions of type Deny and Force Allow can be defined at any one of 5 priorities to allow further refinement of the permitted traffic defined by the set of Allow rules. Rules are run in priority order from highest (Priority 4) to lowest (Priority 0). Within a specific priority level the rules are processed in order based on the rule action (Force Allow, Deny, Allow, log only).

The priority context Allows a User to successively refine traffic controls using Deny and Force Allow rule combinations. Within the same priority context, an Allow rule can be negated with a Deny rule, and a Deny rule can be negated by a Force Allow rule.

**Note:** Rule actions of type Allow run only at priority 0 while rule actions of type Log Only run only at priority 4.

### Putting rule action and priority together

Rules are run in priority order from highest (Priority 4) to lowest (Priority 0). Within a specific priority level the rules are processed in order based on the rule action. The order in which rules of equal priority are processed is as follows:

- Bypass
- Log Only
- Force Allow
- Deny
- Allow

**Note:** Remember that rule actions of type Allow run only at priority 0 while rule actions of type Log Only run only at priority 4.

**Note:** It is important to remember that if you have a Force Allow rule and a Deny rule at the same priority the Force Allow rule takes precedence over the Deny rule and therefore traffic matching the Force Allow rule will be permitted.

## Firewall settings

The **Firewall** module provides bidirectional stateful firewall protection. It prevents denial of service attacks and provides coverage for all IP-based protocols and frame types as well as filtering for ports and IP and MAC addresses.

The Firewall section of the **Computer or Policy editor**[1] has the following tabbed sections:

- "General" on the next page
- "Interface Isolation" on page 880
- "Reconnaissance" on page 881
- "Advanced" on page 883
- "Firewall events" on page 883

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

## General

### Firewall

You can configure this policy or computer to inherit its firewall On/Off state from its parent policy or you can lock the setting locally.

### Firewall Stateful Configurations

Select which firewall stateful configuration to apply to this policy. If you have defined multiple Interfaces for this policy (above), you can specify independent configurations for each interface. For more information on creating a stateful configuration see "Define stateful firewall configurations" on page 889.

### Port Scan (Computer Editor only)

**Last Port Scan:** The last time that the Deep Security manager ran a port scan on this computer.

**Scanned Ports:** The ports that were scanned during the most recent port scan.

**Open Ports:** Listed beneath the IP address of the local computer will be a list of ports that were found to be open.

The **Scan For Open Ports** and the **Cancel Port Scan** buttons let you initiate or cancel a port scan on this computer. Deep Security Manager will scan the range of ports defined in **Computer or Policy editor**[1] **> Settings > General > Open Ports > Ports to Scan**.

> **Note:** Regardless of the ports configured to be scanned, Deep Security Manager will always scan the agent or appliance's listening port number for heartbeat connections from the Manager.

### Assigned Firewall Rules

Displays the firewall rules that are in effect for this policy or computer. To add or remove firewall rules, click **Assign/Unassign** This will display a window showing all available firewall rules from which you can select or deselect rules.

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

From a **Computer or Policy editor**[1] window, you can edit a firewall rule so that your changes apply only locally in the context of your editor, or you can edit the rule so that the changes apply globally to all other policies and computers that are using the rule.

**To edit the Rule locally,** right-click the rule and click **Properties**.

**To edit the Rule globally,** right-click the rule and click **Properties (Global)**.

For more information on creating firewall rules, see "Create a firewall rule" on page 864.

## Interface Isolation

### Interface Isolation

You can configure this policy or computer to inherit its Interface Isolation enabled or disabled state from its parent policy or you can lock the setting locally.

**Warning:** Before you enable Interface Isolation make sure that you have configured the interface patterns in the proper order and that you have removed or added all necessary string patterns. Only interfaces matching the highest priority pattern will be permitted to transmit traffic. Other interfaces (which match any of the remaining patterns on the list) will be "restricted". Restricted Interfaces will block all traffic unless an Allow Firewall Rule is used to allow specific traffic to pass through.

To configure the Interface Isolation policy:

1. On the Interface Isolation tab, select **Enable interface isolation**.
2. Configure the **Interface Patterns**. (See below)
3. Click **Save**.

### Interface Patterns

When Interface Isolation is enabled, the firewall will try to match the regular expression patterns to interface names on the local computer.

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

**Note:** Deep Security uses POSIX basic regular expressions to match interface names. For information on basic POSIX regular expressions, see https://pubs.opengroup.org/onlinepubs/009695399/basedefs/xbd_chap09.html#tag_09_03

Only interfaces matching the highest priority pattern will be permitted to transmit traffic. Other interfaces (which match any of the remaining patterns on the list) will be "restricted". Restricted Interfaces will block all traffic unless an **Allow** firewall rule is used to allow specific traffic to pass through.

Selecting **Limit to one active interface** will restrict traffic to only a single interface (even if more than one interface matches the highest priority pattern).

## Reconnaissance

### Reconnaissance Scans

The **Reconnaissance** page allows you to enable and configure traffic analysis settings on your computers. This feature can detect possible reconnaissance scans that attackers often use to discover weaknesses before beginning a targeted attack.

**Note:** Reconnaissance scans do not work in TAP mode. Reconnaissance scans can only be detected on IPv4 traffic.

To enable reconnaissance protection, you must also enable the Firewall and Stateful Inspection on the **Computer or Policy editor**[1] **> Firewall > General** tab. You should also go to the **Computer or Policy editor**[2] **> Firewall > Advanced** tab and enable the **Generate Firewall Events for packets that are 'Out of Allowed Policy'** setting. This will generate firewall events that are required for reconnaissance.

When setting up Reconnaissance scans, you have the following options:

- **Reconnaissance Scan Detection Enabled:** Turn the ability to detect reconnaissance scans on or off. The default is all scans are enabled in report mode with notifications. If you

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

want to turn off the notifications or switch from report more to a temporary blocking mode, select **Yes** from the drop-list and make your changes.

- **Computers/Networks on which to perform detection:** Choose from the list the IPs to protect. Choose from existing IP Lists. (You can use the **Policies > Common Objects > Lists > IP Lists** page to create an IP List specifically for this purpose.)
- **Do not perform detection on traffic coming from:** Select from a set of IP Lists which computers and networks to ignore. (As above, you can use the **Policies > Common Objects > Lists > IP Lists** page to create an IP List specifically for this purpose.)

For each type of attack, the agent or appliance can be instructed to send the information to the Deep Security Manager where an alert will be triggered. You can configure the Deep Security Manager to send an email notification when the alerts are triggered. For more information, see **Administration > System Settings > Alerts**. Select **Notify DSM Immediately** for this option.

> **Note:** For the "Notify DSM Immediately" option to work, the agents and appliances must be configured for **agent or appliance-initiated** or **bidirectional** communication in **Computer or Policy editor**[1] **> Settings > General.**) If enabled, the agent or appliance will initiate a heartbeat to the Deep Security Manager immediately upon detecting the attack or probe.

Once an attack has been detected, you can instruct the agents and appliances to block traffic from the source IPs for a period of time. Use the **Block Traffic** drop-down lists to set the number of minutes.

The alerts are:

- **Computer OS Fingerprint Probe:** The agent or appliance detects an attempt to discover the computers OS.
- **Network or Port Scan:** The agent or appliance reports a network or port scan if it detects that a remote IP is visiting an abnormal ratio of IPs to ports. Normally, an agent or appliance computer will only see traffic destined for itself, so a port scan is the most common type of probe that will be detected. The statistical analysis method used in computer or port scan detection is derived from the "TAPS" algorithm proposed in the paper "Connectionless Port Scan Detection on the Backbone" presented at IPCCC in 2006.
- **TCP Null Scan:** The agent or appliance detects packages with no flags set.

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

- **TCP SYNFIN Scan:** The agent or appliance detects packets with only the SYN and FIN flags set.
- **TCP Xmas Scan:** The agent or appliance detects packets with only the FIN, URG, and PSH flags set or a value of 0xFF (every possible flag set).

**Note:** "Network or Port Scans" differs from the other types of reconnaissance in that it cannot be recognized by a single packet and requires Deep Security to watch traffic for a period of time.

The agent or appliance reports a computer or port scan if it detects that a remote IP is visiting an abnormal ratio of IPs to ports. Normally an agent or appliance computer will only see traffic destined for itself, so a port scan is by far the most common type of probe that will be detected. However, if a computer is acting as a router or bridge it could see traffic destined for a number of other computers, making it possible for the agent or appliance to detect a computer scan (ex. scanning a whole subnet for computers with port 80 open).
Detecting these scans can take several seconds since the agent or appliance needs to be able to track failed connections and decide that there are an abnormal number of failed connections coming from a single computer in a relatively short period of time.

**Note:** Deep Security Agents running on Windows computers with browser applications may occasionally report false-positive reconnaissance scans due to residual traffic arriving from closed connections.

For information on how to handle reconnaissance warnings, see "Warning: Reconnaissance Detected" on page 1333.

## Advanced

### Events

Set whether to generate events for packets that are "Out of Allowed Policy". These are packets that have been blocked because they have not been specifically allowed by an **Allow** firewall rule. Setting this option to **Yes** may generate a large number of events depending on the firewall rules you have in effect.

## Firewall events

Firewall events are displayed the same way as they are in the main Deep Security Manager window except that only events relating to this policy or specific computer are displayed.

## Firewall settings with Oracle RAC

Deep Security supports Oracle RAC. For a list of supported versions of Oracle RAC, see "Software requirements" on page 502.

The default Linux Server Deep Security policy is compatible with the Oracle RAC environment, with the exception of firewall settings. Because there are complex communication channels between RAC nodes, the RAC nodes will fail to create a virtual NIC and scan the NIC, due to firewall interference. As a result, Oracle Clusterware would fail to start on some nodes. You can disable the firewall or customize the firewall settings.

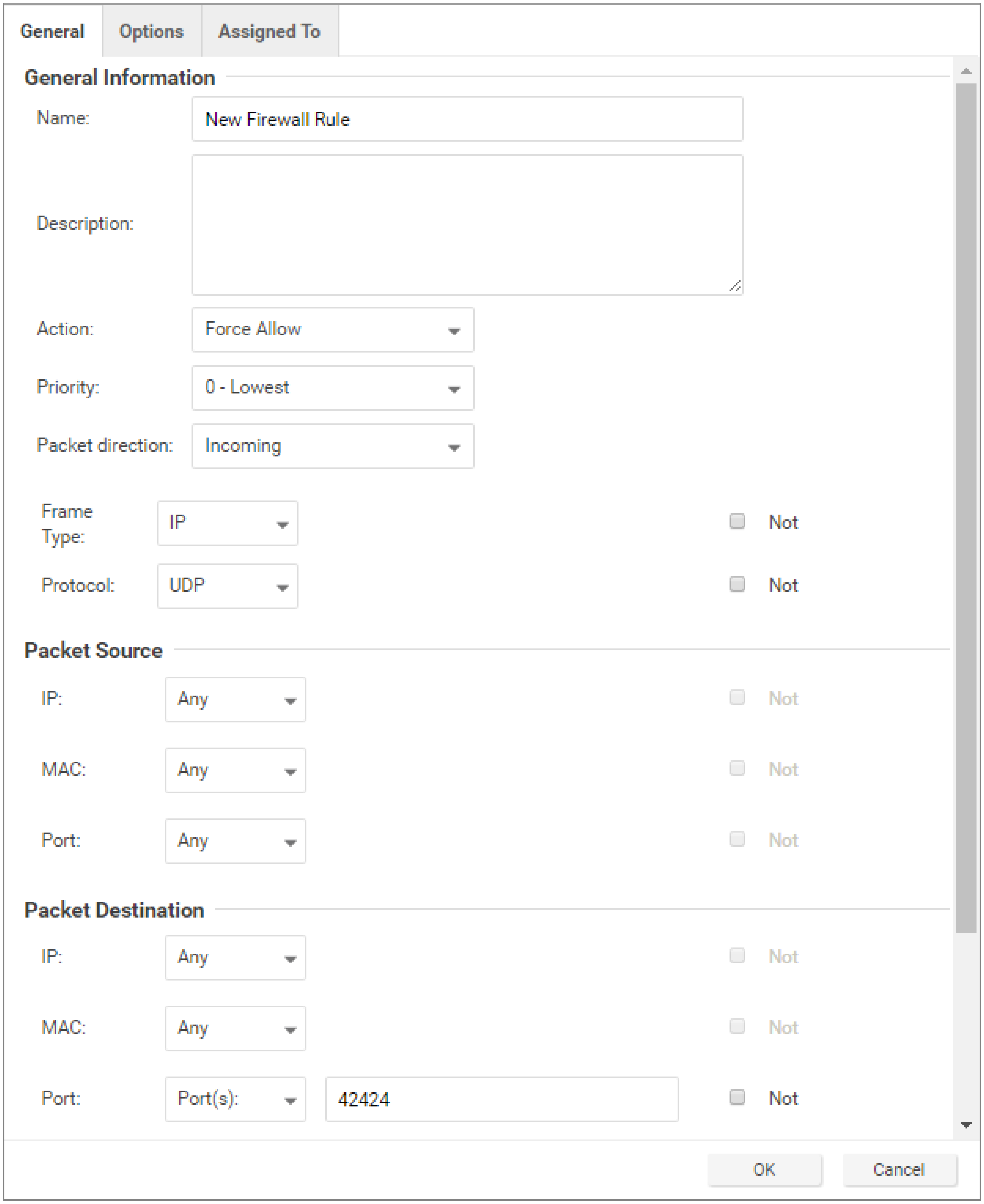
### Add a rule to allow communication between nodes

1. In the Deep Security Manager, go to the **Policies** tab.
2. Right-click the **Linux Server** policy and click **Duplicate**.
3. Click the new **Linux Server_2** policy and click **Details**.
4. Give the policy a new name, for example, "Oracle RAC" and click **Save**.
5. Click **Firewall**.
6. Click **Assign/Unassign**.
7. Click **New > New Firewall Rule**.
8. Under **General Information**, set the **Name** to something descriptive, like "Allow communication with Oracle nodes". Set **Action** to "Force Allow" and set **Protocol** to "Any".
9. Under **Packet Source**, set **MAC** to "MAC List". In the **Select MAC List** that appears, select "New". A "New MAC List Properties" dialog box appears.
10. Give the MAC list a name, like "Oracle RAC MAC list". Under **MAC(s): (One MAC per line)**, add all of the MAC addresses used by all Oracle nodes (including MACs from both private and public NICs). Click **OK** when finished.
11. Under **Packet Destination**, set **MAC** to "MAC List". In the **Select MAC List** that appears, select the MAC list you created in step 10 and then click **OK**.
12. In the Firewall Rules list for the policy, ensure that this new rule is selected and click **OK** and then click **Save**.

### Add a rule to allow UDP port 42424

Follow the steps described in the procedure above to add a new rule that allows UDP port 42424. This port number is used by the Cluster Synchronization Service daemon (CSSD), Oracle Grid Interprocess Communication (GIPCD) and Oracle HA Services daemon (OHASD).

**Note:** Please note that the MAC list that you created above may not be able to cover this rule. This rule is essential for Oracle RAC.



General Information

| | | |
|---|---|---|
| Name: | New Firewall Rule | |
| Description: | | |
| Action: | Force Allow | |
| Priority: | 0 - Lowest | |
| Packet direction: | Incoming | |
| Frame Type: | IP | □ Not |
| Protocol: | UDP | □ Not |

Packet Source

| | | |
|---|---|---|
| IP: | Any | □ Not |
| MAC: | Any | □ Not |
| Port: | Any | □ Not |

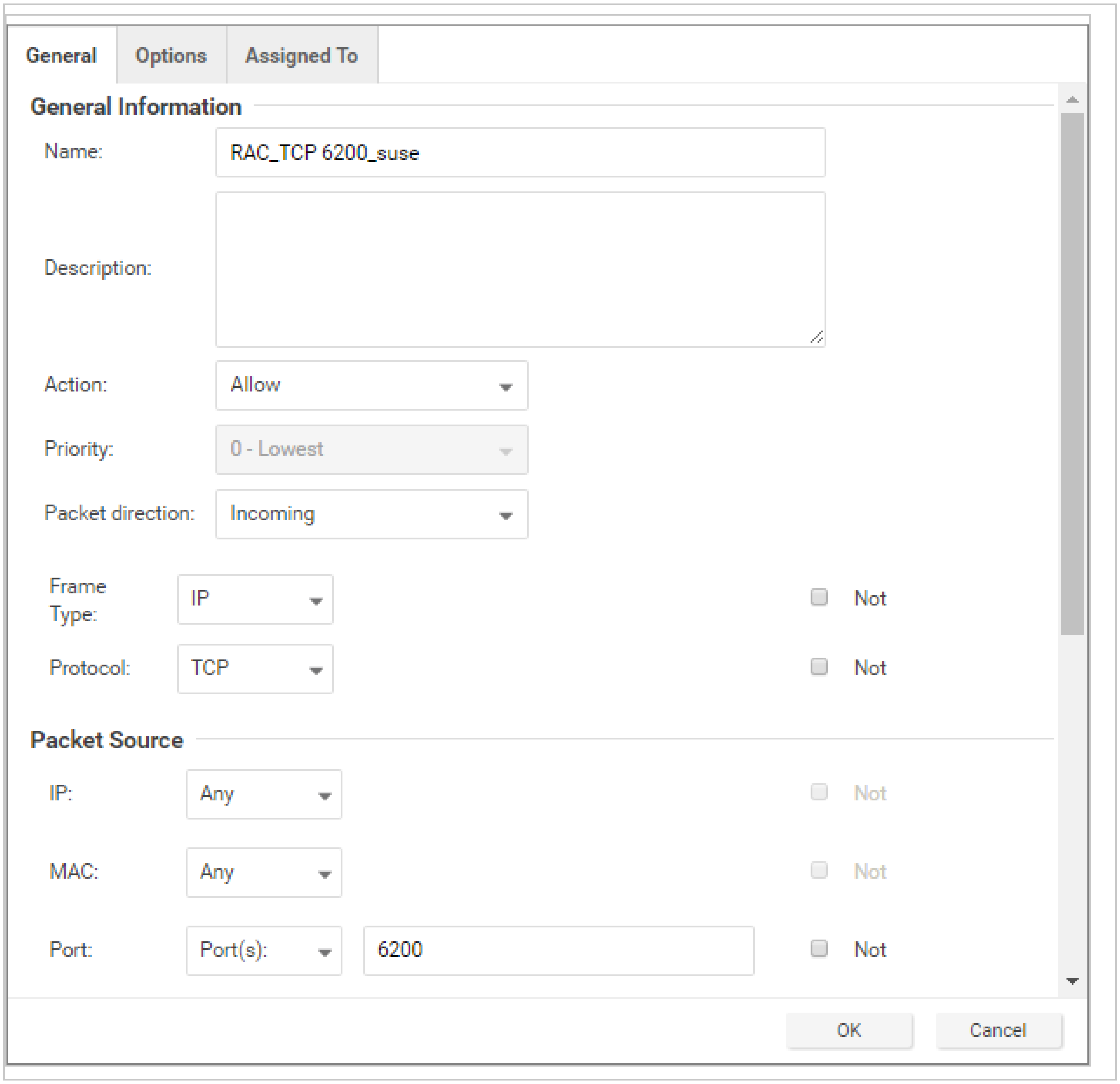
Packet Destination

| | | | |
|---|---|---|---|
| IP: | Any | | □ Not |
| MAC: | Any | | □ Not |
| Port: | Port(s): | 42424 | □ Not |

## Allow other RAC-related packets

Oracle RAC will send a very large number of packets with Frame Type C08A and 0ACB. Blocking them may cause some unpredictable behavior.

- **Allow TCP post 6200:** Add the public IP addresses of the RAC nodes in the **IP** fields under **Packet Source** and **Packet Destination** and set destination port to 6200. This port number is used by Oracle Notification Services (ONS). This port is configurable, so check the value on your system set the correct port number if it is something other than 6200.



General Information

Name: RAC_TCP 6200_suse

Description:

Action: Allow

Priority: 0 - Lowest

Packet direction: Incoming

Frame Type: IP □ Not

Protocol: TCP □ Not

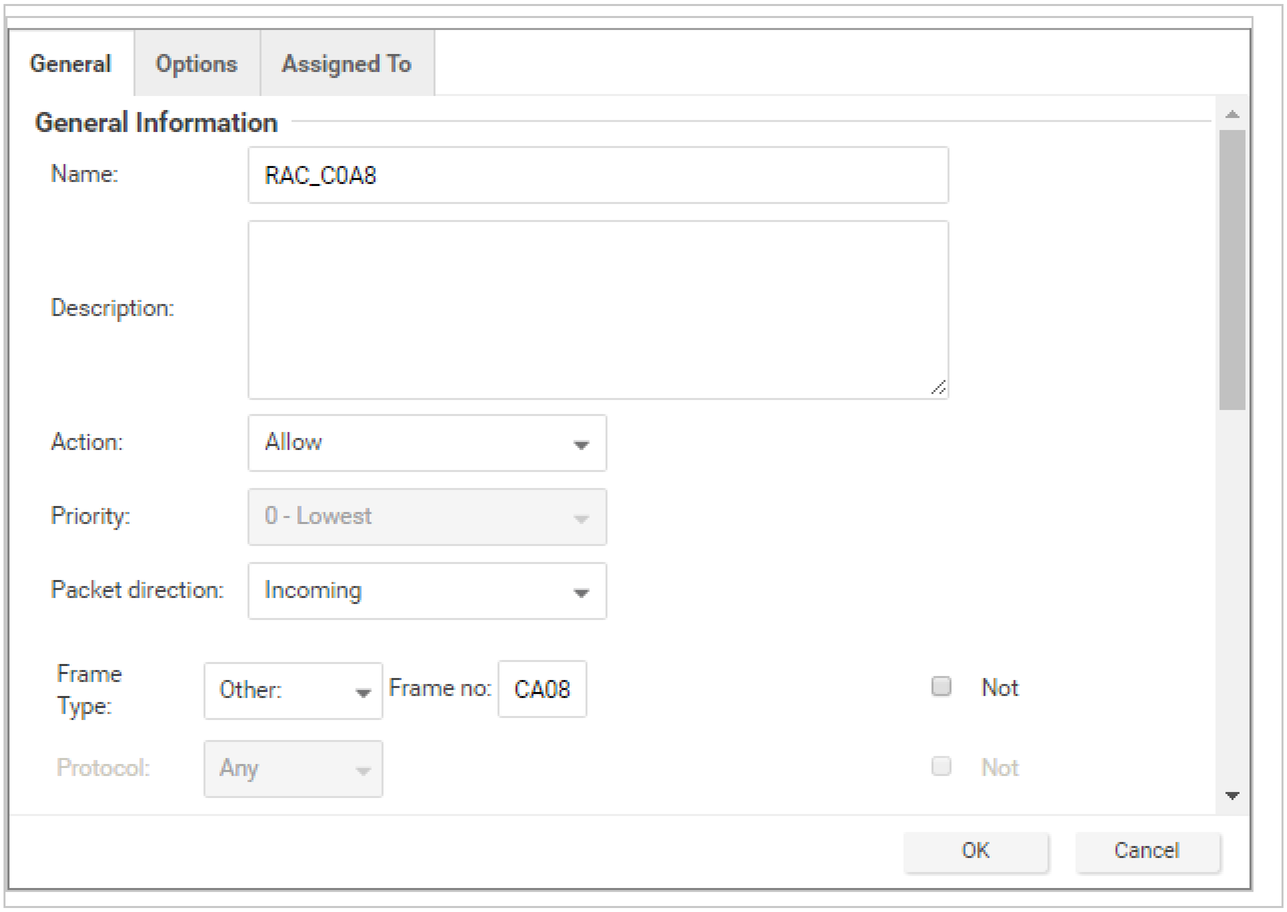
Packet Source

IP: Any □ Not

MAC: Any □ Not

Port: Port(s): 6200 □ Not

- **Allow Frame Type C0A8:** Add a rule with the **Frame Type** set to "Other" and the **Frame no** set to "C0A8".



General Information

Name: RAC_C0A8

Description:

Action: Allow

Priority: 0 - Lowest

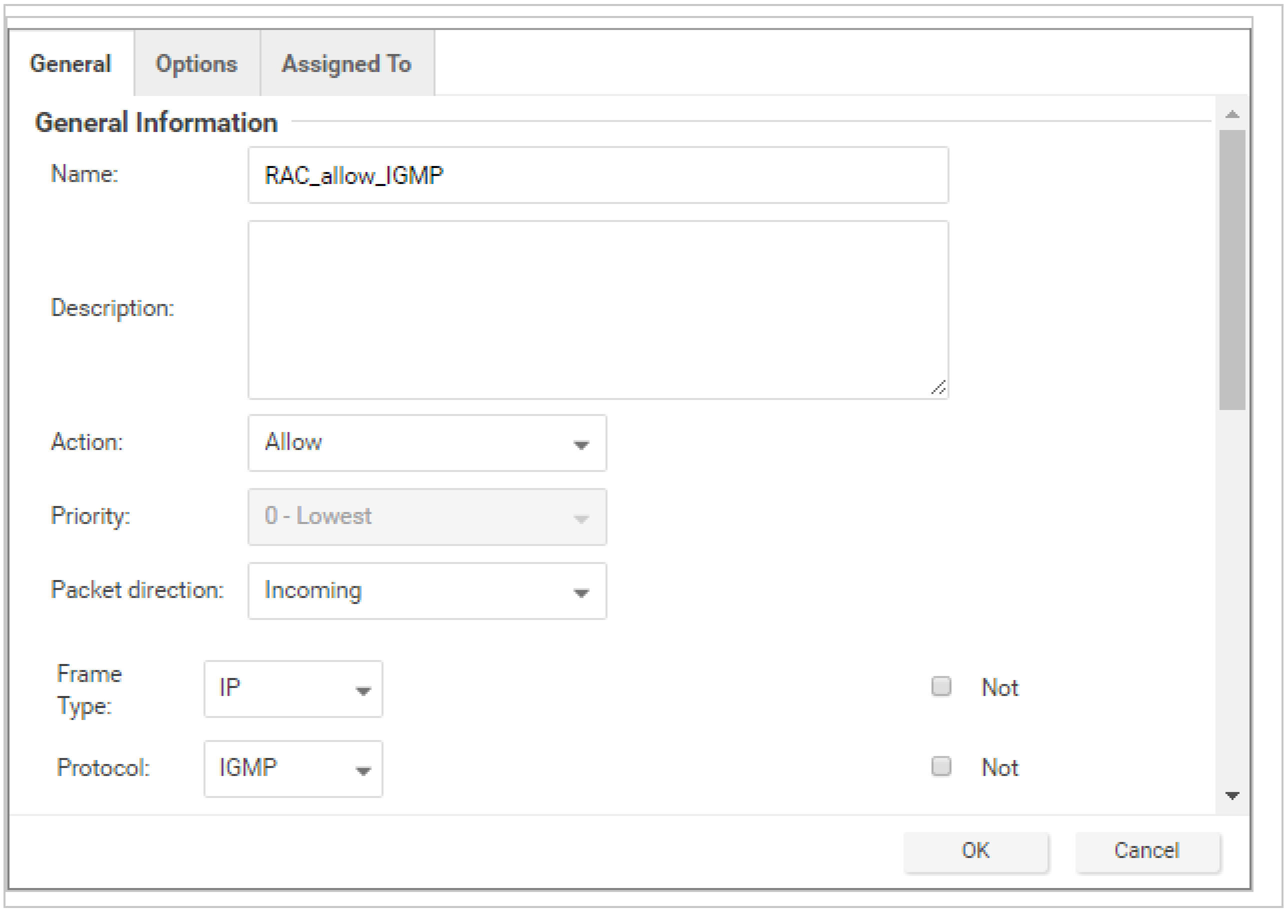
Packet direction: Incoming

Frame Type: Other: Frame no: CA08 □ Not

Protocol: Any □ Not

- **Allow Frame Type 0ACB:** Add a rule with the **Frame Type** set to "Other" and the **Frame no** set to "0ACB".
- **Allow Frame Type 0AC9:** Add a rule with the **Frame Type** set to "Other" and the **Frame no** set to "0AC9".

- **Allow IGMP protocol:** Add a rule with the **Protocol** set to "IGMP".



General Information

Name: RAC_allow_IGMP

Description:

Action: Allow

Priority: 0 - Lowest

Packet direction: Incoming

Frame Type: IP □ Not

Protocol: IGMP □ Not

Please refer to the following link to check whether there are additional RAC-related components in your system that need extra firewall rules to allow certain ports:

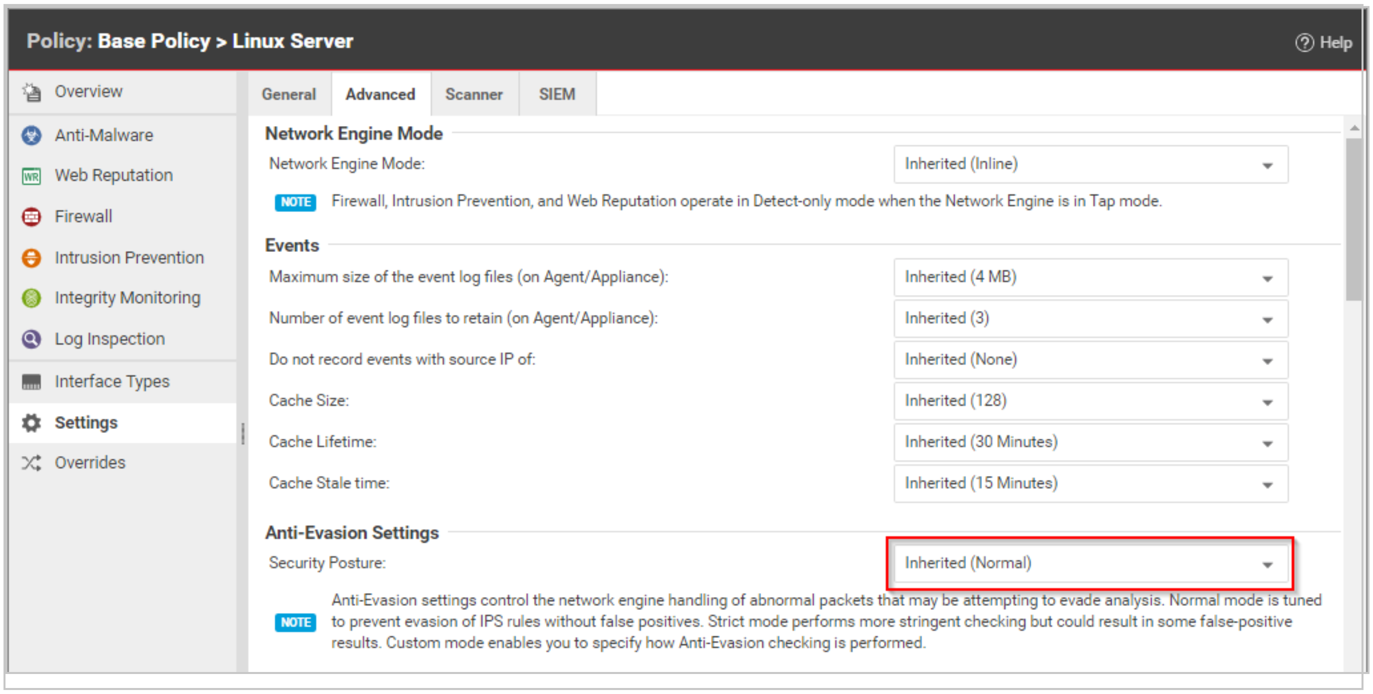
https://docs.oracle.com/database/121/RILIN/ports.htm#RILIN1178

## Ensure that the Oracle SQL Server rule is assigned

Check that the "Oracle SQL Server" Firewall rule is assigned to the Linux Server policy. This is a pre-defined Deep Security Firewall rule that allows port 1521.

## Ensure that anti-evasion settings are set to "Normal"

In the properties for the Linux Server policy, **Settings > Network Engine > Anti-Evasion Settings** are set to "Normal" by default. If this setting is set to "Strict", the RAC database response will be extremely slow.



Network Engine Mode

Network Engine Mode: Inherited (Inline)

NOTE Firewall, Intrusion Prevention, and Web Reputation operate in Detect-only mode when the Network Engine is in Tap mode.

Events

Maximum size of the event log files (on Agent/Appliance): Inherited (4 MB)

Number of event log files to retain (on Agent/Appliance): Inherited (3)

Do not record events with source IP of: Inherited (None)

Cache Size: Inherited (128)

Cache Lifetime: Inherited (30 Minutes)

Cache Stale time: Inherited (15 Minutes)

Anti-Evasion Settings

Security Posture: Inherited (Normal)

NOTE Anti-Evasion settings control the network engine handling of abnormal packets that may be attempting to evade analysis. Normal mode is tuned to prevent evasion of IPS rules without false positives. Strict mode performs more stringent checking but could result in some false-positive results. Custom mode enables you to specify how Anti-Evasion checking is performed.

## Define stateful firewall configurations

Deep Security's stateful firewall configuration mechanism analyzes each packet in the context of traffic history, correctness of TCP and IP header values, and TCP connection state transitions. In the case of stateless protocols like UDP and ICMP, a pseudo-stateful mechanism is implemented based on historical traffic analysis. Packets are handled by the stateful mechanism as follows:

1. A packet is passed to the stateful routine if it has been allowed through by the static firewall rule conditions,
2. The packet is examined to determine whether it belongs to an existing connection, and
3. The TCP header is examined for correctness (e.g. sequence numbers, flag combinations, etc.).

To create a new stateful configuration, you need to:

1. "Add a stateful configuration " on the next page.
2. "Enter stateful configuration information" on the next page.
3. "Select packet inspection options" on the next page.

When you're done with your stateful configuration, you can also learn how to

- "See policies and computers a stateful configuration is assigned to" on page 894
- "Export a stateful configuration " on page 894

- "Delete a stateful configuration " on page 894

## Add a stateful configuration

There are three ways to define a stateful configuration on the **Policies > Common Objects > Other > Firewall Stateful Configurations** page:

- Create a new configuration. Click **New** > **New Firewall Stateful Configuration**.
- Import a configuration from an XML file. Click **New** > **Import From File**.
- Copy and then modify an existing configuration. Right-click the configuration in the Firewall Stateful Configurations list and then click **Duplicate**. To edit the new configuration, select it and then click **Properties**.

## Enter stateful configuration information

Enter a **Name** and **Description** for the configuration.

## Select packet inspection options

You can define options for IP, TCP, UDP and ICMP packet inspection, end enable Active or Passive FTP.

### IP packet inspection

Under the **General** tab, select the **Deny all incoming fragmented packets** to drop any fragmented packets. Dropped packets will bypass fragmentation analysis and generate an "IP fragmented packet" log entry. Packets with a total length smaller than the IP header length are dropped silently.

Warning: Attackers sometimes create and send fragmented packets in an attempt to bypass Firewall Rules.

Note: The Firewall Engine, by default, performs a series of checks on fragmented packets. This is default behavior and cannot be reconfigured. Packets with the following characteristics are dropped:

- **Invalid fragmentation flags/offset:** A packet is dropped when either the **DF** and **MF** flags in the IP header are set to 1, or the header contains the **DF** flag set to 1 and an **Offset** value different than 0.

- **First fragment too small:** A packet is dropped if its **MF** flag is set to 1, its **Offset** value is at 0, and it has total length of less than 120 bytes (the maximum combined header length).
- **IP fragment out of boundary:** A packet is dropped if its **Offset** flag value combined with the total packet length exceeds the maximum datagram length of 65535 bytes.
- **IP fragment offset too small:** A packet is dropped if it has a non-zero **Offset** flag with a value that is smaller than 60 bytes.

#### TCP packet inspection

Under the **TCP** tab, select which of the following options you would like to enable:

- **Deny TCP packets containing CWR, ECE flags:** These flags are set when there is network congestion.

  **Note:** RFC 3168 defines two of the six bits from the Reserved field to be used for ECN (Explicit Congestion Notification), as follows:
  - Bits 8 to 15: CWR-ECE-URG-ACK-PSH-RST-SYN-FIN
  - TCP Header Flags Bit Name Reference:
    - Bit 8: CWR (Congestion Window Reduced) [RFC3168]
    - Bit 9: ECE (ECN-Echo) [RFC3168]

  **Warning:** Automated packet transmission (such as that generated by a denial of service attack, among other things) will often produce packets in which these flags are set.

- **Enable TCP stateful inspection:** Enable stateful inspection at the TCP level. If you enable stateful TCP inspection, the following options become available:
  - **Enable TCP stateful logging:** TCP stateful inspection events will be logged.
  - **Limit the number of incoming connections from a single computer to:** Limiting the number of connections from a single computer can lessen the effect of a denial of service attack.
  - **Limit the number of outgoing connections to a single computer to:** Limiting the number of outgoing connections to a single computer can significantly reduce the effects of Nimda-like worms.
  - **Limit the number of half-open connections from a single computer to:** Setting a limit here can protect you from DoS attacks like SYN Flood. Although most servers have

timeout settings for closing half-open connections, setting a value here can prevent half-open connections from becoming a significant problem. If the specified limit for SYN-SENT (remote) entries is reached, subsequent TCP packets from that specific computer will be dropped.

> Note: When deciding on how many open connections from a single computer to allow, choose your number from somewhere between what you would consider a reasonable number of half-open connections from a single computer for the type of protocol being used, and how many half-open connections from a single computer your system can maintain without getting congested.

- **Enable ACK Storm protection when the number of already acknowledged packets exceeds:** Set this option to log an event that an ACK Storm attack has occurred.
  - **Drop Connection when ACK Storm detected:** Set this option to drop the connection if such an attack is detected.

> Note: ACK Storm protection options are only available on Deep Security Agent 8.0 and earlier.

### FTP Options

Under the **FTP Options** tab, you can enable the following options:

> Note: The following FTP options are available in Deep Security Agent version 8.0 and earlier.

- Active FTP
  - **Allow Incoming:** Allow Active FTP when this computer is acting as a server.
  - **Allow Outgoing:** Allow Active FTP when this computer is acting as client.
- Passive FTP
  - **Allow Incoming:** Allow Passive FTP when this computer is acting as a server.
  - **Allow Outgoing:** Allow Passive FTP when this computer is acting as a client.

### UDP packet inspection

Under the **UDP** tab, you can enable the following options:

- **Enable UDP stateful inspection:** Select to enable stateful inspection of UDP traffic.

  > **Note:** The UDP stateful mechanism drops unsolicited incoming UDP packets. For every outgoing UDP packet, the rule will update its UDP "stateful" table and will then only allow a UDP response if it occurs within 60 seconds of the request. If you wish to allow specific incoming UDP traffic, you will have to create a **Force Allow** rule. For example, if you are running a DNS server, you will have to create a **Force Allow** rule to allow incoming UDP packets to destination port 53.

  > **Warning:** Without stateful inspection of UDP traffic, an attacker can masquerade as a DNS server and send unsolicited UDP "replies" from source port 53 to computers behind a firewall.

  - **Enable UDP stateful logging:** Selecting this option will enable the logging of UDP stateful inspection events.

### ICMP packet inspection

Under the **ICMP** tab, you can enable the following options:

> **Note:** ICMP stateful inspection is available in Deep Security Agent version 8.0 or earlier.

- **Enable ICMP stateful inspection:** Select to enable stateful inspection of ICMP traffic.

  > **Note:** The ICMP (pseudo-)stateful mechanism drops incoming unsolicited ICMP packets. For every outgoing ICMP packet, the rule will create or update its ICMP "stateful" table and will then only allow a ICMP response if it occurs within 60 seconds of the request. (ICMP pair types supported: Type 0 & 8, 13 & 14, 15 & 16, 17 & 18.)

  > **Warning:** With stateful ICMP inspection enabled, you can, for example, only allow an ICMP echo-reply in if an echo-request has been sent out. Unrequested echo-replies could be a sign of several kinds of attack including a Smurf amplification attack, a Tribe Flood Network communication between master and daemon, or a Loki 2 back-door.

  - **Enable ICMP stateful logging:** Selecting this option will enable the logging of ICMP stateful inspection events.

### Export a stateful configuration

You can export all stateful configurations to a .csv or .xml file by clicking **Export** and selecting the corresponding export action from the list. You can also export specific stateful configurations by first selecting them, clicking **Export** and then selecting the corresponding export action from the list.

### Delete a stateful configuration

To delete a stateful configuration, right-click the configuration in the Firewall Stateful Configurations list, click **Delete** and then click **OK**.

> **Note:** Stateful configurations that are assigned to one or more computers or that are part of a policy cannot be deleted.

### See policies and computers a stateful configuration is assigned to

You can see which policies and computers are assigned to a stateful inspection configuration on the **Assigned To** tab. Click on a policy or computer in the list to see their properties.

## Scan for open ports

The Deep Security Manager can be instructed to scan a computer for open ports by right-clicking the computer and selecting **Actions > Scan for Open ports**, or by clicking the **Scan for Open Ports** button in the **Firewall** page of the **Computer editor**[1] window (where the results of the latest scan are displayed).

(Port scans can also be initiated by right-clicking an existing computer on the Manager's **Computers** page and choosing "Scan for Open Ports". Another way to initiate port scans is to create a **Scheduled Task** to regularly carry out port scans on a list of computers.)

By default, the range of ports that are scanned is the range known as the "Common Ports", 1-1024, but you can define a different set of ports to scan.

> **Note:** The agent's port number for incoming heartbeat connections from the Manager is always scanned regardless of port range settings. It is the port on the computer to which communications initiated by the Manager are sent. If communication direction is set to

[1] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

"Agent/Appliance Initiated" for a computer (**Computer or Policy editor**[1] **> Settings > General**), however, that port number will be closed.

1. Go to **Policies > Common Objects > Lists > Port Lists** and click **New** in the menu bar. The **New Port List** window will appear.
2. Type a name and description for the new port list and then define the ports in the **Port(s)** text box using the accepted formats. (For example, to scan ports 100, 105, and 110 through 120, you would type "100" on the first line "105" on the second, and "110-120" on the third.) Click **OK**.
3. Go to **Computer or Policy editor**[2] **> Settings > General** and click the "Ports to Scan" menu. Your newly defined Port List will be one of the choices.

## Container Firewall rules

If you are using Deep Security Agent 11.2 or higher to protect containers that use an overlay network, you may need to add some Firewall rules to allow network traffic for the Swarm or Kubernetes services because the default Firewall rules block that traffic.

### Kubernetes Firewall rules

If you are using Kubernetes, add the following rules to bypass the k8s communication traffic and export service traffic:

| Name | Action Type | Priority | Direction | Frame Type | Protocol | Source IP | Source Port | Destination IP | Destination Port |
|---|---|---|---|---|---|---|---|---|---|
| HTTP incoming TCP 80 destination port | Force Allow | 0 - Lowest | Incoming | IP | TCP | Any | N/A | Any | 80 |
| HTTP outgoing TCP 80 | Force Allow | 0 - Lowest | Outgoing | IP | TCP | Any | 80 | Any | Any |

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

| Name | Action Type | Priority | Direction | Frame Type | Protocol | Source IP | Source Port | Destination IP | Destination Port |
|---|---|---|---|---|---|---|---|---|---|
| source port | | | | | | | | | |
| K8s incoming TCP 10054 port | Force Allow | 0 - Lowest | Incoming | IP | TCP | Any | Any | Any | 10054 |
| K8s outgoing TCP 10054 port | Force Allow | 0 - Lowest | Outgoing | IP | TCP | Any | Any | Any | 10054 |
| K8s outgoing TCP 443 port | Force Allow | 0 - Lowest | Outgoing | IP | TCP | Any | Any | Any | 443 |
| K8s outgoing TCP 6443 port | Force Allow | 0 - Lowest | Incoming | IP | TCP | Any | Any | Any | 6443 |
| K8s outgoing TCP 6443 port | Force Allow | 0 - Lowest | Outgoing | IP | TCP | Any | Any | Any | 6443 |
| K8s outgoing TCP 8081 port | Force Allow | 0 - Lowest | Incoming | IP | TCP | Any | Any | Any | 8081 |
| K8s outgoing TCP 8081 port | Force Allow | 0 - Lowest | Outgoing | IP | TCP | Any | Any | Any | 8081 |
| K8s outgoing UDP 8472 port | Force Allow | 0 - Lowest | Outgoing | IP | UDP | Any | Any | Any | 8472 |
| K8s outgoing UDP 8285 port | Force Allow | 0 - Lowest | Outgoing | IP | UDP | Any | Any | Any | 8285 |

| Name | Action Type | Priority | Direction | Frame Type | Protocol | Source IP | Source Port | Destination IP | Destination Port |
|---|---|---|---|---|---|---|---|---|---|
| K8s outgoing UDP 8285 port | Force Allow | 0 - Lowest | Incoming | IP | UDP | Any | Any | Any | 8285 |

## Swarm Firewall rules

If you are using Swarm, add the following rules to bypass the k8s communication traffic and export service traffic:

| Name | Action Type | Priority | Direction | Frame Type | Protocol | Source IP | Source Port | Destination IP | Destination Port |
|---|---|---|---|---|---|---|---|---|---|
| HTTP incoming TCP 80 destination port | Force Allow | 0 - Lowest | Incoming | IP | TCP | Any | N/A | Any | 80 |
| HTTP outgoing TCP 80 source port | Force Allow | 0 - Lowest | Outgoing | IP | TCP | Any | 80 | Any | Any |
| Swarm outgoing TCP 443 port | Force Allow | 0 - Lowest | Outgoing | IP | TCP | Any | Any | Any | 443 |
| Swarm incoming TCP 2377, 4789, 7946, 60012 port | Force Allow | 0 - Lowest | Incoming | IP | TCP+UDP | Any | Any | Any | 2377, 4789, 7946, 60012 |
| Swarm outgoing TCP 2377, 4789, 7946, 60012 port | Force Allow | 0 - Lowest | Outgoing | IP | TCP+UDP | Any | 2377, 4789, 7946, 60012 | Any | Any |

# Configure Device Control

## About Device Control

The Device Control module regulates access to external storage devices that are connected to computers. Device Control helps prevent data leaks and, combined with file scanning, helps guard against security risks.

Device Control's enforcement setting (in a policy or computer's **Device Control** tab) can be set to three options for each supported device type which from unlimited to restricted is "Full-Access", "Read-Only", and "Block".

Actions against a specific device type will be taken when that type of device is connected to the protected endpoint. If a user's action triggers the violation, Device Control events will be sent to Deep Security Console (in **Events & Reports > Events > Device Control Events**).

Exceptions can be added to a policy or a computer (in the computer's **Device Control tab > Exceptions**) to allow for full access for the device even when the action is set to "Read-Only" or "Block".

To enable and configure Device Control, see Set up Device Control.

## Device Control protocols

### Actions against device type

When Device Control is enabled, each device type is assigned a "protocol," the permissions users have when they access it.

| Protocol | Read | Copy | Exclude | Write | Delete |
|---|---|---|---|---|---|
| Full-Access | ✓ | ✓ | ✓ | ✓ | ✓ |
| Read-Only | ✓ | ✓ | ✕ | ✕ | ✕ |
| Block | ✕ | ✕ | ✕ | ✕ | ✕ |

### USB Autorun

Device Control allows you to prevent the execution of USB autorun when a USB device is connected to a computer.

## Set up Device Control

1. Go to **Policies**. (Alternatively, to enable it on a specific computer, go to the computer's **Device Control** tab.)
2. Double-click the policy for which you want to enable Device Control.
3. Select **Device Control > General**.
4. For **Device Control State**, select **On**.
5. Select **Save**.

## Configure protocols

The following table shows available action settings for each device type.

| | Available setting | Description |
|---|---|---|
| USB Mass Storage<br>**Note:** This feature is supported by Deep Security Agent 20.0.0-4959+ for Windows. | • Full Access<br>• Read Only<br>• Block | Configure access policy of USB devices |
| USB AutoRun Function | • Allow<br>• Block | Allow or block USB device auto run |
| Mobile (MTP/PTP)<br>**Note:** This is not currently supported by the agent for Windows Server Core. | • Allow<br>• Block | Configure access policy of USB mobile device |

## Configure USB device exceptions

### Create new device

To allow access to specific USB devices when USB Mass Storage is set to Block or Read Only, set exception rules.

For each exception rule, type a name, then specify Vendor, Model, and Serial Number.

An access violation will be bypassed if the access matches the Vendor, Model, and Serial Number in exception rules. For information on USB devices, see Excluding USB storage devices and mobile phones in Device Control.

### Select existing devices

Existing devices can appear in multiple policies. To include existing devices in a policy, click **Select existing devices in lists** and select the relevant devices.

## Device Control event tagging

The events generated by the Device Control module are displayed in the Deep Security console, under **Events & Reports > Device Control Events**. Event tagging can help you to sort events and determine which events need to be investigated further and which events are legitimate.

You can manually apply tags to events by right-clicking the event and then clicking **Add Tag(s)**. You can choose to apply the tag to only the selected event or to any similar Device Control events.

You can also use the auto-tagging feature to group and label multiple events. To configure this feature in the Deep Security console, go to **Events and Reports > Device Control Events > Auto-Tagging > New Trusted Source**. There are three sources that you can use to perform the tagging:

- A Local Trusted Computer.
- The Trend Micro Certified Safe Software Service.
- A Trusted Common Baseline, which is a set of file states collected from a group of computers.

For more information on event tagging, see Apply tags to identify and group events.

# Configure Integrity Monitoring

## About Integrity Monitoring

The integrity monitoring module scans for unexpected changes to registry values, registry keys, services, processes, installed software, ports and files on Deep Security Agents. Using a baseline secure state as a reference, the integrity monitoring module performs scans on the above and logs an event (and an optional alert) if it detects any unexpected changes.

To enable and configure integrity monitoring, see "Set up Integrity Monitoring" below.

To more information on creating integrity monitoring rules, see "Create an Integrity Monitoring rule" on page 909. You can create a rule from a file or registry monitoring template, or by using the Deep Security XML-based "About the Integrity Monitoring rules language" on page 913.

## Set up Integrity Monitoring

The Integrity Monitoring protection module detects changes to files and critical system areas like the Windows registry that could indicate suspicious activity. It does this by comparing current conditions to a baseline reading it has previously recorded. Deep Security ships with predefined Integrity Monitoring rules and new Integrity Monitoring rules are provided in security updates.

Integrity Monitoring detects changes made to the system, but does not prevent or undo the changes.

You can enable Integrity Monitoring in policies or at the computer level by performing the following:

1. "Enable Integrity Monitoring" on the next page
2. "Run a Recommendation scan" on the next page
3. "Apply the Integrity Monitoring rules" on page 903
4. "Build a baseline for the computer" on page 905
5. "Periodically scan for changes" on page 905
6. "Test Integrity Monitoring" on page 905

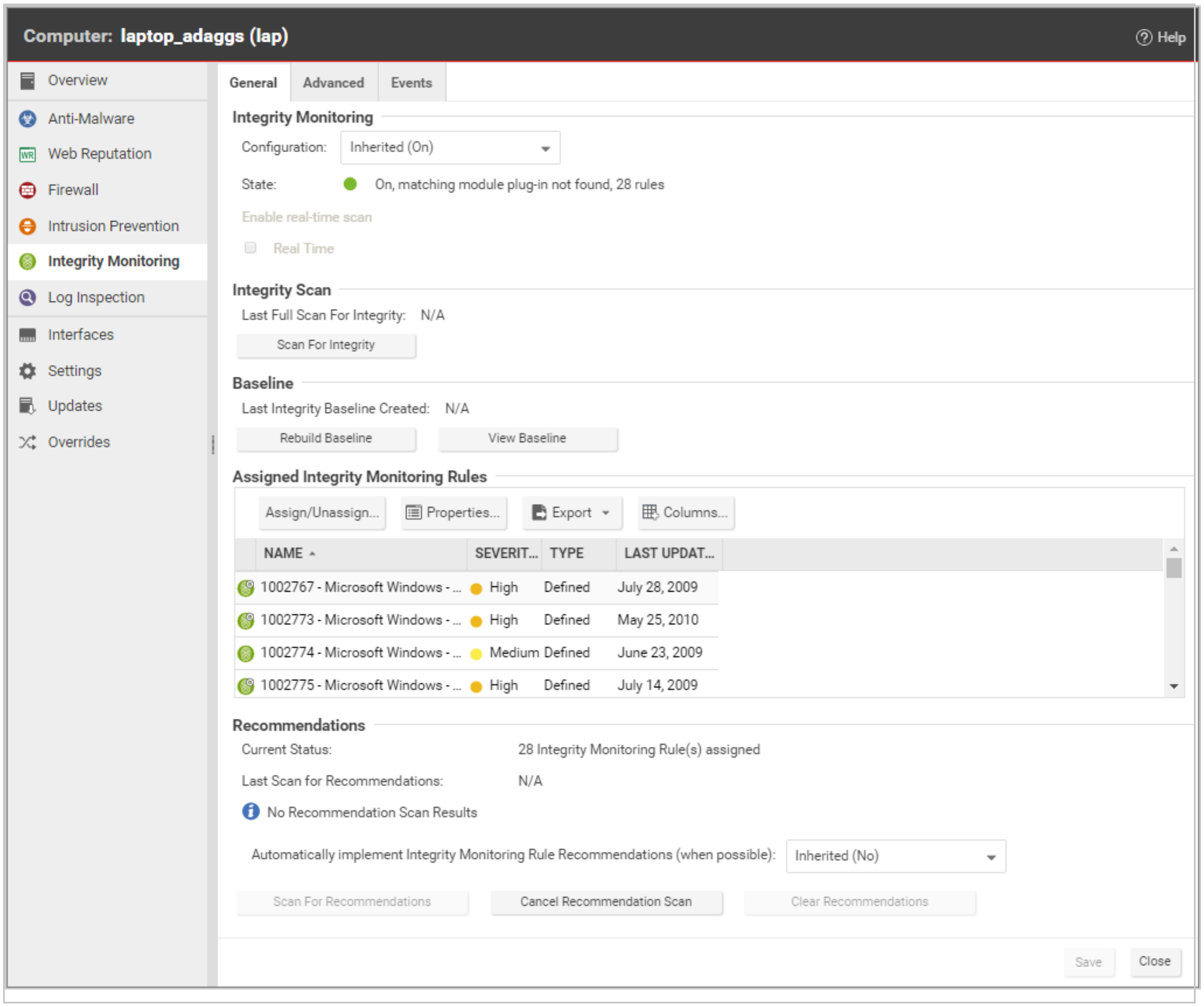
Once you have enabled Integrity Monitoring, you may familiarize yourself with the following topics:

- "Types of Integrity Monitoring scans" on page 906
- "Integrity Monitoring scan performance settings" on page 907

- "Integrity Monitoring event tagging" on page 908

## Enable Integrity Monitoring

You can enable Integrity Monitoring in the settings for a computer or in policies. To do this, open the **Policy** or **Computer** editor and go to **Integrity Monitoring** > **General**. Set **Configuration** to On or Inherited (On), and then click **Save**.



Integrity Monitoring

Configuration: Inherited (On)

State: On, matching module plug-in not found, 28 rules

Enable real-time scan

□ Real Time

Integrity Scan

Last Full Scan For Integrity: N/A

Baseline

Last Integrity Baseline Created: N/A

Assigned Integrity Monitoring Rules

| NAME | SEVERIT... | TYPE | LAST UPDAT... |
|---|---|---|---|
| 1002767 - Microsoft Windows - ... | High | Defined | July 28, 2009 |
| 1002773 - Microsoft Windows - ... | High | Defined | May 25, 2010 |
| 1002774 - Microsoft Windows - ... | Medium | Defined | June 23, 2009 |
| 1002775 - Microsoft Windows - ... | High | Defined | July 14, 2009 |

Recommendations

Current Status: 28 Integrity Monitoring Rule(s) assigned

Last Scan for Recommendations: N/A

No Recommendation Scan Results

Automatically implement Integrity Monitoring Rule Recommendations (when possible): Inherited (No)

## Run a Recommendation scan

Run a Recommendation scan on the computer to get recommendations about which rules would be appropriate. To do this, open the **Computer** editor and go to **Integrity Monitoring** > **General**.

In the **Recommendations** section, click **Scan for Recommendations**. You can optionally specify that Deep Security should implement the rule recommendations that it finds.

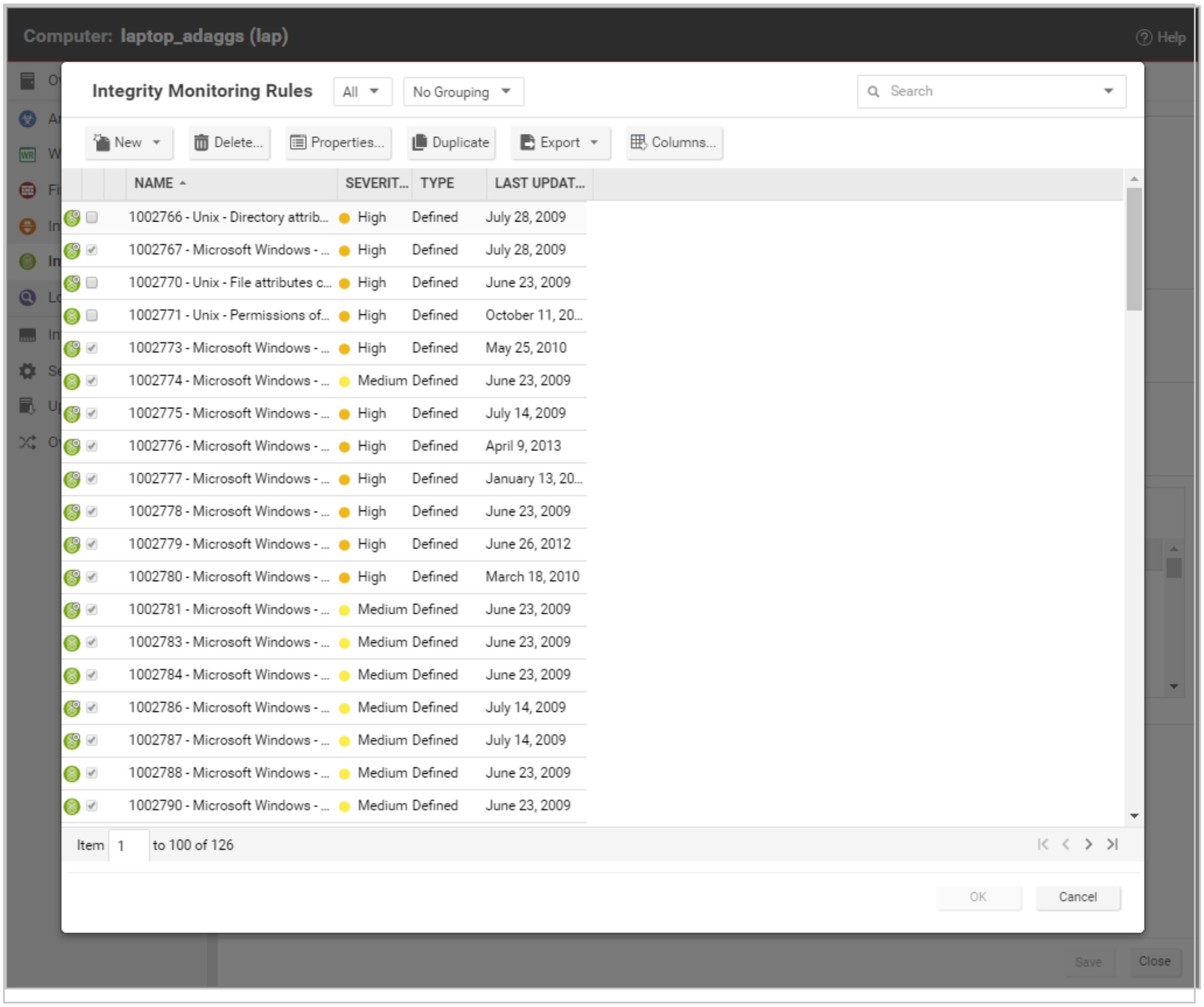
Recommended Integrity Monitoring rules may result in too many monitored entities and attributes. The best practice is to decide what is critical and should be monitored, then create custom rules or tune the predefined rules. Pay extra attention to rules that monitor frequently-changed properties such as process IDs and source port numbers because they can be noisy and may need some tuning.

If you have enabled real-time integrity monitoring scans and find that some recommended rules produce too many events because they are monitoring directories that change frequently, you can disable real-time scanning for those rules. Go to **Policies > Common Objects > Rules > Integrity Monitoring Rules** and double-click the rule. On the **Options** tab, deselect **Allow Real Time Monitoring**.

## Apply the Integrity Monitoring rules

When you run a Recommendation scan, you can have Deep Security implement the recommended rules automatically. You can also manually assign rules.

In the **Computer** or **Policy** editor, go to **Integrity Monitoring** > **General**. The **Assigned Integrity Monitoring Rules** section displays the rules that are in effect for this policy or computer. To add or remove Integrity Monitoring Rules, click **Assign/Unassign**. This displays a window showing all available Integrity Monitoring Rules, from which you can select or deselect rules.



| | NAME | SEVERIT... | TYPE | LAST UPDAT... |
|---|---|---|---|---|
| □ | 1002766 - Unix - Directory attrib... | ● High | Defined | July 28, 2009 |
| ☑ | 1002767 - Microsoft Windows - ... | ● High | Defined | July 28, 2009 |
| □ | 1002770 - Unix - File attributes c... | ● High | Defined | June 23, 2009 |
| □ | 1002771 - Unix - Permissions of... | ● High | Defined | October 11, 20... |
| ☑ | 1002773 - Microsoft Windows - ... | ● High | Defined | May 25, 2010 |
| ☑ | 1002774 - Microsoft Windows - ... | ● Medium | Defined | June 23, 2009 |
| ☑ | 1002775 - Microsoft Windows - ... | ● High | Defined | July 14, 2009 |
| ☑ | 1002776 - Microsoft Windows - ... | ● High | Defined | April 9, 2013 |
| ☑ | 1002777 - Microsoft Windows - ... | ● High | Defined | January 13, 20... |
| ☑ | 1002778 - Microsoft Windows - ... | ● High | Defined | June 23, 2009 |
| ☑ | 1002779 - Microsoft Windows - ... | ● High | Defined | June 26, 2012 |
| ☑ | 1002780 - Microsoft Windows - ... | ● High | Defined | March 18, 2010 |
| ☑ | 1002781 - Microsoft Windows - ... | ● Medium | Defined | June 23, 2009 |
| ☑ | 1002783 - Microsoft Windows - ... | ● Medium | Defined | June 23, 2009 |
| ☑ | 1002784 - Microsoft Windows - ... | ● Medium | Defined | June 23, 2009 |
| ☑ | 1002786 - Microsoft Windows - ... | ● Medium | Defined | July 14, 2009 |
| ☑ | 1002787 - Microsoft Windows - ... | ● Medium | Defined | July 14, 2009 |
| ☑ | 1002788 - Microsoft Windows - ... | ● Medium | Defined | June 23, 2009 |
| ☑ | 1002790 - Microsoft Windows - ... | ● Medium | Defined | June 23, 2009 |

Item 1 to 100 of 126

Some Integrity Monitoring rules written by Trend Micro require local configuration to function properly. If you assign one of these rules to your computers or one of these rules gets assigned automatically, an alert is raised to notify you that configuration is required.

You can edit an Integrity Monitoring rule locally so that the changes apply only to the computer or policy being edited, or globally so that the changes apply to all other policies or computers that are using the rule. To edit a rule locally, right-click it and click **Properties**. To edit a rule globally, right-click it and click **Properties (Global)**.

You can also create custom rules to monitor for specific changes that concern your organization, such as a new user being added or new software being installed. For information on how to create a custom rule, see "About the Integrity Monitoring rules language" on page 913.

Integrity Monitoring rules should be as specific as possible to improve performance and to avoid conflicts and false positives. For example, do not create a rule that monitors the entire hard drive.

## Build a baseline for the computer

The baseline is the original secure state against which an Integrity Scan's results are compared. To create a new baseline for Integrity Scans on a computer, open the **Computer** editor, go to **Integrity Monitoring** > **General** and click **Rebuild Baseline**.

To view the current baseline data, click **View Baseline**.

> **Note:** Due to performance issues related to large amounts of baseline data, in the latest version of Deep Security Manager, **View Baseline** is not visible. For more information, see Database performance issue due to lots of Integrity Monitoring baseline data.

It is recommended to run a new baseline scan after applying patches.

## Periodically scan for changes

Periodically scan for changes. To perform an on-demand scan, open the **Computer** editor, go to **Integrity Monitoring** > **General** and click **Scan for Integrity**. You can also create a scheduled task that performs scans on a regular basis.

## Test Integrity Monitoring

Before continuing with further Integrity Monitoring configuration steps, test that the rules and baseline are working correctly:

1. Ensure Integrity Monitoring is enabled.
2. Go to the **Computer or Policy editor**[1] **> Integrity Monitoring > Assigned Integrity Monitoring Rules**. Click **Assign/Unassign**.
3. If you are a Windows user, search for **1002773 - Microsoft Windows - 'Hosts' file modified** and enable the rule. This rule raises an alert when changes are made to `C:\windows\system32\drivers\etc\hosts`.

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

If you are a Linux user, search for **1003513 - Unix - File attributes changes in /etc location** and enable the rule. This rule raises an alert when changes are made to the `/etc/hosts` file.

4. Modify the preceding file and save the changes.
5. Go to **Computer editor**[1] **> Integrity Monitoring > General** and click **Scan for Integrity**.
6. Go to **Events & Reports > Integrity Monitoring Events** to verify the record of the modified host file. If the detection is recorded, the Integrity Monitoring module is working correctly.

## Types of Integrity Monitoring scans

There are three options for performing Integrity Monitoring scans:

- **On-demand scans:** You can initiate an on-demand integrity monitoring scan as needed by opening the **Computer editor**[2], and going to **Integrity Monitoring > General**. In the Integrity Scan section, click **Scan for Integrity**.
- **Scheduled scans:** You can schedule integrity monitoring scans just like other Deep Security operations. Deep Security checks the entities that are being monitored and identifies and records an event for any changes since the last time it performed a scan. Multiple changes to monitored entities between scans are not tracked; only the last change are detected. To detect and report multiple changes to an entity's state, consider increasing the frequency of scheduled scans (for example, daily instead of weekly) or enable real-time scanning for entities that change frequently. To enable scheduled integrity monitoring scans, go to **Administration > Scheduled Tasks > New**. In the New Scheduled Task Wizard, select **Scan Computers for Integrity Changes** and the frequency for the scheduled scan. Fill in the information requested by the **New Scheduled Task Wizard** with your desired specifications. For more information on scheduled tasks, see "Schedule Deep Security to perform tasks" on page 1600.
- **Real-time scans:** You can enable real-time scanning. When this option is selected, Deep Security monitors entities for changes in real time and raises integrity monitoring events when it detects changes. Events are forwarded in real time via syslog to the SIEM or when the next heartbeat communication to the Deep Security Manager occurs. To enable real-

[1] **To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).**

[2] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

time scans, go to the **Computer or Policy Editor**[1] **> Integrity Monitoring > General** and select **Real Time**. With Deep Security Agent 11.0 or later on 64-bit Linux platforms and with Deep Security Agent 11.2 or later on 64-bit Windows servers, the real-time scan results indicate the user and process that changed the file. For details about which platforms support this feature, see "Supported features by platform" on page 425.

> **Note:** Real-time monitoring of an entire disk for changes to any file would affect performance and result in too many integrity monitoring events. As a safeguard, if you choose to monitor the root drive (C:\) in real time, Deep Security only monitors executable files and scripts. If you want to perform real-time monitoring of all files, specify a folder other than the root drive.

## Integrity Monitoring scan performance settings

Changing the following settings may help to improve the performance of Integrity Monitoring scans:

### Limit CPU usage

Integrity Monitoring uses local CPU resources during the system scan that leads to the creation of the initial baseline and during the system scan that compares a later state of the system to the previously created baseline. If you are finding that Integrity Monitoring is consuming more resources than you want it to, you can restrict the CPU usage to the following levels:

- **High:** Scans files one after another without pausing
- **Medium:** Pauses between scanning files to conserve CPU resources
- **Low:** Pauses between scanning files for a longer interval than the medium setting

To change the **Integrity Monitoring CPU Usage Level** setting, open the **Computer or Policy editor**[2] and go to **Integrity Monitoring** > **Advanced**.

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

#### Change the content hash algorithm

You can select the hash algorithms to be used by the Integrity Monitoring module to store baseline information. You can select more than one algorithm, but this is not recommended because of the detrimental effect on performance.

You can change the content hash algorithm

#### Enable a VM Scan Cache configuration

Using scan caching for Integrity Monitoring improves the efficiency of scans by eliminating the unnecessary scanning of identical content across multiple VMs in large VMware deployments. To select which scan cache configuration is used by a virtual machine, open the **Computer or Policy editor**[1] and go to **Integrity Monitoring > Advanced > VM Scan Cache**.

### Integrity Monitoring event tagging

The events generated by the Integrity Monitoring module are displayed in Deep Security Manager, under **Events & Reports** > **Integrity Monitoring Events**. Event tagging can help you to sort events and determine which ones are legitimate and which ones need to be investigated further.

You can manually apply tags to events by right-clicking the event and then clicking **Add Tag(s)**. You can choose to apply the tag to only the selected event or to any similar Integrity Monitoring events.

You can also use the auto-tagging feature to group and label multiple events. To configure this feature in the Deep Security Manager, go to **Events and Reports** > **Integrity Monitoring Events** > **Auto-Tagging** > **New Trusted Source**. There are three sources that you can use to perform the tagging:

- A Local Trusted Computer.
- The Trend Micro Certified Safe Software Service.
- A Trusted Common Baseline, which is a set of file states collected from a group of computers.

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

For more information on event tagging, see "Apply tags to identify and group events" on page 1057.

## Create an Integrity Monitoring rule

Integrity Monitoring rules describe how Deep Security Agents should scan for and detect changes to a computer's files, directories, and registry keys and values, as well as changes in installed software, processes, listening ports, and running services. Integrity Monitoring rules can be assigned directly to computers or can be made part of a policy.

> **Note:** This article specifically covers how to create an Integrity Monitoring rule. For information on how to configure the Integrity Monitoring module, see "Set up Integrity Monitoring" on page 901.

There are two types of Integrity Monitoring rules: those that you have created, and those that are issued by Trend Micro. For more information on how to configure rules issued by Trend Micro, see the "Configure Trend Micro Integrity Monitoring rules" on page 911 section.

To create a new Integrity Monitoring rule, you need to:

1. "Add a new rule" below.
2. "Enter Integrity Monitoring rule information " on the next page.
3. "Select a rule template and define rule attributes" on the next page.

When you're done with your rule, you can also learn how to

- "Configure rule events and alerts" on page 912
- "See policies and computers a rule is assigned to" on page 913
- "Export a rule" on page 913
- "Delete a rule" on page 913

### Add a new rule

There are three ways to add an Integrity Monitoring rule on the **Policies** > **Common Objects** > **Rules** > **Integrity Monitoring Rules** page. You can:

- Create a new rule. Click **New** > **New Integrity Monitoring Rule**.
- Import a rule from an XML file. Click **New** > **Import From File**.

- Copy and then modify an existing rule. Right-click the rule in the Integrity Monitoring Rules list and then click **Duplicate**. To edit the new rule, select it and then click **Properties**.

## Enter Integrity Monitoring rule information

1. Enter a **Name** and **Description** for the rule.

   > **Tip:** It is good practice to document all Integrity Monitoring rule changes in the Description field of the rule. Make a note of when and why rules were created or deleted for easier maintenance.

2. Set the **Severity** of the rule.

   > **Note:** Setting the severity of a rule has no effect on how the rule is implemented or applied. Severity levels can be useful as sorting criteria when viewing a list of Integrity Monitoring rules. More importantly, each severity level is associated with a severity value; this value is multiplied by a computer's Asset Value to determine the ranking of an event. (See **Administration > System Settings > Ranking**.)

## Select a rule template and define rule attributes

Go to the **Content** tab and select from one of the following three templates:

### Registry Value template

Create an Integrity Monitoring rule to specifically monitor changes to registry values.

> **Note:** The Registry Value template is only for Windows-based computers .

1. Select the **Base Key** to monitor and whether or not to monitor contents of sub keys.
2. List **Value Names** to be included or excluded. You can use "?" and "*" as wildcard characters.
3. Enter **Attributes** to monitor. Entering "STANDARD" will monitor changes in registry size, content and type. For more information on Registry Value template attributes see the "RegistryValueSet" on page 945 documentation.

### File template

Create an Integrity Monitoring rule to specifically monitor changes to files.

1. Enter a **Base Directory** for the rule (for example, `C:\Program Files\MySQL`.) Select **Include Sub Directories** to include the contents of all subdirectories relative to the base directory. Wildcards are not supported for base directories.
2. Use the **File Names** fields to include or exclude specific files. You can use wildcards ("`?`" for a single character and "`*`" for zero or more characters.

   > **Note:** Leaving the **File Names** fields blank will cause the rule to monitor all files in the base directory. This can use significant system resources if the base directory contains numerous or large files.

3. Enter **Attributes** to monitor. Entering "STANDARD" will monitor changes in file creation date, last modified date, permissions, owner, group, size, content, flags (Windows), and SymLinkPath (Linux). For more information on File template attributes see the "FileSet" on page 929 documentation.

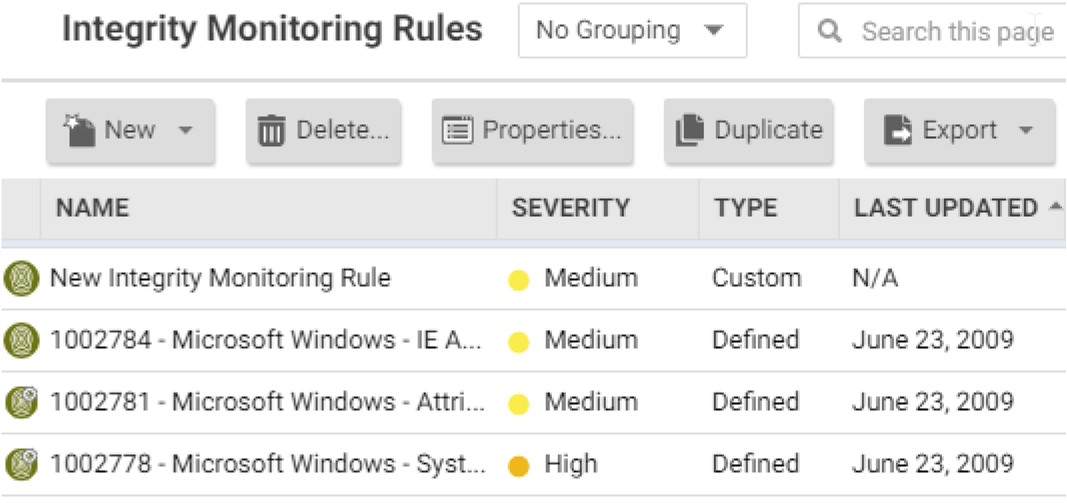
### Custom (XML) template

Create a custom Integrity Monitoring rule template to monitor directories, registry values, registry keys, services, processes, installed software, ports, groups, users, files, and the WQL using the Deep Security XML-based "About the Integrity Monitoring rules language" on page 913.

> **Tip:** You can create your rule in your preferred text editor and paste it to the **Content** field when you are done.

## Configure Trend Micro Integrity Monitoring rules

Integrity Monitoring rules issued by Trend Micro cannot be edited in the same way as the custom rules you create. Some Trend Micro rules cannot be modified at all, while other rules may offer limited configuration options. Both of these rule types will show as "Defined" under the "Type" column, but rules that can be configured will display a gear in the Integrity Monitoring icon (⚙).



| NAME | SEVERITY | TYPE | LAST UPDATED |
|---|---|---|---|
| New Integrity Monitoring Rule | ● Medium | Custom | N/A |
| 1002784 - Microsoft Windows - IE A... | ● Medium | Defined | June 23, 2009 |
| 1002781 - Microsoft Windows - Attri... | ● Medium | Defined | June 23, 2009 |
| 1002778 - Microsoft Windows - Syst... | ● High | Defined | June 23, 2009 |

You can access the configuration options for a rule by opening the properties for the rule and clicking on the **Configuration** tab.

Rules issued by Trend Micro also show the following additional information under the **General** tab:

- When the rule was first issued and last updated, as well as a unique identifier for the rule.
- The minimum versions of the Agent and the Deep Security Manager that are required for the rule to function.

Although you cannot edit rules issued by Trend Micro directly, you can duplicate them and then edit the copy.

## Configure rule events and alerts

Any changes detected by an Integrity Monitoring rule is logged as an event in the Deep Security Manager.

### Real-time event monitoring

By default, events are logged at the time they occur. If you only want events to be logged when you manually perform a scan for changes, deselect **Allow Real Time Monitoring**.

### Alerts

You can also configure the rules to trigger an alert when they log an event. To do so, open the properties for a rule, click on **Options**, and then select **Alert when this rule logs an event**.

### See policies and computers a rule is assigned to

You can see which policies and computers are assigned to an Integrity Monitoring rule on the **Assigned To** tab. Click on a policy or computer in the list to see their properties.

### Export a rule

You can export all Integrity Monitoring rules to a .csv or .xml file by clicking **Export** and selecting the corresponding export action from the list. You can also export specific rules by first selecting them, clicking **Export** and then selecting the corresponding export action from the list.

### Delete a rule

To delete a rule, right-click the rule in the Integrity Monitoring Rules list, click **Delete** and then click **OK**.

> **Note:** Integrity Monitoring rules that are assigned to one or more computers or that are part of a policy cannot be deleted.

## Integrity Monitoring rules language

### About the Integrity Monitoring rules language

The Integrity Monitoring rules language is a declarative XML-based language that describes the system components and associated attributes that should be monitored by Deep Security. It also provides a means to specify what components within a larger set of components should be excluded from monitoring.

> **Tip:** If you only need to monitor for unauthorized changes to files or the Windows registry, you can use File and Registry rule templates instead of creating a custom one. For more information on using these templates, see "Create an Integrity Monitoring rule" on page 909.

To create a new custom Integrity Monitoring rule, start with the procedure in "Create an Integrity Monitoring rule" on page 909 (selecting **Custom (XML)** as the template type), then create your custom rule according to the Integrity Monitoring rules language, as covered in the following sections:

### Entity Sets

System components included in an Integrity Monitoring rule are referred to as "Entities". Each type of component is a class of Entity. For example, files, registry keys, and processes are each a class of Entity. The Integrity Monitoring Rules language provides a tag for describing a set of Entities (an Entity Set) for each class of Entity. The following **Entity Set** types are available to be used in a rule:

- "DirectorySet" on page 926: rules will scan the integrity of directories
- "FileSet" on page 929: rules will scan the integrity of files
- "GroupSet" on page 934**:** rules will scan the integrity of groups
- "InstalledSoftwareSet" on page 935: rules will scan the integrity of installed software
- "PortSet" on page 938**:** rules will scan the integrity of listening ports
- "ProcessSet" on page 941: rules will scan the integrity of processes
- "RegistryKeySet" on page 944: rules will scan registry keys
- "RegistryValueSet" on page 945: rules will scan registry values
- "ServiceSet" on page 948: rules will scan the integrity of services

- "UserSet" on page 950: rules will scan the integrity of users
- "WQLSet" on page 954: rules will monitor the integrity of the results of a Windows Management Instrumentation WQL query statement

A single Integrity Rule can contain multiple Entity Sets. This allows you to, for example, secure an application with a single rule that monitors multiple files and registry entries.

#### Hierarchies and wildcards

For Entity Sets that represent a hierarchical data type such as FileSet and RegistryKeySet, section-based pattern matching is supported:

- `/` (forward slash) : demarcates sections of the pattern to be applied to levels of the hierarchy
- `**` (two stars) : matches zero or more sections

The following wildcards are supported:

- `?` (question mark) : matches one character
- `*` (one star) : matches zero or more characters

"Escaping" characters is also supported:

- `\` (back slash) : escapes the next character

The pattern is divided into sections using the " `/` " character, with each section of the pattern being applied to successive levels of the hierarchy as long as it continues to match. For example, if the pattern:

```
/a?c/123/*.java
```

is applied to the path:

```
/abc/123/test.java
```

Then:

- `"a?c` " matches "abc"
- `"123` " matches "123"
- `"*.java` " matches "test.java"

When the pattern is applied to the path:

```
/abc/123456/test.java
```

Then:

- `"a?c` " matches "abc"
- " `123` " does *not* match "123456", and so no more matching is performed

The " `**` " notation pattern matches zero or more sections, and so:

```
/abc/**/*.java
```

matches both "abc/123/test.java" and "abc/123456/test.java". It would also match "abc/test.java" and "abc/123/456/test.java".

### Syntax and concepts

This section will present some example Integrity Monitoring rules. The examples will use the **FileSet** Entity Set but the topics and components described are common to all Entity Sets. A minimal Integrity Monitoring rule could look like this:

```
<FileSet base="C:\Program Files\MySQL">
 </FileSet>
```

The "base" attribute specifies the base directory for the FileSet. Everything else about the rule will be relative to this directory. If nothing further is added to the rule, everything (including subdirectories) below the "base" will be monitored for changes.

> **Note:** The " `*` " and " `?` " wildcards can be used in a "base" attribute string, but only in the last path component of the base. So this is valid:
>
> `base="C:\program files\CompanyName * Web Server"`
>
> but this is not:
>
> `base="C:\* files\Microsoft Office"`

Within an Entity Set, "include" and "exclude" tags can be used to control pattern matching. These tags have a "key" attribute that specifies the pattern to match against. The source of the key varies by Entity Set. For example, for Files and Directories it is their path, while for Ports it is the unique protocol/IP/portNumber tuple.

**Note:** If a path supplied in an include or exclude rule is syntactically invalid, the Agent will generate an "Integrity Monitoring Rule Compile Issue" Agent Event and supply the rule ID and the path (after expansion) as parameters. An example of an invalid path would be `C:\test1\D:\test2` since a file name may not contain two volume identifiers.

### Include tag

The include tag is essentially an allow list. Using it means that only those Entities matched by it (or other include tags) will be included. By adding an include tag, the following rule now only monitors changes to files with the name "*.exe" in the "C:\Program Files\MySQL" folder and sub folders:

```
<FileSet base="C:\Program Files\MySQL">
 <include key="**/*.exe"/>
 </FileSet>
```

"Includes" can be combined. The following rule will monitor changes to files with the names "*.exe" and "*.dll" in the "C:\Program Files\MySQL" folder and sub folders:

```
<FileSet base="C:\Program Files\MySQL">
 <include key="**/*.exe"/>
 <include key="**/*.dll"/>
 </FileSet>
```

It is also possible to combine multiple criteria in a single include block, in which case **all** criteria must be true for a given Entity to be included. The following "include" tag requires that an Entity both end in ".exe" and start with "sample" to be included. Although this requirement could be represented more succinctly, the usefulness of this becomes more apparent as key patterns are combined with other features of the Entity, as described in the "Features" section below.

```
<include>
 <key pattern="**/*.exe"/>
 <key pattern="**/sample*"/>
 </include>
```

The following is another way to express the same requirements:

```
<include key="**/*.exe">
 <key pattern="**/sample*"/>
 </include>
```

### Exclude tag

The exclude tag functions as a block list, removing files from the set that would otherwise be returned. The following (unlikely) example would place everything but temp files under watch.

```
<FileSet base="C:\Program Files\MySQL">
 <include key="**"/>
 <exclude key="**/*.tmp"/>
 </FileSet>
```

The following rule excludes the "MySQLInstanceConfig.exe" from the set of EXEs and DLLs:

```
<FileSet base="C:\Program Files\MySQL">
 <include key="**/*.exe"/>
 <include key="**/*.dll" />
 <exclude key="**/MySQLInstanceConfig.exe"/>
 </FileSet>
```

Like the "include" tag, the "exclude" tag can be written to require multiple criteria. The following example shows a multi-criteria "exclude" tag.

```
<exclude>
 <key pattern="**/MySQLInstanceConfig*" />
 <key pattern="**/*.exe" />
 </exclude>
```

### Case sensitivity

The case sensitivity of pattern matching for an include or exclude tag may be controlled by the "casesensitive" attribute. The attribute has three allowed values:

- **true**
- **false**
- **platform**

The default value for this attribute is "platform", which means that the case sensitivity of the pattern will match the platform on which it is running. In the following example, both "Sample.txt" and "sample.txt" would be returned on a Windows system, but only "Sample.txt" would be returned on a Unix system:

```
<FileSet base="C:\Program Files\MySQL">
 <include key="**/*Sample*"/>
 </FileSet>
```

In this example, only "Sample.txt" would be returned on Windows and Unix:

```
<FileSet base="C:\Program Files\MySQL">
 <include key="**/*Sample*" casesensitive="true"/>
 </FileSet>
```

**Note:** A case sensitive setting of "true" is of limited use on a platform such as Windows which is case insensitive when it comes to most object names.

### Entity features

The inclusion and exclusion of Entities based on features other than their "key" is also supported for some Entity types. The set of features differs by Entity type. The following example will include all executable files. It does not depend on the file extension as previous examples using file extensions did, but instead will check the first few hundred bytes of the file to determine if it is executable on the given OS.

```
<FileSet base="C:\Program Files\MySQL">
 <include key="**" executable="true"/>
 </FileSet>
```

Feature attributes must appear in an "include" or "exclude" tag. To use them as part of a multi-criteria include or exclude, they must be specified as attributes of the enclosing include or exclude tag. The following example includes all files that contain the string "MySQL" in their name and are also executable:

```
<include executable="true">
 <key pattern="**/*MySQL*"/>
 </include>
```

The previous example can be more succinctly expressed as:

```
<include key="**/*MySQL*" executable="true"/>
```

Some feature attributes are simply matches against the value of one of the Entity's attributes. In such cases, wildcard matches using " `*` " and " `?` " are sometimes supported. The help pages for the individual "Entity Sets" on page 914 indicate which attributes can be used in include or exclude rules in this way, and whether they support wildcard matching or simple string matching.

**Note:** Where wildcard matches *are* supported, it is important to note that the match is against the string value of the attribute and that no normalization takes place. Constructs available for Entity key matches such as `"**` " and the use of " `/` " to separate hierarchical components don't apply. Matching a path name on Windows requires the use of " `\` " since that is the character which appears in the value of the attribute being tested, whereas Unix systems will use " `/` " in path values so matches against Unix paths need to use " `/` ".

The following is an example of a feature match using the "state" attribute:

```
<ServiceSet>
 <include state="running"/>
 </ServiceSet>
```

**Note:** Wildcards are not supported in state matches.

The following example matches any processes where the path of the binary ends in "\notepad.exe":

```
<ProcessSet>
 <include path="*\notepad.exe"/>
 </ProcessSet>
```

The following example matches any processes where the command-line begins with "/sbin/":

```
<ProcessSet>
 <include commandLine="/sbin/*"/>
 </ProcessSet>
```

**Note:** Be careful when using wildcards. A wildcard expression like " `**` " will look at every file in every sub directory beneath "base". Creating a baseline for such an expression can take a lot of time and resources.

#### ANDs and ORs

It is possible to express logical ANDs and ORs through the use of multi-criteria includes and excludes and multiple includes and excludes.

There are several ways that a multi criteria include or exclude can be used to express an AND. The most straightforward is to include multiple criteria within a single enclosing tag. The following example shows a simple multi-criteria AND-ing:

```
<include>
 <key pattern="**/*MySQL*" />
 <key pattern="**/*.exe"/>
 </include>
```

As well, any criteria expressed as an attribute of the including tag will be grouped with the enclosed criteria as part of the multi-criteria requirement. The following example shows the previous multi-criteria "include" re-written in this way:

```
<include key="**/*.exe">
 <key pattern="**/*MySQL*" />
 </include>
```

Finally, if multiple criteria are expressed as attributes of an include or exclude they are treated as an AND:

```
<include executable="true" key="**/*MySQL*" />
```

ORs are expressed simply by the inclusion of multiple include or exclude tags. The following code includes files if their extensions are ".exe" OR ".dll":

```
<include key="**/*.dll" />
 <include key="**/*.exe" />
```

### Order of evaluation

All "includes" are processed first, regardless of order of appearance in the rule. If an object name matches at least one "include" tag, it is then tested against the "exclude" tags. It is removed from the set of monitored objects if it matches at least one "exclude" tag.

### Entity attributes

A given Entity has a set of attributes that can be monitored. If no attributes are specified for an Entity Set (i.e. the attributes wrapper tag is not present) then the STANDARD set of attributes for that Entity is assumed. (See the *Shorthand Attributes* sections for the individual "Entity Sets" on page 914.)

However, for a given Entity Set only certain attributes of the Entity may be of interest for Integrity Monitoring. For example, changes to the contents of a log file are most likely expected and allowed. However changes to the permissions or ownership should be reported.

The "attributes" tag of the Entity Sets allows this to be expressed. The "attributes" tag contains a set of tags enumerating the attributes of interest. The set of allowed "attribute" tags varies depending on the Entity Set for which they are being supplied.

**Note:** If the "attributes" tag is present, but contains no entries, then the Entities defined by the rule are monitored for existence only.

The following example monitors executable files in "C:\Program Files\MySQL" whose name includes "SQL" for changes to their "last modified", "permissions", and "owner" attributes:

```
<FileSet base="C:\Program Files\MySQL" >
 <include key="**/*SQL*" executable="true"/>
 <attributes>
 <lastModified/>
 <permissions/>
 <owner/>
 </attributes>
 </FileSet>
```

The following example monitors the "permissions", and "owner" attributes of log files in "C:\Program Files\MySQL":

```
<FileSet base="C:\Program Files\MySQL" >
 <attributes>
 <permissions/>
 <owner/>
 </attributes>
 <include key="**/*.log" />
 </FileSet>
```

In the following example, the STANDARD set of attributes will be monitored. (See Shorthand Attributes, below)

```
<FileSet base="C:\Program Files\MySQL" >
 <include key="**/*.log" />
 </FileSet>
```

In the following example, no attributes will be monitored. Only the existence of the Entities will be tracked for change.

```
<FileSet base="C:\Program Files\MySQL" >
 <attributes/>
 <include key="**/*.log" />
 </FileSet>
```

#### Shorthand attributes

Shorthand attributes provide a way to specify a group of attributes using a single higher level attribute. Like regular attributes the set of allowed values differs based on the Entity Set for which they are being supplied.

Shorthand Attributes are useful in cases where a set of attributes naturally group together, in cases where exhaustively listing the set of attributes would be tedious, and in cases where the set of attributes represented by the high level attribute may change with time or system configuration. An example of each case follows:

| Attribute | Description |
|---|---|
| STANDARD | The set of attributes to monitor for the Entity Set. This is different than "every possible attribute" for the Entity Set. For example, it would not include every possible hash algorithm, just the ones deemed sufficient. For the list of "standard" attributes for each Entity Set, see sections for the individual "Entity Sets" on page 914. |
| CONTENTS | This is Shorthand for the hash, or set of hashes, of the contents of the file. Defaults to SHA-1. |

#### onChange attribute

An EntitySet may be set to monitor changes in real time. If the onChange attribute of an EntitySet is set to true (the default value) then the entities returned by the EntitySet will be monitored for changes in real time. When a change is detected the Entity is immediately compared against its baseline for variation. If the onChange attribute of an EntitySet is set to false, it will be run only when a baseline is built or when it is triggered via a scheduled task or on demand by the Deep Security Manager.

The following sample monitors the MySQL binaries in real time:

```
<FileSet base="C:\Program Files\MySQL" onChange="true">
 <include key="**/*.exe"/>
 <include key="**/*.dll" />
 </FileSet>
```

#### Environment variables

Environment variables can be included in the base value used in Entity Sets. They are enclosed in "${}". The variable name itself is prefaced with "env.".

The following example sets the base directory of the FileSet to the path stored in the PROGRAMFILES environment variable:

```
<FileSet base="${env.PROGRAMFILES}"/>
```

**Note:** The values of referenced environment variables are read and stored by the Deep Security Agent on Agent startup. If the value of an environment variable changes, the Agent must be restarted to register the change.

If a referenced environment variable is not found, the Entity Sets referencing it are not scanned or monitored, but the rest of the configuration is used. An alert is triggered indicating that the variable is not present. The Agent reports an invalid environment variable using Agent event "Integrity Monitoring Rule Compile Issue". The ID of the Integrity Monitoring rule and the environment variable name are supplied as parameters to the event.

The following are the default environment variables that Integrity Monitoring uses:

| Name | Value |
|---|---|
| ALLUSERSPROFILE | C:\ProgramData |
| COMMONPROGRAMFILES | C:\Program Files\Common Files |
| PROGRAMFILES | C:\Program Files |
| SYSTEMDRIVE | C: |
| SYSTEMROOT | C:\Windows |
| WINDIR | C:\Windows |

## Environment variable overrides

Override environment variables when non-standard locations are used in the Windows operating system. For example, the **Microsoft Windows - 'Hosts' file modified** Integrity Monitoring rule, which monitors changes to the Windows `hosts` file, looks for that file in the `C:\WINDOWS\system32\drivers\etc` folder. However not all Windows installations use the `C:\WINDOWS\` directory, so the Integrity Monitoring rule uses the `WINDIR` environment variable and represents the directory as `%WINDIR%\system32\drivers\etc`.

**Note:** Environment variables are used primarily by the virtual appliance when performing agentless Integrity Monitoring on a virtual machine. This is because the virtual appliance has no way of knowing if the operating system on a particular virtual machine is using standard directory locations.

1. Open the Computer or Policy editor[1] where you want to override an environment variable.
2. Click **Settings > Advanced**.
3. In the **Environment Variable Overrides** section, click **View Environment Variables** to display the **Environment Variable Overrides** page.
4. Click **New** in the menu bar and enter a new name-value pair (for example, `WINDIR` and `D:\Windows`) and click **OK**.

### Registry values

Registry values can be included in the base value used in Entity Sets. They are enclosed in ${}. The path to the registry value itself is prefaced with "reg.". The following example sets the base directory of the FileSet to the path stored in the `"HKLM\Software\Trend Micro\Deep Security Agent\InstallationFolder`" registry value:

```
<FileSet base="${reg.HKLM\Software\Trend Micro\Deep Security
Agent\InstallationFolder}"/>
```

The values of referenced registry values are read when a new or changed rule is received by the Agent. The Agent also checks all rules at startup time and will rebuild the baseline for affected Rules if any referenced registry values change.

If a referenced registry value is not found, the EntitySets referencing it are not scanned or monitored, but the rest of the configuration is used. An alert notifying that the variable is not present is raised. The Agent reports an invalid environment variable expansion using Agent Event 8012. The ID of the Integrity Monitoring rule and the registry value path are supplied as parameters to the event.

**Note:** A wildcard is allowed only in the last hierarchical component of a base name. For example, `base="HKLM\Software\ATI*"` is valid and will find both "HKLM\Software\ATI" and "HKLM\Software\ATI Technologies"; however, `base="HKLM\*\Software\ATI*` is invalid.

### Use of ".."

The ".." convention for referencing a parent directory is supported in all current versions of the Agent. The Agent will attempt to normalize base directory names for FileSet and DirectorySet elements by resolving ".." references and converting Windows short names to long names. For

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

example, on some newer versions of Windows the following FileSet would have a base directory of `C:\Users`. On earlier versions of Windows it would be `C:\Documents and Settings`.

```
<FileSet base="${env.USERPROFILE}\..">
 <include key="*/Start Menu/Programs/Startup/*"/>
 </FileSet>
```

**Best practices**

Rules should be written to only include objects and attributes that are of significance. This will ensure that no events are reported if other attributes of the object change. For example, your change monitoring policy may place restrictions on permission and ownership of files in `/bin`. Your Integrity Monitoring rule should monitor owner, group, and permissions, but not other attributes like lastModified or hash values.

When using Integrity Monitoring rules to detect malware and suspicious activity, monitor services, watch for use of NTFS data streams, and watch for executable files in unusual places such as "`/tmp`" or "`${env.windir}\temp`".

Always be as specific as possible when specifying what objects to include in a rule. The fewer objects you include, the less time it will take to create your baseline and the less time it will take to scan for changes. Exclude objects which are expected to change and only monitor the attributes you are concerned about.

When creating a rule, do not:

- Use "`**/...`" from a top-level of the hierarchy such as "`/`", "C:\", or "`HKLM\Software`".
- Use more than one content hash type unless absolutely necessary.
- Reference user-specific locations such as `HKEY_CURRENT_USER`, `${env.USERPROFILE}`, or `${env.HOME}`.

Any of these statements in your integrity monitoring rules will cause performance issues as the Deep Security Agent searches through many items in order to match the specified patterns.

## DirectorySet

**Note:** The Integrity Monitoring module scans for unexpected changes to directories, registry values, registry keys, services, processes, installed software, ports, groups, users, files, and the WQL query statement on Deep Security Agents. To enable and configure Integrity Monitoring, see "Set up Integrity Monitoring" on page 901.

The DirectorySet tag describes a set of Directories.

### Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

| Attribute | Description | Required | Default Value | Allowed Values |
|---|---|---|---|---|
| base | Sets the base directory of the DirectorySet. Everything else in the tag is relative to this directory | Yes | N/A | String values resolving to syntactically valid path (Path is not required to exist) **Note**: UNC paths are allowed by Windows Agents, but require that the remote system allow access by the "LocalSystem" account of the Agent computer. The Agent is a Windows service and runs as LocalSystem, aka NT AUTHORITY\SYSTEM. When accessing a network resource, the LocalSystem uses the computer's credentials, which is an account named *DOMAIN\MACHINE*$. The access token presented to the remote computer also contains the "Administrators" group for the computer, so remote shares must grant read privileges to either the Agent computer's account, the Agent computer's Administrators group, or "Everyone". For testing access to UNC paths, launch a Windows command prompt running as a service under the LocalSystem account. With that, you can try accessing network and local resources, or launch other applications that will run under the LocalSystem account.<br>If the base value is not syntactically valid, the FileSet will not be processed. The rest of the config will be evaluated. |
| onChange | Whether the directories returned should be monitored in real time. | No | false | true, false |
| followLinks | Will this DirectorySet follow symbolic links. | No | false | true, false |

### Entity Set Attributes

These are the attributes of the Entity that may be monitored by Integrity Monitoring Rules.

- **Created:** Timestamp when the directory was created
- **LastModified:** Timestamp when the directory was last modified
- **LastAccessed:** Timestamp when the directory was last accessed. On Windows this value does not get updated immediately, and recording of the last accessed timestamp can be disabled as a performance enhancement. See File Times for details. The other problem with this attribute is that the act of scanning a directory requires that the Agent open the directory, which will change its last accessed timestamp.
- **Permissions:** The directory's security descriptor (in SDDL format) on Windows or Posix-style ACLs on Unix systems that support ACLs, otherwise the Unix style rwxrwxrwx file permissions in numeric (octal) format.
- **Owner:** User ID of the directory owner (commonly referred to as the "UID" on Unix)
- **Group:** Group ID of the directory owner (commonly referred to as the "GID" on Unix)
- **Flags:** Windows-only. Flags returned by the GetFileAttributes() Win32 API. Windows Explorer calls these the "Attributes" of the file: Read-only, Archived, Compressed, etc.
- **SymLinkPath:** If the directory is a symbolic link, the path of the link is stored here. On Windows, use the SysInternals "junction" utility to create the Windows equivalent of symbolic links.
- **InodeNumber** (Unix and Linux only): Inode number of the disk on which the inode associated with the file is stored
- **DeviceNumber** (Unix and Linux only): Device number of the disk on which the inode associated with the directory is stored

### Short Hand Attributes

The following are the Short Hand Attributes, and the attributes to which they map.

- **STANDARD:**
  - Created
  - LastModified
  - Permissions
  - Owner
  - Group

- Flags (Windows only)
- SymLinkPath

#### Meaning of "Key"

Key is a pattern to match against the path of the directory relative to the directory specified by "dir". This is a hierarchical pattern, with sections of the pattern separated by "/" matched against sections of the path separated by the file separator of the given OS.

#### Sub Elements

- **Include**
- **Exclude**

See "About the Integrity Monitoring rules language" on page 913 for a general description of Include and Exclude for their allowed attributes and sub elements. Only information specific to includes and excludes relating to this EntitySet class are included here.

## FileSet

> **Note:** The Integrity Monitoring module scans for unexpected changes to directories, registry values, registry keys, services, processes, installed software, ports, groups, users, files, and the WQL query statement on Deep Security Agents. To enable and configure Integrity Monitoring, see "Set up Integrity Monitoring" on page 901.

The FileSet tag describes a set of Files.

#### Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

| Attribute | Description | Required | Default Value | Allowed Values |
|---|---|---|---|---|
| base | Sets the base directory of the FileSet. Everything else in the tag is relative to this directory. | Yes | N/A | String values resolving to syntactically valid path (Path is not required to exist). **Note**: UNC paths are allowed by Windows Agents, but require that the remote system allow access by the "LocalSystem" account of the Agent computer. The Agent is a Windows service and runs as LocalSystem, |

| Attribute | Description | Required | Default Value | Allowed Values |
|---|---|---|---|---|
| | | | | aka NT AUTHORITY\SYSTEM. When accessing a network resource, the LocalSystem uses the computer's credentials, which is an account named *DOMAIN\MACHINE*$. The access token presented to the remote computer also contains the "Administrators" group for the computer, so remote shares must grant read privileges to either the Agent computer's account, the Agent computer's Administrators group, or "Everyone". For testing access to UNC paths, launch a Windows command prompt running as a service under the LocalSystem account. With that, you can try accessing network and local resources, or launch other applications that will run under the LocalSystem account.<br>If the base value is not syntactically valid, the FileSet will not be processed. The rest of the config will be evaluated. |
| onChange | Whether the files returned should be monitored in real time. | No | false | true, false |
| followLinks | Will this FileSet follow symbolic links. | No | false | true, false |

#### Entity Set Attributes

These are the attributes of the FileSet that can be monitored by Integrity Monitoring Rules.

**Note:** For Created, LastModified, and LastAccessed in a Linux environment, the Real-time Integrity Monitoring module detects scans where the file contents have changed, but does not detect a change such as touching a file, reading a file, or any other change that updates only metadata such as the time a file was altered.

- **Created:** Timestamp when the file was created
- **LastModified:** Timestamp when the file was last modified

- **LastAccessed:** Timestamp when the file was last accessed. On Windows this value does not get updated immediately, and recording of the last accessed timestamp can be disabled as a performance enhancement. See File Times for details. The other problem with this attribute is that the act of scanning a file requires that the Agent open the file, which will change its last accessed timestamp. On Unix, the Agent will use the O_NOATIME flag if it is available when opening the file, which prevents the OS from updating the last accessed timestamp and speeds up scanning.
- **Permissions:** The file's security descriptor (in SDDL format) on Windows or Posix-style ACLs on Unix systems that support ACLs, otherwise the Unix style rwxrwxrwx file permissions in numeric (octal) format.
- **Owner:** User ID of the file owner (commonly referred to as the "UID" on Unix)
- **Group:** Group ID of the file owner (commonly referred to as the "GID" on Unix)
- **Size:** size of the file
- **Sha1:** SHA-1 hash
- **Sha256:**SHA-256 hash
- **Md5:** MD5 hash (deprecated)
- **Flags:** Windows-only. Flags returned by the GetFileAttributes() Win32 API. Windows Explorer calls these the "Attributes" of the file: Read-only, Archived, Compressed, etc.
- **SymLinkPath** (Unix and Linux only): If the file is a symbolic link, the path of the link is stored here. Windows NTFS supports Unix-like symlinks, but only for directories, not files. Windows shortcut objects are not true symlinks since they are not handled by the OS; the Windows Explorer handles shortcut files (*.lnk) but other applications that open a *.lnk file will see the contents of the lnk file.
- **InodeNumber** (Unix and Linux only): Inode number of the disk on which the inode associated with the file is stored
- **DeviceNumber** (Unix and Linux only): Device number of the disk on which the inode associated with the file is stored
- **BlocksAllocated** (Linux and Unix only): The number of blocks allocated to store the file.
- **Growing:** If the size of the file stays the same or increases between scans the value is "true", otherwise "false". This is mainly useful for log files that have data appended to them. Note that rolling over a log file will trigger a change in this attribute.
- **Shrinking:** If the size of the file stays the same or decreases between scans the value is "true", otherwise "false".

### Short Hand Attributes

The following are the Short Hand Attributes, and the attributes to which they map.

- **CONTENTS:** Resolves to the content hash algorithm set in **Computer or Policy editor**[1] **> Integrity Monitoring > Advanced**.
- **STANDARD:** Created, LastModified, Permissions, Owner, Group, Size, Contents, Flags (Windows only), SymLinkPath (Unix only)

### Drives Mounted as Directories

Drives mounted as directories are treated as any other directory, unless they are a network drive in which case they are ignored.

### Alternate Data Streams

NTFS based file systems support the concept of alternate data streams. When this feature is used it behaves conceptually like files within the file.

**Note:** To demonstrate this, type the following at the command prompt:

```
echo plain > sample.txt
echo alternate > sample.txt:s
more < sample.txt
more < sample.txt:s
```

The first "more" will show only the text "plain", the same text that will be displayed if the file is opened with a standard text editor, such as notepad. The second "more", which accesses the "s" stream of sample.txt will display the string "alternate".

For FileSets, if no stream is specified, then all streams are included. Each stream is a separate Entity entry in the baseline. The available attributes for streams are:

- **size**
- **Sha1**

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

- **Sha256**
- **Md5** (deprecated)
- **Contents**

The following example would include both streams from the demonstration above:

```
<include key="**/sample.txt" />
```

To include or exclude specific streams, the ":" notation is used. The following example matches only the "s" stream on sample.txt and not the main sample.txt stream:

```
<include key="**/sample.txt:s" />
```

Pattern matching is supported for the stream notation. The following example would include sample.txt, but exclude all of its alternate streams:

```
<include key="**/sample.txt" />
 <exclude key="**/sample.txt:*" />
```

#### Meaning of "Key"

Key is a pattern to match against the path of the file relative to the directory specified by "base". This is a hierarchical pattern, with sections of the pattern separated by "/" matched against sections of the path separated by the file separator of the given OS

#### Sub Elements

- **Include**
- **Exclude**

See "About the Integrity Monitoring rules language" on page 913 for a general description of Include and Exclude for their allowed attributes and sub elements. Only information specific to includes and excludes relating to the FileSet Entity Set class are included here.

#### Special attributes of Include and Exclude for FileSets:

### executable

Determines if the file is executable. This does not mean that its permissions allow it to be executed. Instead the contents of the file are checked, as appropriate for platform, to determine if the file is an executable file.

**Note:** This is a relatively expensive operation since it requires the Agent to open the file and examine the first kilobyte or two of its content looking for a valid executable image header. Opening and reading every file is much more expensive than simply scanning directories and matching file names based on wild card patterns, so any include and exclude rules using "executable" will result in slower scan times than those that do not use it.

## GroupSet

**Note:** The Integrity Monitoring module scans for unexpected changes to directories, registry values, registry keys, services, processes, installed software, ports, groups, users, files, and the WQL query statement on Deep Security Agents. To enable and configure Integrity Monitoring, see "Set up Integrity Monitoring" on page 901.

GroupSet represents a set of groups. Note these are local groups only.

### Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

| Attribute | Description | Required | Default Value | Allowed Values |
|---|---|---|---|---|
| onChange | Will be monitored in real time | No | false | true, false |

### Entity Set Attributes

These are the attributes of the entity that can be monitored:

- **Description:** (Windows only) The textual description of the group.
- **Group:** The group ID and name. The group name is part of the entity key, but it's still important to be able to monitor the group ID-name pairing in case groups are renamed and given new IDs. Operating systems generally enforce security based on its ID.
- **Members:** A comma separated list of the members of the group.
- **SubGroups:** (Windows only) A comma separated list of sub-groups of the group.

### Short Hand Attributes

- **Standard:** Group Members SubGroups

### Meaning of "Key"

The key is the group's name. This is not a hierarchical Entity Set. Patterns are applied only to the group name. As a result the "**" pattern is not applicable. The following example monitors the "Administrators" group for additions and deletions. (The "Member" attribute is included implicitly because it is a part of the STANDARD set, and no attributes are explicitly listed.)

```
<GroupSet>
 <include key="Administrators" />
 </GroupSet>
```

### Include and Exclude

See "About the Integrity Monitoring rules language" on page 913 for a general description of Include and Exclude and their allowed attributes and sub elements.

## InstalledSoftwareSet

**Note:** The Integrity Monitoring module scans for unexpected changes to directories, registry values, registry keys, services, processes, installed software, ports, groups, users, files, and the WQL query statement on Deep Security Agents. To enable and configure Integrity Monitoring, see "Set up Integrity Monitoring" on page 901.

Represents a set of installed software. The "key" used to uniquely identify an installed application is platform-specific, but it is often a shorthand version of the application name or a unique numeric value.

On Windows, the key can be something readable like "FogBugz Screenshot_is1" or it can be a GUID like
 "{90110409-6000-11D3-8CFE-0150048383C9}". You can examine these by looking at the sub-keys of HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

On Linux the key is the RPM package name, as shown by the command:

```
rpm -qa --qf "%{NAME}\n"
```

On Solaris the key is the package name as shown by the **pkginfo** command.

### Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the computer where Integrity Monitoring is enabled.

| Attribute | Description | Required | Default Value | Allowed Values |
|---|---|---|---|---|
| onChange | Will be monitored in real time | No | false | true, false |

### Entity Set Attributes

These are the attributes of the Entity that can be monitored by Integrity Monitoring Rules. Presence of the attributes is dependent on both the platform and the application itself - installation programs do not necessarily populate all of the attributes.

- **Manufacturer:** The publisher or manufacturer of the application
- **Name:** The friendly name or display name of the application. (Not available on Linux.)
- **InstalledDate:** Date of installation. This is normally returned as YYYY-MM-DD [HH:MM:SS], but many installers on Windows format the date string in a different manner so this format is not guaranteed. (Not available on AIX.)
- **InstallLocation:** The directory where the application is installed. (Only available on Windows and Solaris.)
- **Parent:** For patches and updates, this gives the key name of this item's parent. (Only available on Windows.)
- **Size:** The estimated size of the application, if available. On Windows this attribute is read from the "EstimatedSize" registry value under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\*. The value in that location is expressed in KB, so the Agent multiplies it by 1024 before returning the value. Note that not all Windows applications populate the EstimatedSize field in the registry. (Not available on AIX.)
- **Version:** The version of the installed application. On Windows, this comes from the "DisplayVersion" registry value.

### Short Hand Attributes

These are the short hand attributes of the Entity and the attributes to which they resolve

- **STANDARD:** InstalledDate, Name, Version

### Meaning of "Key"

The key is the name of the installed software. This is not a hierarchical key, so the ** pattern does not apply. On Windows the key is often a GUID, especially for anything installed via the Windows Installer (aka MSI). Use the name="XXX" feature if you need to include or exclude based on the display name rather than the GUID.

The following example would monitor for the addition and deletion of new software.

```
<InstalledSoftwareSet>
 <include key="*"/>
 <attributes/>
 </InstalledSoftwareSet>
```

### Sub Elements

- **Include**
- **Exclude**

See "About the Integrity Monitoring rules language" on page 913 for a general description of Include and Exclude for their allowed attributes and sub elements. Only information specific to includes and excludes relating to this EntitySet class are included here.

### Special attributes of Include and Exclude for InstalledSoftwareSets:

#### name (Windows only)

Allows wildcard matching using ? and * on the display name of the application (the "name" attribute of the Entity). For example:

```
<InstalledSoftwareSet>
 <include name="Microsoft*"/>
 <InstalledSoftwareSet>
```

will match all installed applications whose display name (as shown by the Control Panel) starts with "Microsoft".

#### manufacturer

Allows wildcard matching using ? and * on the publisher or manufacturer of the application. For example:

```
<InstalledSoftwareSet>
 <include manufacturer="* Company "/>
 <InstalledSoftwareSet>
```

will match all installed applications whose manufacturer ends with " Company ".

## PortSet

**Note:** The Integrity Monitoring module scans for unexpected changes to directories, registry values, registry keys, services, processes, installed software, ports, groups, users, files, and the WQL query statement on Deep Security Agents. To enable and configure Integrity Monitoring, see "Set up Integrity Monitoring" on page 901.

Represents a set of listening ports.

### Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

| Attribute | Description | Required | Default Value | Allowed Values |
|---|---|---|---|---|
| onChange | Will be monitored in real time | No | false | true, false |

### Entity Set Attributes

These are the attributes of the Entity that can be monitored by Integrity Monitoring Rules.

- **Created:** Windows only - XP SP2+ and Server 2003 SP1+ required. Returned by the GetExtendedTcpTable() or GetExtendedUdpTable() functions of the Windows API. Indicates when the bind operation that created this TCP or UDP link occurred.
- **Listeners:** The number of active listeners on this protocol, IP address, and port number combination. This reflects the number of sockets bound-to and listening-on the given port, and may be greater than the number of processes listening on the port if processes bind multiple sockets to the port. This attribute has no value if only one socket is bound to the given port.
- **Path:** (Windows only - XP SP2+ and Server 2003 SP1+ required.) Gives the full path, if available, of the module that owns the port. On Windows this comes from the GetOwnerModuleFromXxxEntry() functions of the Windows API. According to Microsoft documentation, the resolution of connection table entries to owner modules is a best practice.
- **Process:** (Windows only - XP SP2+ and Server 2003 SP1+ required.) Gives the short name, if available, of the module that owns the port. On Windows this comes from the GetOwnerModuleFromXxxEntry() functions of the Windows API. According to Microsoft documentation, the resolution of connection table entries to owner modules is a best

practice. In a few cases, the owner module name returned can be a process name, such as "svchost.exe", a service name (such as "RPC"), or a component name, such as "timer.dll".

- **ProcessId:** (Windows only - XP SP2+ and Server 2003 SP1+ required.) Gives the PID of the process that issued the bind for this port.
- **User:** (Linux only). Gives the user that owns the port.

#### Meaning of "Key"

The key is in the following format:

<PROTOCOL>/<IP ADDRESS>/<PORT>

For example:

```
tcp/172.14.207.94/80
 udp/172.14.207.94/68
```

#### IPV6

If the IP address is IPv6 the key is in the same format, but the protocol is TCP6 or UDP6 and the IP address is an IPv6 address as returned by the getnameinfo command:

```
tcp6/3ffe:1900:4545:3:200:f8ff:fe21:67cf/80
 udp6/3ffe:1900:4545:3:200:f8ff:fe21:67cf/68
```

#### Matching of the Key

This is not a hierarchical key, so ** is not applicable. Unix-style glob matching is possible using * and ?. The following pattern matches port 80 on the IP addresses 72.14.207.90 through 72.14.207.99:

```
*/72.14.207.9?/80
```

The following pattern matches port 80 on the IP addresses 72.14.207.2, 72.14.207.20 through 72.14.207.29 as well as 72.14.207.200 through 72.14.207.255:

```
*/72.14.207.2*/80
```

The following pattern matches port 80 on any IP.

```
*/80
```

The following example would monitor for any change in the listening ports but ignore port 80 for TCP in IPv4 and IPv6:

```
<PortSet>
 <include key="*"/>
 <exclude key="tcp*/*/80"/>
 </PortSet>
```

### Sub Elements

- **Include**
- **Exclude**

See "About the Integrity Monitoring rules language" on page 913 for a general description of Include and Exclude and their allowed attributes and sub elements. Only information specific to includes and excludes relating to this EntitySet class are included here.

#### Special attributes of Include and Exclude for PortSets:

Various other attributes of the port may be used in include and exclude feature tests. These tests compare a value against the value of an attribute of the port; take note of the platform support for various attributes - not all attributes are available across platforms or even platform revisions, hence the use of these tests in include and exclude tags is of limited use. The feature tests support Unix glob-style wildcarding with * and ?, and there is no normalization of path separators or other characters - it is a simple match against the value of the attribute.

### Path

Checks for a wildcard match against the path attribute of the port. The following example would monitor ports owned by processes running the main IIS binary:

```
<PortSet>
 <include path="*\system32\inetsrv\inetinfo.exe"/>
 </PortSet>
```

### Process

Checks for a wildcard match against the process attribute of the port. The following example would monitor ports owned by anything running in a svchost.exe or outlook.* binary:

```
<PortSet>
 <include process="svchost.exe"/>
 <include process="outlook.*"/>
 </PortSet>
```

### User

Checks for a wildcard match against the user attribute of the port. The following example would monitor ports on a Unix system that were owned by the super-user (root):

```
<PortSet>
 <include user="root"/>
 </PortSet>
```

## ProcessSet

**Note:** The Integrity Monitoring module scans for unexpected changes to directories, registry values, registry keys, services, processes, installed software, ports, groups, users, files, and the WQL query statement on Deep Security Agents. To enable and configure Integrity Monitoring, see "Set up Integrity Monitoring" on page 901.

Represents a set of processes.

### Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

| Attribute | Description | Required | Default Value | Allowed Values |
|---|---|---|---|---|
| onChange | Will be monitored in real time | No | false | true, false |

### Entity Set Attributes

These are the attributes of the Entity that can be monitored by Integrity Monitoring Rules.

- **CommandLine:** The full command-line as shown by "ps -f" (Unix), "ps w" (Linux), or Process Explorer (Windows).
- **Group:** The group under which the process is running.
  - Under Unix this is the "effective" group ID of the process, which determines shared resource access and, in some cases, file access. Group ID can change if the process drops privileges or otherwise switches its effective group credentials. For example, a program could change group IDs temporarily and obtain write privileges to copy installation files into a directory where the user has read-only privileges.
  - On Windows this is the “current" Primary Group of the process as established by a user-specific access token created at login, which sets access and resource privileges for the user and any processes they execute.

> **Note:** In addition to a Primary Group, Windows processes typically have one or more additional group credentials associated with them. These additional group credentials are not monitored by the Agent – they can be viewed in the Security tab of the process properties in Process Explorer.

- **Parent:** The PID of the process that created this process.
- **Path:** The full path to the binary of the process. On Windows, this comes from the GetModuleFileNameEx() API. On Linux and Solaris 10, it comes from reading the symlink /proc/{pid}/exe or /proc/{pid}/path/a.out respectively. (Not available on Solaris 9 and AIX.)
- **Process:** The short name of the process binary (no path). For example, for "c:\windows\notepad.exe" it would be "notepad.exe" and for "/usr/local/bin/httpd" it would be "httpd".
- **Threads:** The number of threads currently executing in the process.
- **User:** The user under which the process is running. Under Unix this is the "effective" user ID of the process, which can change over time if the process drops privileges or otherwise switches its effective user credentials.

### Short Hand Attributes

- **STANDARD:** CommandLine, Group, Parent, Path (where available), Process User

### Meaning of "Key"

The key is a combination of the "Process" attribute (the short name of the executable) and the PID. The PID is appended to the name with a path separator in between, ex. notepad.exe\1234 on Windows and httpd/1234 on Unix. The use of the path separator is to allow include or exclude matching of key="abc/*" to work as expected.

### Sub Elements

- **Include**
- **Exclude**

See "About the Integrity Monitoring rules language" on page 913 for a general description of include for their allowed attributes and sub elements. Only information specific to includes and excludes relating to this EntitySet class are included here.

**Special attributes of Include and Exclude for ProcessSets:**

The following example would monitor the set of running processes for notepad.exe regardless of the PID.

```
<ProcessSet>
 <include key="notepad.exe\*" />
 </ProcessSet>
```

Various other attributes of a process can be used in include and exclude feature tests. The feature tests support Unix glob-style wildcarding with * and ?, and there is no normalization of path separators or other characters - it is a simple glob-style match against the value of the attribute.

### CommandLine

Checks for a wildcard match against the commandLine attribute of the process. The following example would monitor any process whose command-line matches "*httpd *":

```
<ProcessSet>
 <include commandLine="*httpd *" />
 </ProcessSet>
```

### Group

Checks for a wildcard match against the group attribute of the process. The text version of the group name is used rather than the numeric form: use "daemon" rather than "2" to test for the daemon group on Linux. The following example would monitor any process running as one of the groups root, daemon, or lp:

```
<ProcessSet>
 <include group="root" />
 <include group="daemon" />
 <include group="lp" />
 </ProcessSet>
```

### Path

Checks for a wildcard match against the path attribute of the process. The path attribute is not available on some platforms. The following example would monitor any process whose binary resides under System32:

```
<ProcessSet>
 <include path="*\System32\*" />
 </ProcessSet>
```

#### User

Checks for a wildcard match against the user attribute of the process. The text version of the user name is used rather than the numeric form: use "root" rather than "0" (zero) to test for the superuser on Unix. The following example would monitor any process running as one of the built in system users (ex. NT AUTHORITY\SYSTEM, NT AUTHORITY\LOCAL SERVICE, NT AUTHORITY\NETWORK SERVICE):

```
<ProcessSet>
 <include user="NT AUTHORITY\*" />
 </ProcessSet>
```

## RegistryKeySet

**Note:** The Integrity Monitoring module scans for unexpected changes to directories, registry values, registry keys, services, processes, installed software, ports, groups, users, files, and the WQL query statement on Deep Security Agents. To enable and configure Integrity Monitoring, see "Set up Integrity Monitoring" on page 901.

The RegistryKeySet tag describes a set keys in the registry (Windows only).

### Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

| Attribute | Description | Required | Default Value | Allowed Values |
|---|---|---|---|---|
| base | Sets the base key of the RegistryKeySet. Everything else in the tag is relative to this key. The base must begin with one of the following registry branch names:<br>HKEY_CLASSES_ROOT (or HKCR),<br>HKEY_LOCAL_MACHINE (or HKLM),<br>HKEY_USERS (or HKU),<br>HKEY_CURRENT_CONFIG (or HKCC) | Yes | N/A | String values resolving to syntactically valid registry key path |

### Entity Set Attributes

These are the attributes of the Entity that can be monitored by Integrity Monitoring Rules.

- **Owner**
- **Group**
- **Permissions**
- **LastModified** ("LastWriteTime" in Windows registry terminology)
- **Class**
- **SecurityDescriptorSize**

### Short Hand Attributes

- **STANDARD:** Group, Owner, Permissions, LastModified

### Meaning of "Key"

Registry Keys are stored hierarchically in the registry, much like directories in a file system. For the purpose of this language the "key path" to a key is considered to look like the path to a directory. For example the "key path" to the "Deep Security Agent" key of the Agent would be:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\Deep Security Agent
```

The "key" value for includes and excludes for the RegistryValueSet is matched against the key path. This is a hierarchical pattern, with sections of the pattern separated by "/" matched against sections of the key path separated by "\".

### Sub Elements

- **Include**
- **Exclude**

See "About the Integrity Monitoring rules language" on page 913 for a general description of include for their allowed attributes and sub elements.

## RegistryValueSet

> **Note:** The Integrity Monitoring module scans for unexpected changes to directories, registry values, registry keys, services, processes, installed software, ports, groups, users, files, and the WQL query statement on Deep Security Agents. To enable and configure Integrity Monitoring, see "Set up Integrity Monitoring" on page 901.

A set of Registry values (Windows only).

### Tag Attributes

These are XML attributes of the tag itself as opposed to the attributes of the entity monitored by Integrity Monitoring Rules.

| Attribute | Description | Required | Default Value | Allowed Values |
|---|---|---|---|---|
| base | Sets the base key of the RegistryValueSet. Everything else in the tag is relative to this key. The base must begin with one of the registry branch names:<br>HKEY_CLASSES_ROOT (or HKCR),<br>HKEY_LOCAL_MACHINE (or HKLM),<br>HKEY_USERS (or HKU),<br>HKEY_CURRENT_CONFIG (or HKCC) | Yes | N/A | String values resolving to syntactically valid registry key |

### Entity Set Attributes

These are the attributes of the Entity that can be monitored by Integrity Monitoring Rules:

- Size
- Type
- Sha1
- Sha256
- Md5 (deprecated)

### Short Hand Attributes

- **CONTENTS:** Resolves to the content hash algorithm set in **Computer or Policy editor**[1] **> Integrity Monitoring > Advanced**.
- **STANDARD:** Size, Type, Contents

### Meaning of "Key"

Registry Values are name-value pairs stored under a key in the registry. The key under which they are stored may in turn be stored under another key, very much like files and directories on a file system. For the purpose of this language the "key path" to a value is considered to look like

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

the path to a file. For example, the "key path" to the InstallationFolder value of the Agent would be:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Trend Micro\Deep Security
Agent\InstallationFolder
```

The "key" value for includes and excludes for the RegistryValueSet is matched against the key path. This is a hierarchical pattern, with sections of the pattern separated by "/" matched against sections of the key path separated by "\"

### Default Value

Each registry key has an unnamed or default value.

This value can be explicitly specified for inclusion and exclusion by using a trailing "/" in patterns. For example, "**/" will match all subordinate unnamed values, and "*Agent/**/" will match all unnamed values below a key matching "*Agent".

> **Note:** Registry value names can contain any printable character, including quotes, backslash, the "@" symbol, etc.

The Agent deals with this in Entity key names by using backslash as an escape character, but only backslashes themselves are escaped. It does this so that it can tell the difference between a value name containing a backslash and a backslash that occurs as part of the registry path. This means that value names which end with a backslash character will match rules designed to match the default or unnamed value.

See the table below for example registry value names and the resulting Entity key.

| Value | Escaped Form | Example |
|---|---|---|
| Hello | Hello | HKLM\Software\Sample\Hello |
| "Quotes" | "Quotes" | HKLM\Software\Sample\"Quotes" |
| back\slash | back\\slash | HKLM\Software\Sample\back\\slash |
| trailing\ | trailing\\ | HKLM\Software\Sample\trailing\\ |
| | | HKLM\Software\Sample\ |
| @ | @ | HKLM\Software\Sample\@ |

### Sub Elements

- **Include**
- **Exclude**

See "About the Integrity Monitoring rules language" on page 913 for a general description of Include and Exclude for their allowed attributes and sub elements.

## ServiceSet

> **Note:** The Integrity Monitoring module scans for unexpected changes to directories, registry values, registry keys, services, processes, installed software, ports, groups, users, files, and the WQL query statement on Deep Security Agents. To enable and configure Integrity Monitoring, see "Set up Integrity Monitoring" on page 901.

The ServiceSet element represents a set of services (Windows only). Services are identified by the "service name", which is not the same as the "name" column shown in the Services administrative tool. The service name can be seen in the service properties and is often shorter than the value shown in the "name" column, which is actually the "Display Name" of the service. For example, the Agent has a service name of "ds_agent" and a display name of "Trend Micro Deep Security Agent".

### Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

| Attribute | Description | Required | Default Value | Allowed Values |
|---|---|---|---|---|
| onChange | Will be monitored in real time | No | false | true, false |

### Entity Set Attributes

These are the attributes of the Entity that can be monitored by Integrity Monitoring Rules.

- **Permissions:** The service's security descriptor in SDDL format.
- **Owner:** User ID of the service owner
- **Group:** Group ID of the service owner
- **BinaryPathName:** The path plus optional command-line arguments that Windows uses to start the service.
- **DisplayName:** The "display name" of the service as shown in the properties panel of the service.
- **Description:** Description as it appears in the Services panel
- **State:** The current state of the service. One of: stopped, starting, stopping, running, continuePending, pausePending, paused

- **StartType:** How is the service started? One of: automatic, disabled, manual.
- **LogOnAs:** The name of the account that the service process will be logged on as when it runs.
- **FirstFailure:** Action to take the first time the service fails. Format is "delayInMsec,action", where action is one of None, Restart, Reboot, RunCommand.
- **SecondFailure:** Action to take the second time the service fails. Format is "delayInMsec,action", where action is one of None, Restart, Reboot, RunCommand.
- **SubsequentFailures:** Action to take if the service fails for a third or subsequent time. Format is "delayInMsec,action", where action is one of None, Restart, Reboot, RunCommand.
- **ResetFailCountAfter:** Time after which to reset the failure count to zero if there are no failures, in seconds.
- **RebootMessage:** Message to broadcast to server users before rebooting in response to the "Reboot" service controller action.
- **RunProgram:** Full command line of the process to execute in response to the RunCommand service controller action.
- **DependsOn:** Comma separated list of components that the service depends on
- **LoadOrderGroup:** The load ordering group to which this service belongs. The system startup program uses load ordering groups to load groups of services in a specified order with respect to the other groups. The list of load ordering groups is contained in the following registry value: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\ServiceGroupOrder
- **ProcessId:** This is the numeric ID of the process that hosts the service. Many services may exist in a single Windows process, but for those that run in their own process, the monitoring of this attribute will allow the system to log service restarts.

#### Short Hand Attributes

These are the short hand attributes of the Entity and the attributes to which they resolve

- **STANDARD**: Permissions, Owner, Group, BinaryPathName, Description, State, StartType, LogOnAs, FirstFailure, SecondFailure, SubsequentFailures, ResetFailCountAfter, RunProgram, DependsOn, LoadOrderGroup, ProcessId

#### Meaning of "Key"

The key is the Service's name, which is not necessarily the same as the "name" column shown in the Services administrative tool (that tool shows the "display name" of the service). The service name can be seen in the service properties and is often shorter than the value shown in the "name" column.

> **Note:** This is not a hierarchical Entity Set. Patterns are applied only to the service name. As a result the ** pattern is not applicable.

#### Sub Elements

- **Include**
- **Exclude**

See "About the Integrity Monitoring rules language" on page 913 for a general description of include for their allowed attributes and sub elements. Only information specific to includes and excludes relating to this Entity Set class are included here.

#### Special attributes of Include and Exclude for ServiceSets:

**state**

Include or exclude based on whether the state of the service (stopped, starting, stopping, running, continuePending, pausePending, paused). The following example would monitor the set of running services for change:

```
<ServiceSet>
 <include state="running"/>
 </ServiceSet>
```

## UserSet

> **Note:** The Integrity Monitoring module scans for unexpected changes to directories, registry values, registry keys, services, processes, installed software, ports, groups, users, files, and the WQL query statement on Deep Security Agents. To enable and configure Integrity Monitoring, see "Set up Integrity Monitoring" on page 901.

The UserSet element represents a set of users. On a Windows system it operates on users local to the system - the same users displayed by the "Local Users and Groups" MMC snap-in. Note that these are *local* users only if the Deep Security Agent is running on something other than a domain controller. On a domain controller, a UserSet element will enumerate all of the domain users, which may not be advisable for extremely large domains.

On Unix systems, the users monitored are whatever the "getpwent_r()" and "getspnam_r()" APIs have been configured to return. On AIX systems specifically, the users monitored are those listed in the `/etc/passwd` file.

#### Tag Attributes

These are XML attributes of the tag itself, as opposed to the attributes of the Entity monitored by Integrity Monitoring Rules.

| Attribute | Description | Required | Default Value | Allowed Values |
|---|---|---|---|---|
| onChange | Will be monitored in real time | No | false | true, false |

#### Entity Set Attributes

These are the attributes of the entity that can be monitored:

#### Common Attributes

- **cannotChangePassword:** True or false indicating if the user is permitted to change their password.
- **disabled:** True or false indicating if the account has been disabled. On Windows systems this reflects the "disabled" check box for the user. On Unix systems this will be true if the user's account has expired or if their password has expired and they've exceeded the inactivity grace period for changing it.
- **fullName:** The display name of the user.
- **groups:** A comma-separated list of the groups to which the user belongs.
- **homeFolder:** The path to the home folder or directory.
- **lockedOut:** True or false indicating if the user has been locked out, either explicitly or due to excessive failed password attempts.
- **passwordHasExpired:** True or false indicating if the user's password has expired. Note that on Windows this attribute is only available on Windows XP and newer operating systems.
- **passwordLastChanged:** The timestamp of the last time the user's password was changed. This is recorded by the Deep Security Agent as the number of milliseconds since Jan 1 1970 UTC - Deep Security Manager renders the timestamp in local time based on this value. Note that on Unix platforms, the resolution of this attribute is one day, so the time component of the rendered timestamp is meaningless. (Not supported by AIX.)

- **passwordNeverExpires:** True or false indicating if the password does not expire.
- **user:** The name of the user as known to the operating system. For example, "Administrator" or "root".

### Windows-only Attributes

- **description:** The primary group the user belongs to.
- **homeDriveLetter:** The drive letter to which a network share is mapped as the user's home folder.
- **logonScript:** The path to a script that executes every time the user logs in.
- **profilePath:** A network path if roaming or mandatory Windows user profiles are being used.

### Linux, AIX, and Solaris Attributes

- **group:** The primary group the user belongs to.
- **logonShell:** The path to the shell process for the user.
- **passwordExpiredDaysBeforeDisabled:** The number of days after the user's password expires that the account is disabled. On Solaris, this attribute refers to the number of inactive days before the user is disabled. (Not supported by AIX.)
- **passwordExpiry:** The date on which the user's account expires and is disabled.
- **passwordExpiryInDays:** The number of days after which the user's password must be changed.
- **passwordMinDaysBetweenChanges:** The minimum number of days permitted between password changes.
- **passwordWarningDays:** The number of days before the user's password is to expire that user is warned.

### Short Hand Attributes

- **Standard:**
  - cannotChangePassword
  - disabled
  - groups
  - homeFolder
  - passwordHasExpired

- passwordLastChanged
- passwordNeverExpires
- user
- logonScript (Windows-only)
- profilePath (Windows-only)
- group (Linux-only)
- logonShell (Linux-only)
- passwordExpiryInDays (Linux-only)
- passwordMinDaysBetweenChanges (Linux-only)

### Meaning of "Key"

The key is the username. This is not a hierarchical EntitySet. Patterns are applied only to the user name. As a result the "**" pattern is not applicable.

The following example monitors for any user creations or deletions. (Note that attributes are explicitly excluded so group membership would not be tracked):

```
<UserSet>
 <Attributes/>
 <include key="*" />
 </UserSet>
```

The following example would track the creation and deletion of the "jsmith" account, along with any changes to the STANDARD attributes of the account (since the STANDARD set for this EntitySet is automatically included if no specific attribute list is included):

```
<UserSet>
 <include key="jsmith" />
 </UserSet>
```

### Sub Elements

### Include and Exclude

See "About the Integrity Monitoring rules language" on page 913 for a general description of include for their allowed attributes and sub elements.

### Special attributes of Include and Exclude for UserSets

Various other attributes of the user may be used in include and exclude feature tests. These tests compare a value against the value of an attribute of the user; take note of the platform support for various attributes - not all attributes are available across platforms or even platform revisions, hence the use of these tests in include and exclude elements is of limited use. The feature tests support Unix glob-style wildcarding with * and ?, and there is no normalization of path separators or other characters - it is a simple match against the value of the attribute.

- **Disabled:** Does true or false match the disabled attribute of the user. The following example monitors users with a primary group of either "users" or "daemon":

  ```
  <UserSet>
   <include disabled="true"/>
   </UserSet>
  ```

- **Group:** Does a wildcard match against the primary group of the user. This test is only applicable on Unix systems. The following example would monitor users with a primary group of either "users" or "daemon".

  ```
  <UserSet>
   <include group="users"/>
   <include group="daemon"/>
   </UserSet>
  ```

- **LockedOut:** Does a true or false match against the lockedOut attribute of the user.
- **PasswordHasExpired:** Does a true or false match against the passwordHasExpired attribute of the user.
- **PasswordNeverExpires:** Does a true or false match against the passwordNeverExpires attribute of the user.

## WQLSet

> **Note:** The Integrity Monitoring module scans for unexpected changes to directories, registry values, registry keys, services, processes, installed software, ports, groups, users, files, and the WQL query statement on Deep Security Agents. To enable and configure Integrity Monitoring, see "Set up Integrity Monitoring" on page 901.

The WQLSet element describes a result set from a Windows Management Instrumentation WQL query statement. WQL allows SQL-like queries to be made against many different object classes, with the results forming a table of rows where each row represents an object and each column represents the value of a specific attribute of the object.

**Note:** Many WMI queries consume a large amount of time and computer resources. It is easy to inadvertently issue a query that takes several minutes to complete and returns thousands of rows. It is highly recommended that all queries be tested before use in a WQLSet using a program like Powershell or WMI Explorer.

| Attribute | Description | Required | Default Value | Allowed Values |
|---|---|---|---|---|
| namespace | Sets the namespace of the WMI query. | Yes | N/A | String values representing a valid WMI namespace.<br>The "root\cimv2" namespace is the one most commonly used when querying Windows operating system objects, but others such as "root\directory\LDAP" and "root\Microsoft\SqlServer\ComputerManagement" can be used. See here for a small script called GetNamespaces.vbs that enumerates the available WMI namespaces on a given computer. |
| wql | A WQL query string. | Yes | N/A | A valid WQL string.<br>The query must include the __Path attribute for each returned object; the Agent uses the __Path attribute as the entity key when storing and reporting results, so each returned WMI object must include a __Path. If using a query string such as "SELECT * FROM ..." the __Path attribute will be available, but if using a more selective query such as "SELECT Name FROM ..." you must explicitly include __Path by writing the query as "SELECT __Path,Name FROM ...". |
| onChange | Whether the files returned should be monitored in real time. | No | false | true, false |
| provider | Optionally specifies an alternative WMI namespace provider to use. | No | none | RsopLoggingModeProvider<br>At present this is only required/supported for group policy queries, and "RsopLoggingModeProvider" is the only |

| Attribute | Description | Required | Default Value | Allowed Values |
|---|---|---|---|---|
| | | | | supported value. Group policy queries are special since it's recommended that the RsopLoggingModeProvider be used to create a snapshot of the policy data that is present on a computer. If you create a snapshot of the policy data, the query can be performed against a consistent set of data before the system overwrites or deletes it during a refresh of policy. Creating a snapshot actually creates a new WMI namespace, so when using provider="RsopLoggingModeProvider" in a WQLSet, the namespace attribute should specify the suffix to be added to the created namespace. For example, a typical temporary namespace created by the RsopLoggingModeProvider would be "\\.\Root\Rsop\NS71EF4AA3_FB96_465F_AC1C_DFCF9A3E9010". Specify namespace="Computer" to query "\\.\Root\Rsop\NS71EF4AA3_FB96_465F_AC1C_DFCF9A3E9010\Computer".<br>Since the temporary namespace is a one-time value, it hampers the ability of the Agent to detect changes since the value appears in the entity key. To avoid this, the Agent will remove the portion of the returned __Path value after \Rsop\ and up to the next backslash when the RsopLoggingModeProvider is used. Entity keys will therefore have prefixes like "\\.\Root\Rsop\Computer" rather than "\\.\Root\Rsop\NS71EF4AA3_FB96_465F_AC1C_DFCF9A3E9010\Computer" |
| timeout | Specifies a per-row timeout in milliseconds. | No | 5000 | 1-60000<br>The WMI query is performed in semisynchronous mode, where result rows are fetched one at a time and there is a timeout on the fetching of a single row. If this parameter is not specified, 5000 (5 seconds) is used as the timeout value. |

### Entity Set Attributes

Each "row" returned by the WQL query is treated as a single Entity for Integrity Monitoring purposes, with the returned columns representing the attributes of the entity. Since WMI/WQL is an open-ended specification, there is no set list of available or supported attributes. The query and the schema of the WMI object being queried will determine the attributes being monitored.

For example, the WQLSet:

```
<WQLSet namespace="Computer" wql="select * from RSOP_SecuritySettings where
precedence=1" provider="RsopLoggingModeProvider" />
```

will return attributes of:

```
ErrorCode, GPOID, KeyName, SOMID, Setting, Status, id, precedence
```

whereas a WQLSet that queries network adapters such as:

```
<WQLSet namespace="root\cimv2" wql="select * from Win32_NetworkAdapter where
AdapterTypeId = 0" />
```

will return attributes such as:

```
AdapterType, AdapterTypeId, Availability, Caption, ConfigManagerErrorCode,
ConfigManagerUserConfig, CreationClassName Description, DeviceID, Index,
Installed, MACAddress, Manufacturer, MaxNumberControlled, Name, PNPDeviceID,
PowerManagementSupported, ProductName, ServiceName, SystemCreationClassName,
SystemName, TimeOfLastReset
```

In order to reduce the load on the Agent, it is advisable to explicitly include only the attributes that require monitoring rather than use "select * ..." in queries. This also has the benefit that changes to the WMI schema to add or remove attributes will not be reported as changes to the object unless the attributes are part of the set being monitored. With "select * from Win32_Foobar", a patch to Windows that adds a new attribute to the Win32_Foobar object class would result in the next integrity scan reporting a change for every object of that class since a new attribute has appeared.

The following are some example WMI queries which return desirable Windows system entities.

Query for Windows mounted storage devices: (selecting for * will typically result in 80% returned attributes being null or duplicate values)

```
<WQLSet namespace="root\cimv2" wql="SELECT __
Path,DeviceID,VolumeName,VolumeSerialNumber,DriveType,FileSystem,Access,Medi
aType,Size,FreeSpace FROM Win32_LogicalDisk" />
```

To further the preceding query, the DriveType can be specified to isolate only certain types of mounted logical storage devices, such as type 2 which is a "Removable Disk": (like a removable USB storage drive)

```
<WQLSet namespace="root\cimv2" wql="SELECT __
Path,DeviceID,VolumeName,VolumeSerialNumber,DriveType,FileSystem,Access,Medi
aType,Size,FreeSpace FROM Win32_LogicalDisk WHERE DriveType=2" />
```

(See here for details on the Win32_LogicalDisk class)

**USB Storage Device notes:** U3 USB devices will mount both a type 2 "Removable Disk" device and a type 3 "Compact Disc" device. Also, the above query is for storage devices only. USB non-storage devices will not be included. USB memory card adapters may appear as a type 1 "No Root Directory" device. A badly or Windows incompatible USB storage device may appear as a type 1 "Unknown" device.

Query for all known System Directories where the Drive is "F:" for relevant attributes:

```
<WQLSet namespace="root\cimv2" wql="SELECT __
Path,CreationDate,LastAccessed,LastModified,Drive,Path,FileName,Caption,File
Type,Readable,Writeable FROM Win32_Directory WHERE Drive='F:'" />
```

Query for all known System Files where the Drive is "F:" for relevant attributes:

```
<WQLSet namespace="root\cimv2" wql="SELECT __
Path,CreationDate,LastAccessed,LastModified,Drive,Path,FileName,Name,FileTyp
e,Readable,Writeable FROM CIM_DataFile WHERE Drive='F:'" />
```

#### Meaning of Key

The key is the "__Path" attribute of the returned WMI object, which is generally of the form:

```
SystemName\Namespace:WmiObjectClass.KeyAttribute=Value
[,KeyAttribute=Value...]
```

Some examples:

```
\\TEST-DESK\root\cimv2:Win32_QuickFixEngineering.HotFixID="KB958215-
IE7",ServicePackInEffect="SP0"
 \\TEST-DESK\ROOT\Rsop\NSF49B36AD_10A3_4F20_9541_B4C471907CE7\Computer:RSOP_
RegistryValue.

Path="MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Syste
```

```
m\\LegalNoticeText",precedence=1
 \\TEST-DESK\root\cimv2:BRCM_NetworkAdapter.DeviceID="8"
```

**Include Exclude**

See "About the Integrity Monitoring rules language" on page 913 for a general description of "include" and "exclude" for their allowed attributes and sub elements.

For WQLSet, "include" and "exclude" sub elements should typically not be required. It is preferable to use WQL to specify the exact set of objects to be monitored since that limits the amount of work done by both the agent and the computer's WMI implementation.

The use of any include or exclude sub elements can only reduce the set of objects returned by the query; the WQL must be changed in order to return additional objects. If it is necessary to use include or exclude elements to further restrict the WQL results, "*"and "?" characters can be used as simple wildcards to match against values of the entity key.

# Configure Log Inspection

## About Log Inspection

**Note:** For a list of operating systems where log inspection is supported, see "Supported features by platform" on page 425.

The log inspection protection module helps you identify important events that might be buried in your operating system and application logs. These events can be sent to a security information and event management (SIEM) system or centralized logging server for correlation, reporting, and archiving. All events are also securely collected in the Deep Security Manager. For more information about logging and forwarding events, see "Configure log inspection event forwarding and storage" on page 963.

For information on forwarding events to a syslog server or SIEM, see "Forward Deep Security events to a Syslog or SIEM server" on page 1067.

The log inspection module lets you:

- Meet PCI DSS log monitoring requirements.
- Detect suspicious behavior.
- Collect events across heterogeneous environments containing different operating systems and diverse applications.

- View events such as error and informational events (disk full, service start, service shutdown, etc.).
- Create and maintain audit trails of administrator activity (administrator login or logout, account lockout, policy change, etc.).

To enable and configure log inspection, see "Set up Log Inspection" below.

The log inspection feature in Deep Security enables real-time analysis of third party log files. The log inspection rules and decoders provide a framework to parse, analyze, rank and correlate events across a wide variety of systems. As with intrusion prevention and integrity monitoring, log inspection content is delivered in the form of rules included in a security update. These rules provide a high level means of selecting the applications and logs to be analyzed. To configure and examine log inspection rules, see "Define a Log Inspection rule for use in policies" on page 964.

## Set up Log Inspection

To use log inspection, perform these basic steps:

1. "Turn on the log inspection module" below
2. "Run a recommendation scan" below
3. "Apply the recommended log inspection rules" on the next page
4. "Test Log Inspection" on page 962
5. "Configure log inspection event forwarding and storage" on page 963

For an overview of the log inspection module, see "About Log Inspection" on the previous page.

### Turn on the log inspection module

1. Go to **Policies**.
2. Double-click the policy for which you want to enable log inspection.
3. Click **Log Inspection > General**.
4. For **Log Inspection State**, select **On**.
5. Click **Save**.

### Run a recommendation scan

Rules should be set to gather security events relevant to your requirements. When improperly set, events for this feature can overwhelm the Deep Security database if too many log entries are triggered and stored. Run a recommendation scan on the computer for recommendations about which rules are appropriate to apply.

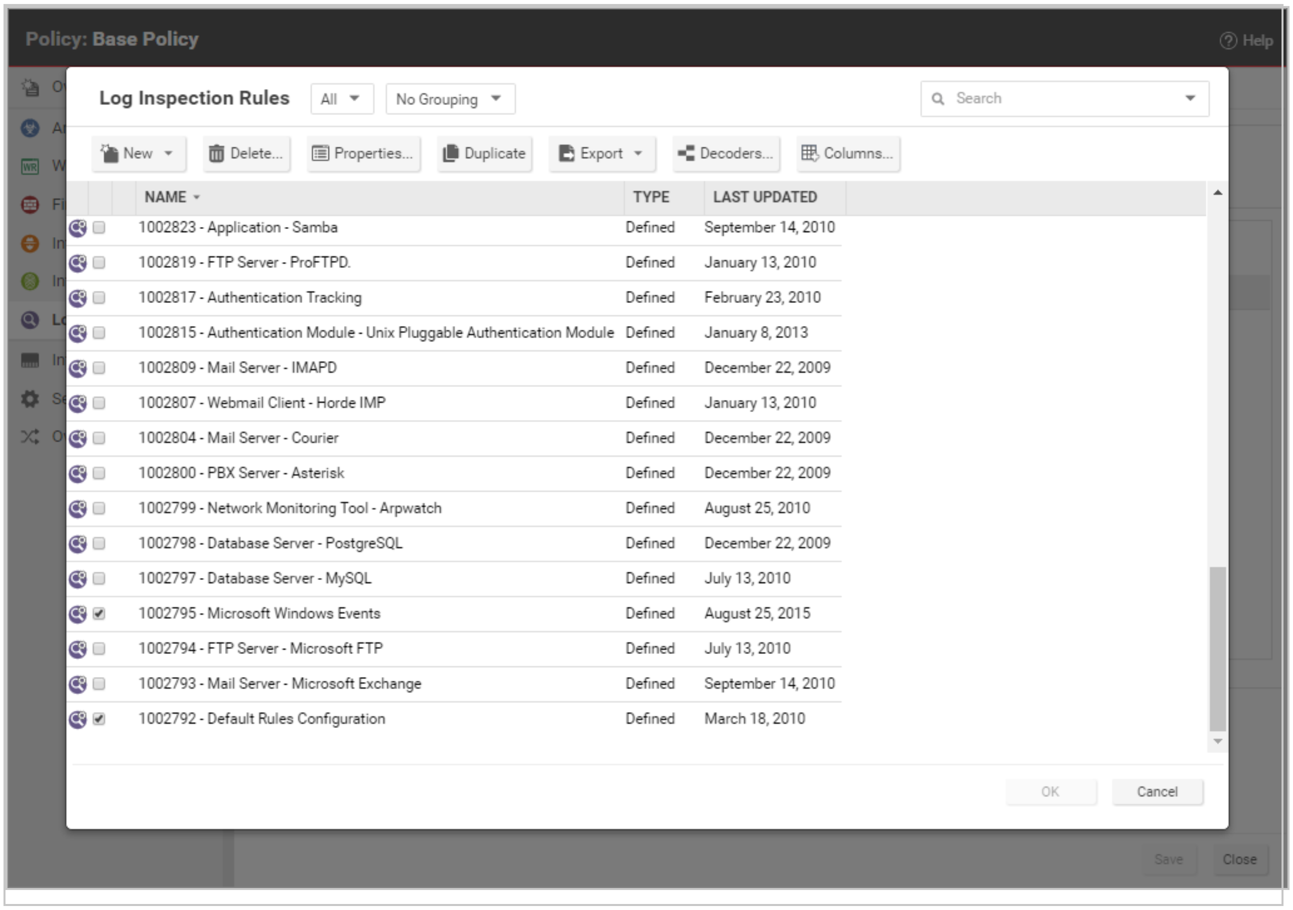
1. Go to **Computers** and double-click the appropriate computer.
2. Click **Log Inspection > General**.
3. For **Automatically implement Log Inspection Rule Recommendations (when possible)**, you can decide whether Deep Security should implement the rules it finds by selecting **Yes** or **No**.
4. In the **Recommendations** section, click **Scan For Recommendations**. Some log inspection rules written by Trend Micro require local configuration to function properly. If you assign one of these rules to your computers or one of these rules gets assigned automatically, an alert will be raised to notify you that configuration is required.

For more information about recommendation scans, see "Manage and run recommendation scans" on page 639.

## Apply the recommended log inspection rules

Deep Security ships with many pre-defined rules covering a wide variety of operating systems and applications. When you run a recommendation scan, you can choose to have Deep Security automatically implement the recommended rules, or you can choose to manually select and assign the rules by following the steps below:

1. Go to **Policies**.
2. Double-click the policy that you want to configure.
3. Click **Log Inspection > General**.
4. In the **Assigned Log Inspection Rules** section, the rules in effect for the policy are displayed. To add or remove log inspection rules, click **Assign/Unassign**.



| | NAME | TYPE | LAST UPDATED |
|---|---|---|---|
| □ | 1002823 - Application - Samba | Defined | September 14, 2010 |
| □ | 1002819 - FTP Server - ProFTPD. | Defined | January 13, 2010 |
| □ | 1002817 - Authentication Tracking | Defined | February 23, 2010 |
| □ | 1002815 - Authentication Module - Unix Pluggable Authentication Module | Defined | January 8, 2013 |
| □ | 1002809 - Mail Server - IMAPD | Defined | December 22, 2009 |
| □ | 1002807 - Webmail Client - Horde IMP | Defined | January 13, 2010 |
| □ | 1002804 - Mail Server - Courier | Defined | December 22, 2009 |
| □ | 1002800 - PBX Server - Asterisk | Defined | December 22, 2009 |
| □ | 1002799 - Network Monitoring Tool - Arpwatch | Defined | August 25, 2010 |
| □ | 1002798 - Database Server - PostgreSQL | Defined | December 22, 2009 |
| □ | 1002797 - Database Server - MySQL | Defined | July 13, 2010 |
| ☑ | 1002795 - Microsoft Windows Events | Defined | August 25, 2015 |
| □ | 1002794 - FTP Server - Microsoft FTP | Defined | July 13, 2010 |
| □ | 1002793 - Mail Server - Microsoft Exchange | Defined | September 14, 2010 |
| ☑ | 1002792 - Default Rules Configuration | Defined | March 18, 2010 |

5. Select or deselect the checkboxes for the rules you want to assign or unassign. You can edit the log inspection rule by right-clicking the rule and selecting **Properties** to edit the rule locally or **Properties (Global)** to apply the changes to all other policies that are using the rule. For more information, see "Examine a Log Inspection rule" on page 986.
6. Click **OK**.

Although Deep Security ships with log inspection rules for many common operating systems and applications, you also have the option to create your own custom rules. To create a custom rule, you can either use the "Basic Rule" template, or you can write your new rule in XML. For information on how to create a custom rule, see "Define a Log Inspection rule for use in policies" on page 964.

## Test Log Inspection

Before continuing with further Log Inspection configuration steps, test that the rules are working correctly:

1. Ensure Log Inspection is enabled.
2. Go to **Computer or Policies editor > Log Inspection > Advanced**. Change **Store events at the Agent/Appliance for later retrieval by DSM when they equal or exceed the following severity level** to **Low (3)** and click **Save**.
3. Go to the **General** tab, and click **Assign/Unassign**. Search for and enable:
   - 1002792 - Default Rules Configuration – This is required for all other Log Inspection rules to work.

   If you're a Windows user, enable:

   - 1002795 - Microsoft Windows Events – This logs events every time the Windows auditing functionality registers an event.

   If you're a Linux user, enable:

   - 1002831 - Unix - Syslog - This inspects the syslog for events.
4. Click **OK**, and then click **Save** to apply the rules to the policy.
5. Attempt to log in to the server with an account that does not exist.
6. Go to **Events & Reports > Log Inspection Events** to verify the record of the failed login attempt. If the detection is recorded, the Log Inspection module is working correctly.

## Configure log inspection event forwarding and storage

When a log inspection rule is triggered, an event is logged. To view these events, go to **Events & Reports > Log Inspection Events** or **Policy editor > Log Inspection > Log Inspection Events**. For more information on working with log inspection events, see "Log inspection events" on page 1306.

Depending on the severity of the event, you can choose to send them to a syslog server (For information on enabling this feature, see "Forward Deep Security events to a Syslog or SIEM server" on page 1067.) or to store events in the database by using the severity clipping feature.

There are two "severity clipping" settings available:

- **Send Agent events to syslog when they equal or exceed the following severity level:** This setting determines which events triggered by those rules get sent to the syslog server, if syslog is enabled.
- **Store events at the Agent for later retrieval by Deep Security Manager when they equal or exceed the following severity level:** This setting determines which log inspection events are kept in the database and displayed in the **Log Inspection Events** page.

To configure severity clipping:

1. Go to **Policies**.
2. Double-click the policy you want to configure.
3. Click **Log Inspection > Advanced**.
4. For **Send Agent/Appliance events to syslog when they equal or exceed the following severity level**, choose a severity level between **Low (0)** and **Critical (15)**.
5. For **Store events at the Agent/Appliance for later retrieval by DSM when they equal or exceed the following severity level**, choose a severity level between **Low (0)** and **Critical (15)**.
6. Click **Save**.

## Define a Log Inspection rule for use in policies

The OSSEC Log Inspection engine is integrated into Deep Security Agents and gives Deep Security the ability to inspect the logs and events generated by the operating system and applications running on the computer. Deep Security Manager ships with a standard set of OSSEC Log Inspection rules that you can assign to computers or policies. You can also create custom rules if there is no existing rule that fits your requirements.

You cannot modify Log Inspection Rules issued by Trend Micro, but you can duplicate them and then modify them.

Log Inspection Rules assigned to one or more computers or are part of a Policy cannot be deleted.

To create Log Inspection rules, perform these basic steps:

- "Create a new Log Inspection rule" on the next page
- "Decoders" on page 967
- "Subrules" on page 968
- "Examples" on page 976
- "Log Inspection rule severity levels and their recommended use" on page 984
- "strftime() conversion specifiers " on page 985
- "Examine a Log Inspection rule" on page 986

For an overview of the Log Inspection module, see "About Log Inspection" on page 959.

## Create a new Log Inspection rule

1. In the Deep Security Manager, go to **Policies** > **Common Objects** > **Rules** > **Log Inspection Rules**.
2. Click **New** > **New Log Inspection Rule**.
3. On the **General** tab, enter a name and an optional description for the rule.
4. The **Content** tab is where you define the rule. The easiest way to define a rule is to select **Basic Rule** and use the options provided to define the rule. If you need further customization, you can select **Custom (XML)** to switch to an XML view of the rule that you are defining.

   Any changes you make in the **Custom (XML)** view are lost if you switch back to the Basic Rule view.

   For further assistance in writing your own Log Inspection rules using the XML-based language, consult the OSSEC documentation or contact your support provider.

   These options are available for the Basic Rule template:

   - **Rule ID:** The Rule ID is a unique identifier for the rule. OSSEC defines 100000 - 109999 as the space for user-defined rules. Deep Security Manager prepopulates the field with a new unique Rule ID.
   - **Level:** Assign a level to the rule. Zero (0) means the rule never logs an event, although other rules that watch for this rule may fire.
   - **Groups:** Assign the rule to one or more comma-separated groups. This can be useful when dependency is used because you can create rules that fire on the firing of a rule, or a rule that belongs to a specific group.
   - **Rule Description:** Description of the rule.

   - **Pattern Matching:** This is the pattern the rule will look for in the logs. The rule is triggered on a match. Pattern matching supports Regular Expressions or simpler String Patterns. The String Pattern pattern type is faster than RegEx but it only supports three special operations:

     - **^ (caret)**: specifies the beginning of text
     - **$ (dollar sign)**: specifies the end of text
     - **| (pipe)**: to create a "OR" between multiple patterns

For information on the regular expression syntax used by the Log Inspection module, see https://www.ossec.net/docs/syntax/regex.html.

- **Dependency:** Setting a dependency on another rule causes your rule to only log an event if the rule specified in this area has also triggered.
- **Frequency** is the number of times the rule has to match within a specific time frame before the rule is triggered.

- **Time Frame** is the period of time in seconds within which the rule has to trigger a certain number of times (the frequency, above) to log an event.

  The **Content** tab only appears for Log Inspection rules that you create yourself. Log Inspection rules issued by Trend Micro have a **Configuration** tab instead that displays the Log Inspection rule's configuration options,if there are any.

5. On the **Files** tab, type the full path to the files you want your rule to monitor and specify the type of file it is.

   The glob character is supported when used in the file name. The glob character is also supported when used in the directory portion of the path no more than twice. For example, `/home/user1/testlog*.txt`, `/home/*/testlog1.txt`, `/home/*/testlog*.txt`, `/home/*/user*/testlog*.txt` are all valid, whereas `/home/*/demo*/user*/testlog1.txt` is invalid.

6. On the **Options** tab, in the **Alert** section, select whether this rule triggers an alert in the Deep Security Manager.

   **Alert Minimum Severity** sets the minimum severity level that will trigger an Alert for rules made using the Basic Rule or Custom (XML) template.

   The Basic Rule template creates one rule at a time. To write multiple rules in a single template you can use the Custom (XML) template. If you create multiple rules with different Levels within a Custom (XML) template, you can use the **Alert Minimum Severity** setting to select the minimum severity that will trigger an Alert for all of the rules in that template.

7. The **Assigned To** tab lists the policies and computers that are using this Log Inspection rule. Because you are creating a new rule, it has not been assigned yet.
8. Click **OK**. The rule is ready to be assigned to policies and computers.

## Decoders

A Log Inspection rule consists of a list of files to monitor for changes and a set of conditions to be met for the rule to trigger. When the Log Inspection engine detects a change in a monitored log file, the change is parsed by a decoder. Decoders parse the raw log entry into the following fields:

- **log:** the message section of the event
- **full_log:** the entire event
- **location:** where the log came from
- **hostname:** hostname of the event source
- **program_name:** program name from the syslog header of the event
- **srcip:** the source IP address within the event
- **dstip:** the destination IP address within the event
- **srcport:** the source port number within the event
- **dstport:** the destination port number within the event
- **protocol:** the protocol within the event
- **action:** the action taken within the event
- **srcuser:** the originating user within the event
- **dstuser:** the destination user within the event
- **id:** any ID decoded as the ID from the event
- **status:** the decoded status within the event
- **command:** the command being called within the event
- **url:** the URL within the event
- **data:** any additional data extracted from the event
- **systemname:** the system name within the event

Rules examine this decoded data looking for information that matches the conditions defined in the rule.

If the matches are at a sufficiently high severity level, any of the following actions can be taken:

- An alert can be raised. Configurable on the **Options** tab of the Log Inspection Rule's **Properties** window.
- The event can be written to syslog. Configurable in the **SIEM** area on **Administration > System Settings > Event Forwarding** tab.

- The event can be sent to the Deep Security Manager. Configurable in the **Log Inspection Syslog Configuration** setting on the **Policy or Computer Editor > Settings > Event Forwarding** tab.

## Subrules

A single Log Inspection rule can contain multiple subrules. These subrules can be of two types: atomic or composite. An atomic rule evaluates a single event and a composite rule examines multiple events and can evaluate frequency, repetition, and correlation between events.

### Groups

Each rule, or grouping of rules, must be defined within a `<group></group>` element. The attribute name must contain the rules you want to be a part of this group. In the following example, it indicates that the group contains the syslog and SSHD rules:

```
<group name="syslog,sshd,">
</group>
```

Notice the trailing comma in the group name. Trailing commas are required if you intend to use the `<if_group></if_group>` tag to conditionally append another subrule to this one.

When a set of Log Inspection rules are sent to an agent, the Log Inspection engine on the agent takes the XML data from each assigned rule and assembles it into what becomes a single long Log Inspection rule. Some group definitions are common to all Log Inspection rules created by Trend Micro. For this reason Trend Micro has included a rule called Default Rules Configuration, which defines these groups and which always gets assigned together with any other Trend Micro rules. If you select a rule for assignment and do not also select the Default Rules Configuration rule, a notice appears informing you that the rule will be assigned automatically. If you create your own Log Inspection rule and assign it to a Computer without assigning any Trend Micro-written rules, you must either copy the content of the Default Rules Configuration rule into your new rule or also select the Default Rules Configuration rule for assignment to the Computer.

### Rules, ID, and Level

A group can contain as many rules as you require. The rules are defined using the `<rule></rule>` element and must have at least two attributes, the `id` and the `level`. The `id` is a unique identifier for that signature and the `level` is the severity of the alert. In the following example, two rules are created, each with a different rule ID and level:

```
<group name="syslog,sshd,">
       <rule id="100120" level="5">
       </rule>
       <rule id="100121" level="6">
       </rule>
</group>
```

Custom rules must have ID values of 100,000 or greater.

You can define additional subgroups within the parent group using the `<group></group>` tag. This subgroup can reference any of the groups listed in the following table:

| Group Type | Group Name | Description |
|---|---|---|
| Reconnaissance | connection_attempt<br>web_scan<br>recon | Connection attempt<br>Web scan<br>Generic scan |
| Authentication Control | authentication_success<br>authentication_failed<br>invalid_login<br>login_denied<br>authentication_failures<br>adduser<br>account_changed | Success<br>Failure<br>Invalid<br>Login Denied<br>Multiple Failures<br>User account added<br>User Account changed or removed |
| Attack/Misuse | automatic_attack<br>exploit_attempt<br>invalid_access<br>spam<br>multiple_spam<br>sql_injection<br>attack<br>virus | Worm (nontargeted attack)<br>Exploit pattern<br>Invalid access<br>Spam<br>Multiple spam messages<br>SQL injection<br>Generic attack<br>Virus detected |
| Access Control | access_denied<br>access_allowed<br>unknown_resource<br>firewall_drop<br>multiple_drops<br>client_misconfig<br>client_error | Access denied<br>Access allowed<br>Access to nonexistent resource<br>Firewall drop<br>Multiple firewall drops<br>Client misconfiguration<br>Client error |
| Network Control | new_host<br>ip_spoof | New computer detected<br>Possible ARP spoofing |
| System Monitor | service_start<br>system_error<br>system_shutdown<br>logs_cleared<br>invalid_request<br>promisc<br>policy_changed | Service start<br>System error<br>Shutdown<br>Logs cleared<br>Invalid request<br>Interface switched to promiscuous mode<br>Policy changed |

| Group Type | Group Name | Description |
|---|---|---|
| | config_changed<br>low_diskspace<br>time_changed | Configuration changed<br>Low disk space<br>Time changed |

If event auto-tagging is enabled, the event is labeled with the group name. Log Inspection rules provided by Trend Micro make use of a translation table that changes the group to a more user-friendly version. For example, login_denied would appear as Login Denied. Custom rules are listed by their group name as it appears in the rule.

### Description

Include a `<description></description>` tag. The description text appears in the event if the rule is triggered.

```
<group name="syslog,sshd,">
       <rule id="100120" level="5">
               <group>authentication_success</group>
               <description>SSHD testing authentication success</description>
       </rule>
       <rule id="100121" level="6">
               <description>SSHD rule testing 2</description>
       </rule>
</group>
```

### Decoded As

The `<decoded_as></decoded_as>` tag instructs the Log Inspection engine to only apply the rule if the specified decoder has decoded the log.

```
<rule id="100123" level="5">
       <decoded_as>sshd</decoded_as>
       <description>Logging every decoded sshd message</description>
</rule>
```

To view the available decoders, go to the **Log Inspection Rule** page and click **Decoders.** Right-click on **1002791-Default Log Decoders** and select **Properties**. Go the **Configuration** tab and click **View Decoders**.

### Match

To look for a specific string in a log, use the `<match></match>`. Here is a Linux sshd failed password log:

```
Jan 1 12:34:56 linux_server sshd[1231]: Failed password for invalid
      user jsmith from 192.168.1.123 port 1799 ssh2
```

Use the **<match></match>** tag to search for the "password failed" string.

```
<rule id="100124" level="5">
       <decoded_as>sshd</decoded_as>
       <match>^Failed password</match>
       <description>Failed SSHD password attempt</description>
</rule>
```

Notice the regex caret ( ^ ) indicating the beginning of a string. Although "Failed password" does not appear at the beginning of the log, the Log Inspection decoder brakes the log into sections. See "Decoders" on page 967 for more information. One of those sections is "log", which is the message part of the log, as opposed to "full_log" which is the log in its entirety.

The following table lists supported regex syntax:

| Regex syntax | Description |
|---|---|
| \w | A-Z, a-z, 0-9 single letters and numerals |
| \d | 0-9 single numerals |
| \s | single space |
| \t | single tab |
| \p | ()*+,-.:;<=>?[] |
| \W | not \w |
| \D | not \d |
| \S | not \s |
| \. | anything |
| + | match one or more of any of the above (for example, \w+, \d+) |
| * | match zero or more of any of the above (for example, \w*, \d*) |
| ^ | indicates the beginning of a string (^somestring) |
| $ | specify the end of a string (somestring$) |
| \| | indicate an "OR" between multiple strings |

### Conditional statements

Rule evaluation can be conditional upon other rules having been evaluated as true. The `<if_sid></if_sid>` tag instructs the Log Inspection engine to only evaluate this subrule if the rule identified in the tag has been evaluated as true. The following example shows three rules: 100123, 100124, and 100125. Rules 100124 and 100125 have been modified to be children of the 100123 rule using the `<if_sid></if_sid>` tag:

```
<group name="syslog,sshd,">
       <rule id="100123" level="2">
               <decoded_as>sshd</decoded_as>
               <description>Logging every decoded sshd message</description>
       </rule>
       <rule id="100124" level="7">
               <if_sid>100123</if_sid>
               <match>^Failed password</match>
               <group>authentication_failure</group>
               <description>Failed SSHD password attempt</description>
       </rule>
       <rule id="100125" level="3">
               <if_sid>100123</if_sid>
               <match>^Accepted password</match>
               <group>authentication_success</group>
               <description>Successful SSHD password attempt</description>
       </rule>
</group>
```

#### Hierarchy of evaluation

The `<if_sid></if_sid>` tag essentially creates a hierarchical set of rules. That is, by including an `<if_sid></if_sid>` tag in a rule, the rule becomes a child of the rule referenced by the `<if_sid></if_sid>` tag. Before applying any rules to a log, the Log Inspection engine assesses the `<if_sid></if_sid>` tags and builds a hierarchy of parent and child rules.

The hierarchical parent-child structure can be used to improve the efficiency of your rules. If a parent rule does not evaluate as true, the Log Inspection engine ignores the children of that parent.

Although the `<if_sid></if_sid>` tag can be used to refer to subrules within an entirely different Log Inspection rule, you should avoid doing this because it makes the rule very difficult to review later.

The list of available atomic rule conditional options is shown in the following table:

| Tag | Description | Notes |
|---|---|---|
| match | A pattern | Any string to match against the event (log). |

| Tag | Description | Notes |
|---|---|---|
| regex | A regular expression | Any regular expression to match against the event (log). |
| decoded_as | A string | Any prematched string. |
| srcip | A source IP address | Any IP address that is decoded as the source IP address. Use ! to negate the IP address. |
| dstip | A destination IP address | Any IP address that is decoded as the destination IP address. Use ! to negate the IP address. |
| srcport | A source port number | Any source port (match format). |
| dstport | A destination port number | Any destination port (match format). |
| user | A username | Any username that is decoded as a username. |
| program_name | A program name | Any program name that is decoded from the syslog process name. |
| hostname | A system hostname | Any hostname that is decoded as a syslog hostname. |
| time | A time range in the format<br>hh:mm - hh:mm or<br>hh:mm am - hh:mm pm | The time range that the event must fall within for the rule to trigger. |
| weekday | A weekday (sunday, monday, tuesday, and so on) | Day of the week that the event must fall on for the rule to trigger. |
| id | An ID | Any ID that is decoded from the event. |
| url | A URL | Any URL that is decoded from the event. |

Use the `<if_sid>100125</if_sid>` tag to make this rule depend on the 100125 rule. This rule is checked only for SSHD messages that already matched the successful login rule.

```
<rule id="100127" level="10">
       <if_sid>100125</if_sid>
       <time>6 pm - 8:30 am</time>
       <description>Login outside business hours.</description>
       <group>policy_violation</group>
</rule>
```

### Restrictions on the Size of the Log Entry

The following example takes the previous example and adds the `maxsize` attribute which tells the Log Inspection engine to only evaluate rules that are less than the maxsize number of characters:

```
<rule id="100127" level="10" maxsize="2000">
       <if_sid>100125</if_sid>
       <time>6 pm - 8:30 am</time>
       <description>Login outside business hours.</description>
       <group>policy_violation</group>
</rule>
```

The following table lists possible atomic rule tree-based options:

| Tag | Description | Notes |
|---|---|---|
| if_sid | A rule ID | Adds this rule as a child rule of the rules that match the specified signature ID. |
| if_group | A group ID | Adds this rule as a child rule of the rules that match the specified group. |
| if_level | A rule level | Adds this rule as a child rule of the rules that match the specified severity level. |
| description | A string | A description of the rule. |
| info | A string | Extra information about the rule. |
| cve | A CVE number | Any Common Vulnerabilities and Exposures (CVE) number that you would like associated with the rule. |
| options | alert_by_email<br>no_email_alert<br>no_log | Additional rule options to indicate if the Alert should generate an e-mail, alert_by_email, should not generate an email, no_email_alert, or should not log anything at all, no_log. |

**Composite Rules**

Atomic rules examine single log entries. To correlate multiple entries, you must use composite rules. Composite rules are supposed to match the current log with those already received. Composite rules require two additional options: the `frequency` option specifies how many times an event or pattern must occur before the rule generates an alert, and the `timeframe` option tells the Log Inspection engine how far back, in seconds, it should look for previous logs. All composite rules have the following structure:

```
<rule id="100130" level="10" frequency="x" timeframe="y">
</rule>
```

For example, you could create a composite rule that creates a higher severity alert after five failed passwords within a period of 10 minutes. Using the `<if_matched_sid></if_matched_sid>` tag you can indicate which rule needs to be seen within the desired frequency and timeframe for your new rule to create an alert. In the following example, the `frequency` attribute is set to trigger when five instances of the event are seen and the `timeframe` attribute is set to specify the time window as 600 seconds.

The `<if_matched_sid></if_matched_sid>` tag is used to define which other rule the composite rule will watch:

```
<rule id="100130" level="10" frequency="5" timeframe="600">
       <if_matched_sid>100124</if_matched_sid>
       <description>5 Failed passwords within 10 minutes</description>
</rule>
```

There are several additional tags that you can use to create more granular composite rules. These rules, as shown in the following table, allow you to specify that certain parts of the event must be the same. This allows you to tune your composite rules and reduce false positives:

| Tag | Description |
|---|---|
| same_source_ip | Specifies that the source IP address must be the same. |
| same_dest_ip | Specifies that the destination IP address must be the same. |
| same_dst_port | Specifies that the destination port must be the same. |
| same_location | Specifies that the location (hostname or agent name) must be the same. |
| same_user | Specifies that the decoded username must be the same. |
| same_id | Specifies that the decoded id must be the same. |

If you wanted your composite rule to alert on every authentication failure, instead of a specific rule ID, you could replace the `<if_matched_sid></if_matched_sid>` tag with the `<if_matched_ group></if_matched_ group>` tag. This allows you to specify a category, such as `authentication_ failure`, to search for authentication failures across your entire infrastructure.

```
<rule id="100130" level="10" frequency="5" timeframe="600">
       <if_matched_group>authentication_failure</if_matched_group>
       <same_source_ip />
       <description>5 Failed passwords within 10 minutes</description>
</rule>
```

In addition to `<if_matched_sid></if_matched_sid>` and `<if_matched_group></if_ matched_ group>` tags, you can also use the `<if_matched_regex></if_matched_regex>` tag to specify a regular expression to search through logs as they are received.

```
<rule id="100130" level="10" frequency="5" timeframe="600">
       <if_matched_regex>^Failed password</if_matched_regex>
       <same_source_ip />
       <description>5 Failed passwords within 10 minutes</description>
</rule>
```

## Examples

Deep Security includes many default Log Inspection rules for dozens of common and popular applications. Through Security Updates, new rules are added regularly. In spite of the growing list of applications supported by Log Inspection rules, you may find the need to create a custom rule for an unsupported or custom application.

The following example creates a custom CMS (content management system) hosted on Microsoft Windows Server with IIS and .Net platform, with a Microsoft SQL Server database as the data repository.

The first step is to identify the following application logging attributes:

1. Where does the application log to?
2. Which Log Inspection decoder can be used to decode the log file?
3. What is the general format of a log file message?

For the CMS example, the answers are as follows:

1. Windows Event Viewer
2. Windows Event Log (eventlog)
3. Windows Event Log Format with the following core attributes:
    - Source: CMS
    - Category: None
    - Event: <Application Event ID>

The second step is to identify the categories of log events by application feature, and then organize the categories into a hierarchy of cascading groups for inspection. Not all inspected groups need to raise events; a match can be used as a conditional statement. For each group, identify the log format attributes which the rule can use as matching criteria. This can also be performed by inspecting all application logs for patterns and logical groupings of log events.

For example, the CMS application supports the following functionality for which Log Inspection rules are created:

- CMS Application Log (Source: CMS)
    - Authentication (Event: 100 to 119)
        - User Login successful (Event: 100)
        - User Login unsuccessful (Event: 101)

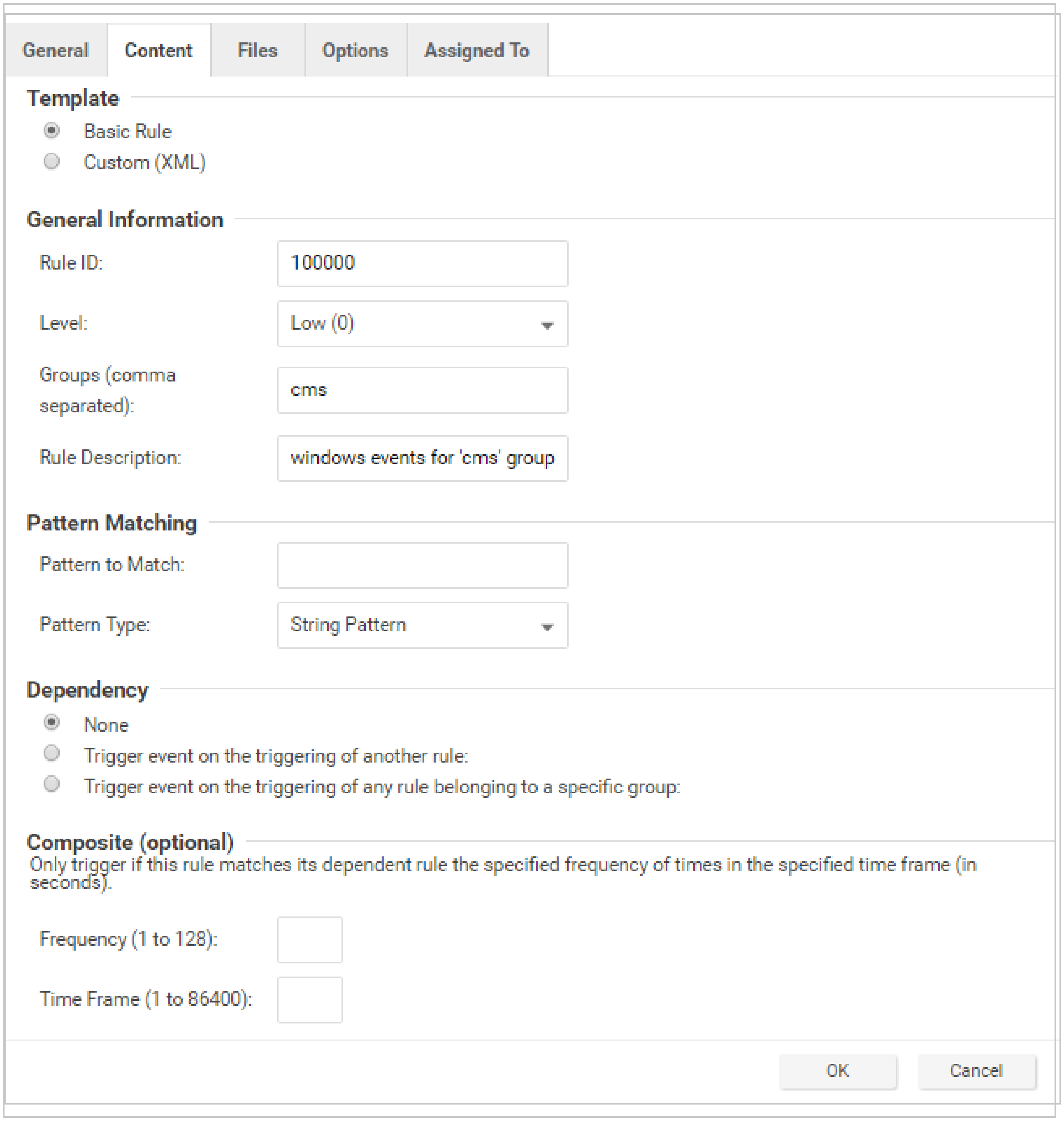
    - Administrator Login successful (Event: 105)
    - Administrator Login unsuccessful (Event: 106)
- General Errors (Type: Error)
    - Database error (Event: 200 to 205)
    - Runtime error (Event: 206-249)
- Application Audit (Type: Information)
    - Content
        - New content added (Event: 450 to 459)
        - Existing content modified (Event: 460 to 469)
        - Existing content deleted (Event: 470 to 479)
    - Administration
        - User
            - New User created (Event: 445 to 446)
            - Existing User deleted (Event: 447 to 449)

This structure provides you with a good basis for rule creation. You can now create a new Log Inspection rule in Deep Security Manager.

**To create the new CMS Log Inspection Rule:**

1. In Deep Security Manager, go to **Policies > Common Objects > Rules > Log Inspection Rules** and click **New** to display the **New Log Inspection Rule Properties** window.
2. Give the new rule a name and a description, and then select the **Content** tab.
3. Select **Basic Rule**. The quickest way to create a new custom rule is to start with a basic rule template.
4. The **Rule ID** field is automatically populated with an unused ID number of 100,000 or greater, the IDs reserved for custom rules.
5. Set the **Level** setting to **Low (0)**.
6. Give the rule an appropriate Group name. In this case, "cms".

7. Provide a short rule description.



**Template**

● Basic Rule
○ Custom (XML)

**General Information**

Rule ID: 100000

Level: Low (0)

Groups (comma separated): cms

Rule Description: windows events for 'cms' group

**Pattern Matching**

Pattern to Match:

Pattern Type: String Pattern

**Dependency**

● None
○ Trigger event on the triggering of another rule:
○ Trigger event on the triggering of any rule belonging to a specific group:

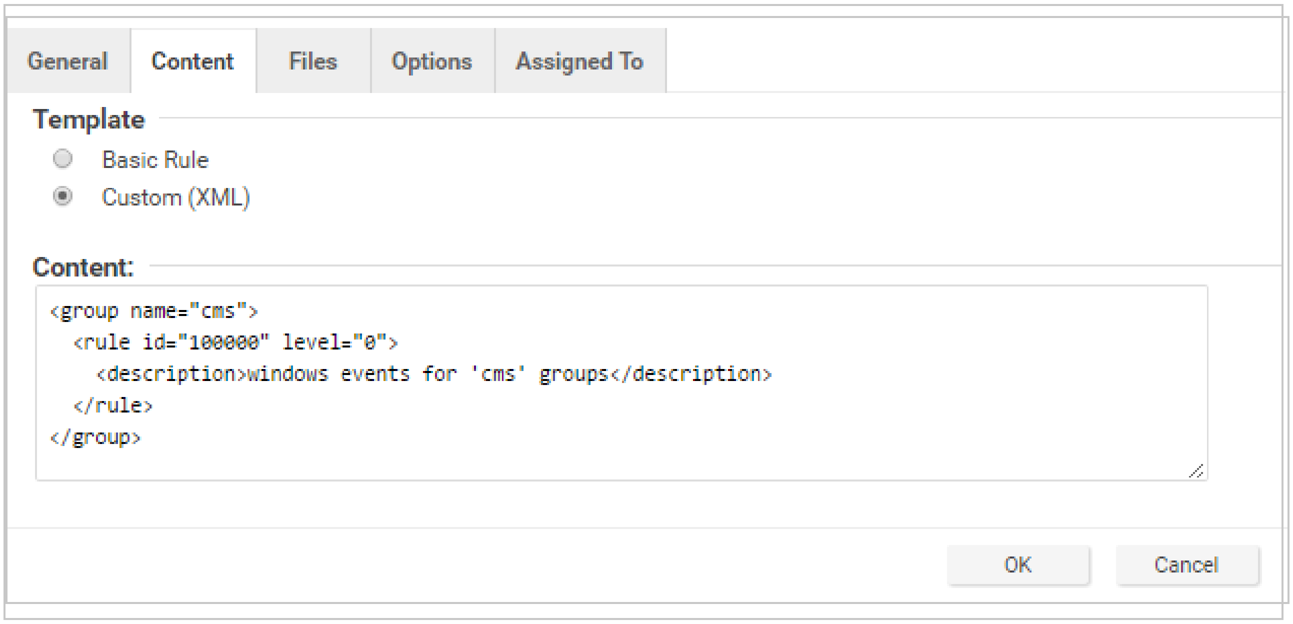
**Composite (optional)**

Only trigger if this rule matches its dependent rule the specified frequency of times in the specified time frame (in seconds).

Frequency (1 to 128):

Time Frame (1 to 86400):

8. Select **Custom (XML)**. The options you selected for your Basic rule will be converted to XML.



Template

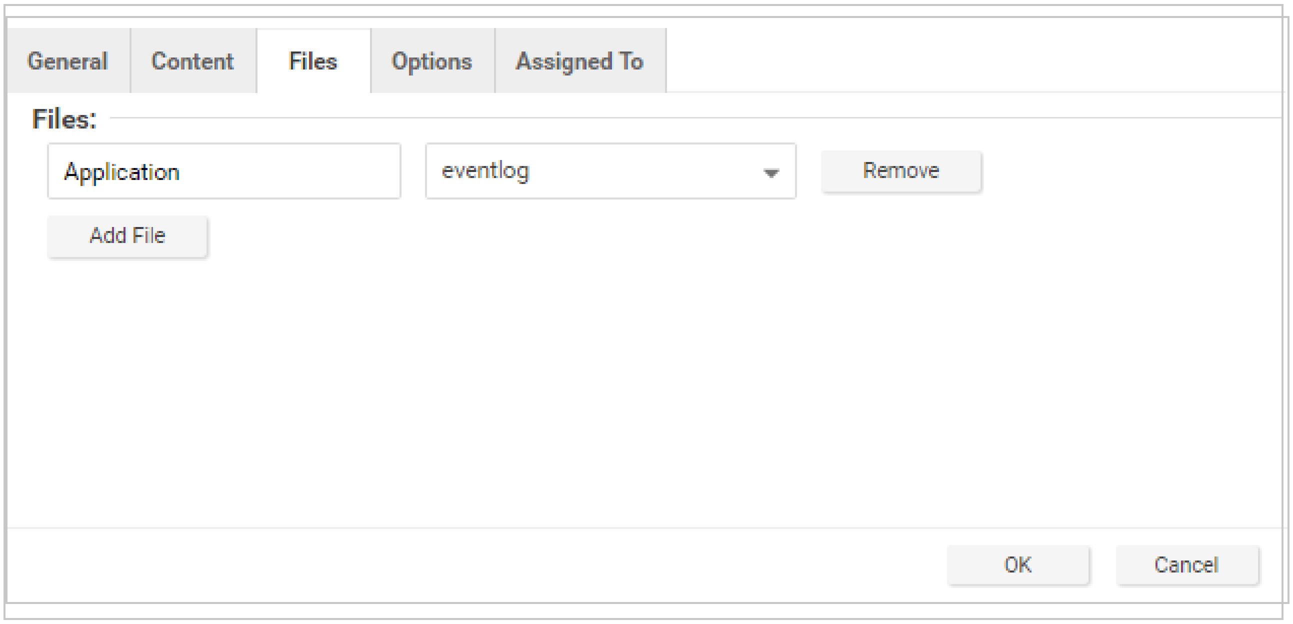
○ Basic Rule

● Custom (XML)

Content:

```
<group name="cms">
  <rule id="100000" level="0">
    <description>windows events for 'cms' groups</description>
  </rule>
</group>
```

9. Select the **Files** tab, and then click the **Add File** to add any application log files and log types to which to apply the rule. In this case, Application, and eventlog as the file type.



Files:

Application | eventlog

**Eventlog** is a unique file type in Deep Security because the location and filename of the log files do not have to be specified. Instead, it is sufficient to type the log name as it is displayed in the Windows Event Viewer. Other log names for the eventlog file type might be Security, System, Internet Explorer, or any other section listed in the Windows Event Viewer. Other file types require the log file's location and filename. C/C++ strftime()

conversion specifiers are available for matching on filenames. See the table for a list of some of the more useful ones.

10. Click **OK** to save the basic rule.
11. Working with the basic rule Custom (XML) created, you can begin adding new rules to the group based on the log groupings identified previously. You need to set the base rule criteria to the initial rule. In the following example, the CMS base rule has identified Windows Event Logs with a Source attribute of `CMS`:

```
<group name="cms">
       <rule id="100000" level="0">
               <category>windows</category>
               <extra_data>^CMS</extra_data>
               <description>Windows events from source 'CMS' group
messages.</description>
       </rule>
```

12. Proceed by building subsequent rules from the identified log groups. The following example identifies the authentication and login success and failure and logs by Event IDs.

```
<rule id="100001" level="0">
       <if_sid>100000</if_sid>
       <id>^100|^101|^102|^103|^104|^105|^106|^107|^108|^109|^110</id>
       <group>authentication</group>
       <description>CMS Authentication event.</description>
</rule>

<rule id="100002" level="0">
       <if_group>authentication</if_group>
       <id>100</id>
       <description>CMS User Login success event.</description>
</rule>
<rule id="100003" level="4">
       <if_group>authentication</if_group>
       <id>101</id>
       <group>authentication_failure</group>
       <description>CMS User Login failure event.</description>
</rule>
<rule id="100004" level="0">
       <if_group>authentication</if_group>
       <id>105</id>
       <description>CMS Administrator Login success event.</description>
</rule>
<rule id="100005" level="4">
       <if_group>authentication</if_group>
       <id>106</id>
       <group>authentication_failure</group>
       <description>CMS Administrator Login failure event.</description>
</rule>
```

13. Add any composite or correlation rules using the established rules. The following example shows a high severity composite rule that is applied to instances where the repeated login failures have occurred five times within a 10 second time period:

```
<rule id="100006" level="10" frequency="5" timeframe="10">
       <if_matched_group>authentication_failure</if_matched_group>
       <description>CMS Repeated Authentication Login failure
event.</description>
</rule>
```

14. Review all rules for appropriate severity levels. For example, error logs should have a severity of level 5 or higher. Informational rules would have a lower severity.
15. Open the newly-created rule, select the **Configuration** tab, and copy your custom rule XML into the rule field. Click **Apply** or **OK** to save the change.

Once the rule is assigned to a policy or computer, the Log Inspection engine should begin inspecting the designated log file immediately.

**The complete Custom CMS Log Inspection Rule:**

```
<group name="cms">
        <rule id="100000" level="0">
               <category>windows</category>
               <extra_data>^CMS</extra_data>
               <description>Windows events from source 'CMS' group
messages.</description>
       </rule>
        <rule id="100001" level="0">
               <if_sid>100000</if_sid>
               <id>^100|^101|^102|^103|^104|^105|^106|^107|^108|^109|^110</id>
               <group>authentication</group>
               <description>CMS Authentication event.</description>
       </rule>
       <rule id="100002" level="0">
               <if_group>authentication</if_group>
               <id>100</id>
               <description>CMS User Login success event.</description>
       </rule>

       <rule id="100003" level="4">
               <if_group>authentication</if_group>
               <id>101</id>
               <group>authentication_failure</group>
               <description>CMS User Login failure event.</description>
       </rule>

       <rule id="100004" level="0">
               <if_group>authentication</if_group>
               <id>105</id>
               <description>CMS Administrator Login success event.</description>
       </rule>

       <rule id="100005" level="4">
               <if_group>authentication</if_group>
               <id>106</id>
               <group>authentication_failure</group>
               <description>CMS Administrator Login failure event.</description>
       </rule>

       <rule id="100006" level="10" frequency="5" timeframe="10">
               <if_matched_group>authentication_failure</if_matched_group>
               <description>CMS Repeated Authentication Login failure
event.</description>
       </rule>

       <rule id="100007" level="5">
               <if_sid>100000</if_sid>
               <status>^ERROR</status>
               <description>CMS General error event.</description>
               <group>cms_error</group>
       </rule>

       <rule id="100008" level="10">
```

```
                <if_group>cms_error</if_group>
                <id>^200|^201|^202|^203|^204|^205</id>
                <description>CMS Database error event.</description>
        </rule>

        <rule id="100009" level="10">
                <if_group>cms_error</if_group>
                <id>^206|^207|^208|^209|^230|^231|^232|^233|^234|^235|^236|^237|^238|
                        ^239^|240|^241|^242|^243|^244|^245|^246|^247|^248|^249</id>
                <description>CMS Runtime error event.</description>
        </rule>

        <rule id="100010" level="0">
                <if_sid>100000</if_sid>
                <status>^INFORMATION</status>
                <description>CMS General informational event.</description>
                <group>cms_information</group>
        </rule>

        <rule id="100011" level="5">
                <if_group>cms_information</if_group>
                <id>^450|^451|^452|^453|^454|^455|^456|^457|^458|^459</id>
                <description>CMS New Content added event.</description>
        </rule>

        <rule id="100012" level="5">
                <if_group>cms_information</if_group>
                <id>^460|^461|^462|^463|^464|^465|^466|^467|^468|^469</id>
                <description>CMS Existing Content modified event.</description>
        </rule>

        <rule id="100013" level="5">
                <if_group>cms_information</if_group>
                <id>^470|^471|^472|^473|^474|^475|^476|^477|^478|^479</id>
                <description>CMS Existing Content deleted event.</description>
        </rule>

        <rule id="100014" level="5">
                <if_group>cms_information</if_group>
                <id>^445|^446</id>
                <description>CMS User created event.</description>
        </rule>

        <rule id="100015" level="5">
                <if_group>cms_information</if_group>
                <id>^447|449</id>
                <description>CMS User deleted event.</description>
        </rule>

</group>
```

## Log Inspection rule severity levels and their recommended use

| Level | Description | Notes |
|---|---|---|
| Level 0 | Ignored, no action taken | Primarily used to avoid false positives. These rules are scanned before all the others and include events with no security relevance. |
| Level 1 | no predefined use | |
| Level 2 | System low priority notification | System notification or status messages that have no security relevance. |
| Level 3 | Successful or authorized events | Successful login attempts, firewall allow events, and so on. |
| Level 4 | System low priority errors | Errors related to bad configurations or unused devices or applications. They have no security relevance and are usually caused by default installations or software testing. |
| Level 5 | User-generated errors | Missed passwords, denied actions, and so on. These messages typically have no security relevance. |
| Level 6 | Low relevance attacks | Indicate a worm or a virus that provide no threat to the system such as a Windows worm attacking a Linux server. They also include frequently triggered IDS events and common error events. |
| Level 7 | no predefined use | |
| Level 8 | no predefined use | |
| Level 9 | Error from invalid source | Include attempts to login as an unknown user or from an invalid source. The message might have security relevance especially if repeated. They also include errors regarding the **admin** or **root** account. |
| Level 10 | Multiple user generated errors | Include multiple bad passwords, multiple failed logins, and so on. They might indicate an attack, or it might be just that a user forgot his or her credentials. |
| Level 11 | no predefined use | |
| Level 12 | High- | Include error or warning messages from the system, kernel, and so on. |

| Level | Description | Notes |
|---|---|---|
| | importance event | They might indicate an attack against a specific application. |
| Level 13 | Unusual error (high importance) | Common attack patterns such as a buffer overflow attempt, a larger than normal syslog message, or a larger than normal URL string. |
| Level 14 | High importance security event | Typically the result of the correlation of multiple attack rules and indicative of an attack. |
| Level 15 | Attack Successful | Very small chance of false positive. Immediate attention is necessary. |

## strftime() conversion specifiers

| Specifier | Description |
|---|---|
| %a | Abbreviated weekday name (for example, Thu) |
| %A | Full weekday name (for example, Thursday) |
| %b | Abbreviated month name (for example, Aug) |
| %B | Full month name (for example, August) |
| %c | Date and time representation (for example, Thu Sep 22 12:23:45 2007) |
| %d | Day of the month (01 - 31) (for example, 20) |
| %H | Hour in 24 h format (00 - 23) (for example, 13) |
| %I | Hour in 12 h format (01 - 12) (for example, 02) |
| %j | Day of the year (001 - 366) (for example, 235) |
| %m | Month as a decimal number (01 - 12) (for example, 02) |
| %M | Minute (00 - 59) (for example, 12) |
| %p | AM or PM designation (for example, AM) |
| %S | Second (00 - 61) (for example, 55) |
| %U | Week number with the first Sunday as the first day of week one (00 - 53) (for example, 52) |
| %w | Weekday as a decimal number with Sunday as 0 (0 - 6) (for example, 2) |
| %W | Week number with the first Monday as the first day of week one (00 - 53) (for example, 21) |
| %x | Date representation (for example, 02/24/79) |
| %X | Time representation (for example, 04:12:51) |
| %y | Year, last two digits (00 - 99) (for example, 76) |
| %Y | Year (for example, 2008) |
| %Z | Time zone name or abbreviation (for example, EST) |
| %% | A % sign (for example, %) |

For more information, see the following:

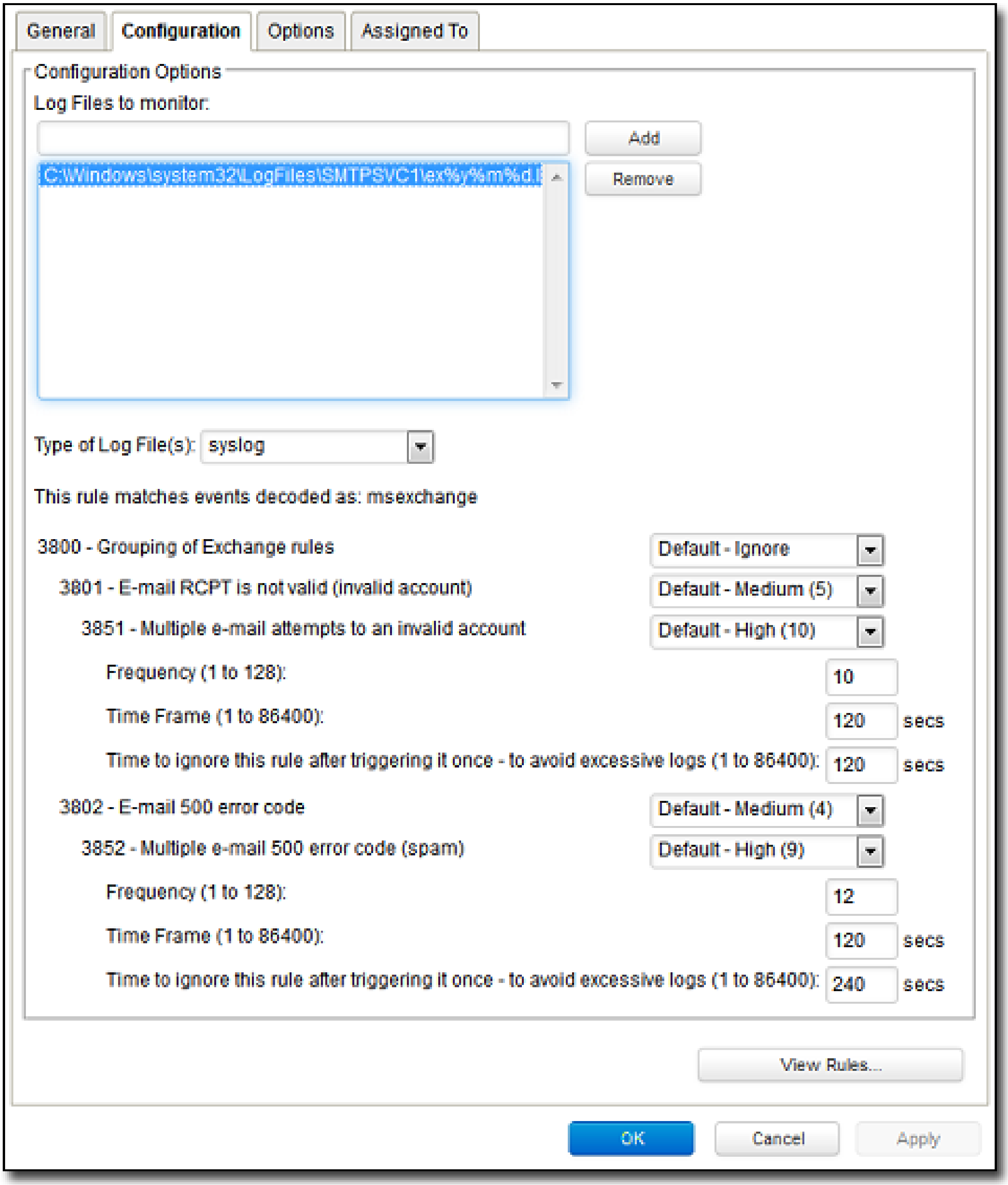
- https://www.php.net/manual/en/function.strftime.php
- www.cplusplus.com/reference/clibrary/ctime/

## Examine a Log Inspection rule

Log Inspection rules are located in Deep Security Manager at **Policies > Common Objects > Rules > Log Inspection Rules**.

### Log Inspection rule structure and the event matching process

The following illustrations shows the contents of the **Configuration** tab of the **Properties** window of the Microsoft Exchange Log Inspection rule:



Configuration Options

Log Files to monitor:

C:\Windows\system32\LogFiles\SMTPSVC1\ex%y%m%d.l

Type of Log File(s): syslog

This rule matches events decoded as: msexchange

3800 - Grouping of Exchange rules: Default - Ignore

3801 - E-mail RCPT is not valid (invalid account): Default - Medium (5)

3851 - Multiple e-mail attempts to an invalid account: Default - High (10)

Frequency (1 to 128): 10

Time Frame (1 to 86400): 120 secs

Time to ignore this rule after triggering it once - to avoid excessive logs (1 to 86400): 120 secs

3802 - E-mail 500 error code: Default - Medium (4)

3852 - Multiple e-mail 500 error code (spam): Default - High (9)

Frequency (1 to 128): 12

Time Frame (1 to 86400): 120 secs

Time to ignore this rule after triggering it once - to avoid excessive logs (1 to 86400): 240 secs

The following is the rule structure:

- 3800 - Grouping of Exchange Rules - Ignore
  - 3801 - Email rcpt is not valid (invalid account) - Medium (4)
    - 3851 - Multiple email attempts to an invalid account - High (9)
      - Frequency - 10
      - Time Frame - 120
      - Ignore - 120
  - 3802 - Email 500 error code - Medium (4)
    - 3852 - Email 500 error code (spam) - High (9)
      - Frequency - 12
      - Time Frame - 120
      - Ignore - 240

The Log Inspection engine applies log events to this structure and checks if a match occurs. For example, if an Exchange event occurs, and this event is an email receipt to an invalid account, the event will match line 3800 (because it is an Exchange event). The event is then be applied to line 3800's subrules: 3801 and 3802.

If there is no further match, this cascade of matches stops at 3800. Because 3800 has a severity level of Ignore, no Log Inspection event would be recorded.

However, an email receipt to an invalid account does match one of 3800's sub-rules: sub-rule 3801. Subrule 3801 has a severity level of Medium(4). If the matching stopped here, a Log Inspection event with a severity level of Medium(4) would be recorded.

But there is still another subrule to be applied to the event: subrule 3851. Subrule 3851 with its three attributes matches if the same event has occurred 10 times within the last 120 seconds. If so, a Log Inspection event with a severity High(9) is recorded. The Ignore attribute tells subrule 3851 to ignore individual events that match subrule 3801 for the next 120 seconds. This is useful for reducing noise.

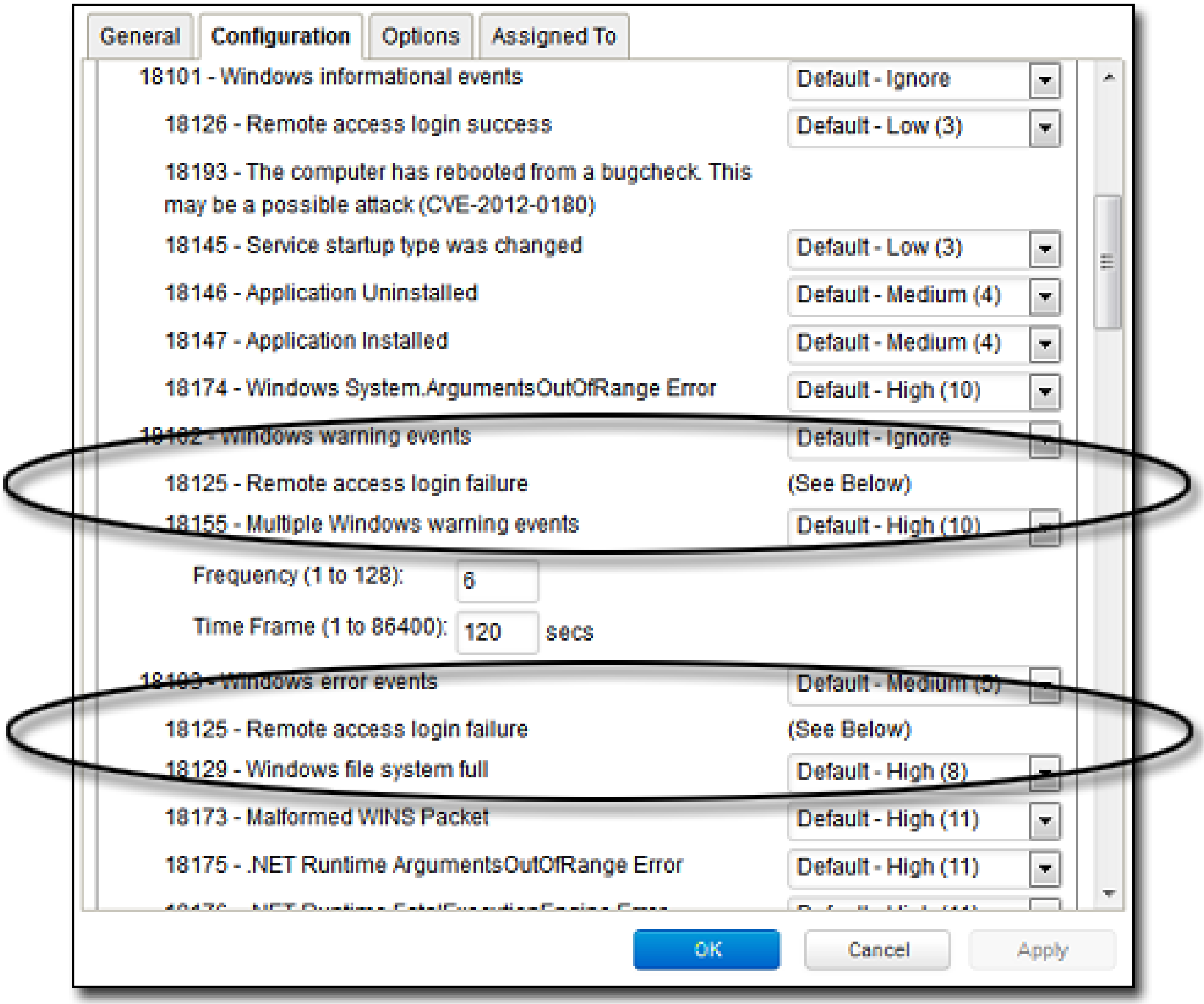
Assuming the parameters of subrule 3851 have been matched, a Log Inspection event with Severity High(9) is now recorded.

Looking at the Options tab of the Microsoft Exchange Rule, you can see that Deep Security Manager raises an alert if any subrules with a severity level of Medium(4) have been matched. Since this is the case in this example, the alert is raised (if **Alert when this rule logs an event** is selected).

### Duplicate Subrules

Some Log Inspection rules have duplicate subrules. To see an example, open the Microsoft Windows Events rule and select the **Configuration** tab. Note that subrule 18125 (Remote access login failure) appears under subrules 18102 and 18103. Also note that in both cases subrule 18125 does not have a severity value, it only says "See Below".

Instead of being listed twice, Rule 18125 is listed once at the bottom of the **Configuration** page:



18101 - Windows informational events — Default - Ignore
18126 - Remote access login success — Default - Low (3)
18193 - The computer has rebooted from a bugcheck. This may be a possible attack (CVE-2012-0180)
18145 - Service startup type was changed — Default - Low (3)
18146 - Application Uninstalled — Default - Medium (4)
18147 - Application Installed — Default - Medium (4)
18174 - Windows System.ArgumentsOutOfRange Error — Default - High (10)
18102 - Windows warning events — Default - Ignore
18125 - Remote access login failure — (See Below)
18155 - Multiple Windows warning events — Default - High (10)
Frequency (1 to 128): 6
Time Frame (1 to 86400): 120 secs
18103 - Windows error events — Default - Medium (5)
18125 - Remote access login failure — (See Below)
18129 - Windows file system full — Default - High (8)
18173 - Malformed WINS Packet — Default - High (11)
18175 - .NET Runtime ArgumentsOutOfRange Error — Default - High (11)
18176 - .NET Runtime FatalExecutionEngineError — Default - High (11)

# Configure Application Control

## About Application Control

Note: You can enable application control for computers running Deep Security Agent 10.0 or higher. For a list of operating systems where application control is supported, see "Supported features by platform" on page 425.

Application control continuously monitors for software changes on your protected servers. Based on your policy configuration, application control either prevents unauthorized software from running until it is explicitly allowed, or allows unauthorized software until it is explicitly blocked. Which option you choose depends on the level of control you want over your environment.

Warning: Application control continuously monitors your server and logs an event whenever a software change occurs. It is not intended for environments with self-changing software or that normally creates executables, such as some web or mail servers. To ensure Application Control is appropriate for your environment, check "What does application control detect as a software change?" on page 995.

Tip: You can automate Application Control creation and configuration using the Deep Security API. For more information, see the Configure Application Control guide in the Deep Security Automation Center.

### Key concepts

**Targeted protection state:** One of the main decisions you need to make when setting up application control is deciding your targeted protection state. Do you want to prevent all new or changed software from running, unless you manually specify that it is allowed? Or do you want it to run by default unless you specifically block it? One approach is to initially allow unrecognized software to run when you first enable application control and there's a lot of unrecognized software. As you add application control rules and the volume of unrecognized software decreases, you could switch to block mode.

**Application control rule:** Rules specify whether software is allowed or blocked on a particular computer.

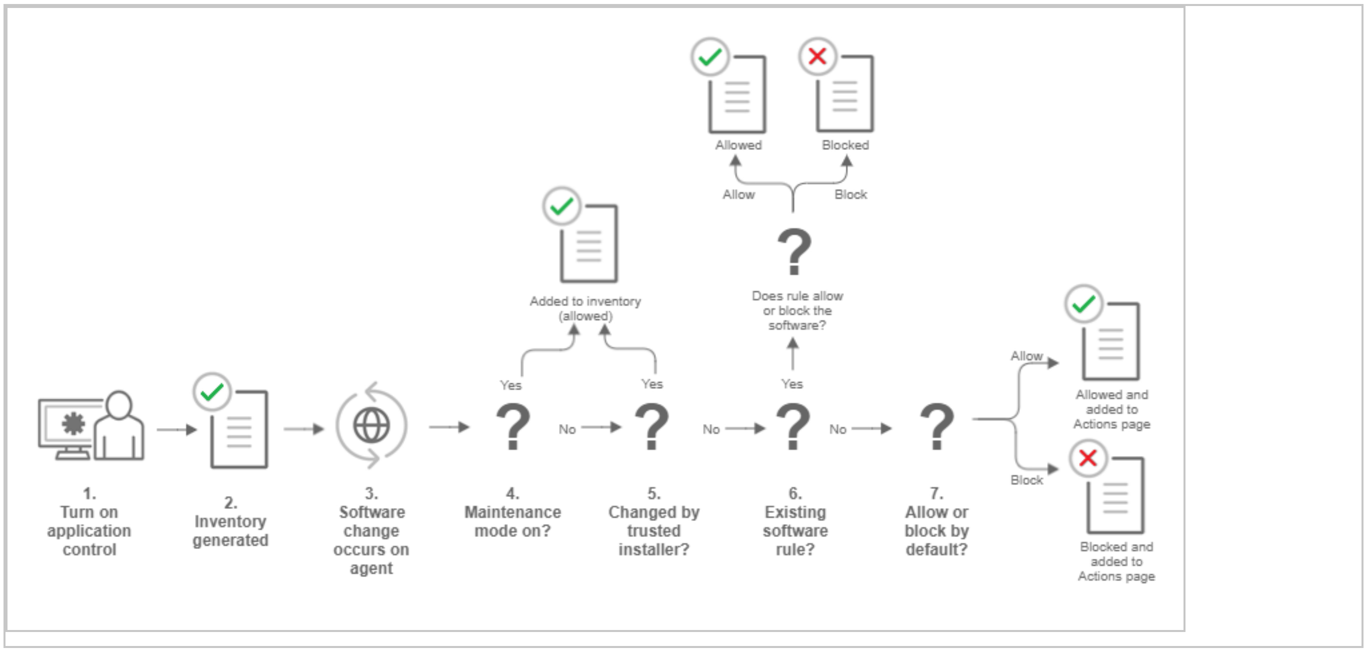
**Inventory:** Initial list of software that is installed on the computer and allowed to run. Make sure only software that you want to allow is installed on the computer. When you enable application control, all currently installed software is added to the computer's inventory and allowed to run. When a computer is in maintenance mode, any software changes made to the computer are added to the computer's inventory and allowed to run. A computer's software inventory is stored on the Deep Security Agent and is not displayed in Deep Security Manager.

**Unrecognized software:** Software that isn't in a computer's inventory and isn't already covered by an application control rule. See "What does application control detect as a software change?" on page 995

**Maintenance mode:** If you are planning to install or update software, we strongly advise that you turn on maintenance mode. In maintenance mode, application control continues to block software that is specifically blocked by an Application Control rule, but allows new or updated software to run and adds it to the computer's inventory. See "Turn on maintenance mode when making planned changes" on page 1001.

**Note:** To improve overall system security, the inventory does not include software on remote file systems, and maintenance mode does not automatically allow new or updated software from remote file systems. Software on remote file systems must be added to the inventory manually.

## How does application control work?


Allowed
Blocked
Allow
Block
Added to inventory (allowed)
Does rule allow or block the software?
Yes
Yes
Yes
Allow
Allowed and added to Actions page
No
No
No
Block
Blocked and added to Actions page
1. Turn on application control
2. Inventory generated
3. Software change occurs on agent
4. Maintenance mode on?
5. Changed by trusted installer?
6. Existing software rule?
7. Allow or block by default?

1. You enable application control in a policy and assign the policy to a computer that is protected by a Deep Security Agent (see "Turn on Application Control" on page 997).

2. When the agent receives the policy, it creates an inventory of all software installed on the computer. All software listed in the inventory is assumed to be safe and is allowed to run on that computer. This inventory list is not visible from Deep Security Manager, which means you need to be absolutely certain that only good software is installed on a computer where you intend to enable application control.
3. After the inventory is finished, application control is aware of any software changes on the computer. A software change could be new software that appears on the computer or changes to existing software.
4. If the computer is in maintenance mode, the Deep Security Agent adds the software to its inventory list and it is allowed to run. This change is not visible in Deep Security Manager. See "Turn on maintenance mode when making planned changes" on page 1001.
5. If the change was made by a trusted installer, the Deep Security Agent adds the software to its inventory list and allows it to run. For example, when Microsoft Windows self-initiates a component update, hundreds of new executable files may be installed. Application control auto-authorizes many file changes that are created by well-known Windows processes and does not list these changes in Deep Security Manager. Removing the "noise" associated with expected software changes provides you with clearer visibility into changes that may need your attention.

   **Note:** The trusted installer feature is available with Deep Security Agent 10.2 or later.

6. If the computer's ruleset contains a rule for this exact piece of software, the software is allowed or blocked according to the rule that's in place. See "What does application control detect as a software change?" on page 995
7. If software is not in the computer's inventory and is not covered by an existing rule, it's considered unrecognized software. The policy assigned to the computer specifies how unrecognized software is handled. Depending on the policy configuration, it's either allowed to run or is blocked. If the software is blocked and it is able to produce error messages in the OS, an error message on the protected computer indicates that the software does not have permissions to run or that access is denied.

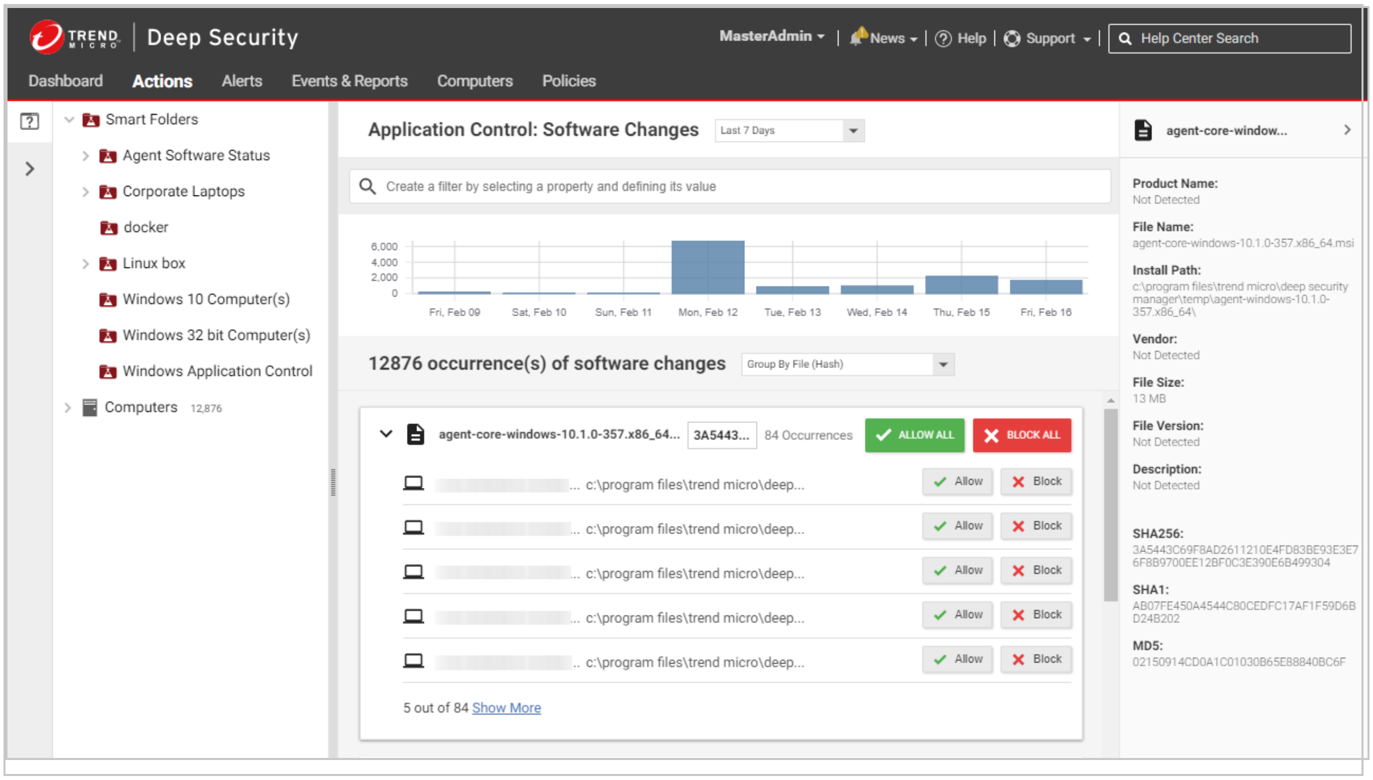
   The unrecognized software appears on the **Application Control - Software Changes** page in Deep Security Manager. On that page, an administrator can click **Allow** or **Block** to create an allow or block rule for that piece of software on a particular computer. An allow or block rule takes precedence over the default action specified in the policy. See "Monitor new and changed software" on page 998.

## A tour of the application control interface

There are a few places in Deep Security Manager where you can see changes related to application control:

- "Application Control: Software Changes (Actions)" below
- "Application Control Rulesets" on the next page
- "Security Events" on page 995

### Application Control: Software Changes (Actions)



12876 occurrence(s) of software changes

agent-core-windows-10.1.0-357.x86_64... 3A5443... 84 Occurrences

[redacted]... c:\program files\trend micro\deep...

[redacted]... c:\program files\trend micro\deep...

[redacted]... c:\program files\trend micro\deep...

[redacted]... c:\program files\trend micro\deep...

[redacted].. c:\program files\trend micro\deep...

5 out of 84 Show More

**Product Name:**
Not Detected

**File Name:**
agent-core-windows-10.1.0-357.x86_64.msi

**Install Path:**
c:\program files\trend micro\deep security manager\temp\agent-windows-10.1.0-357.x86_64\

**Vendor:**
Not Detected

**File Size:**
13 MB

**File Version:**
Not Detected

**Description:**
Not Detected

**SHA256:**
3A5443C69F8AD2611210E4FD83BE93E3E76F8B9700EE12BF0C3E390E6B499304

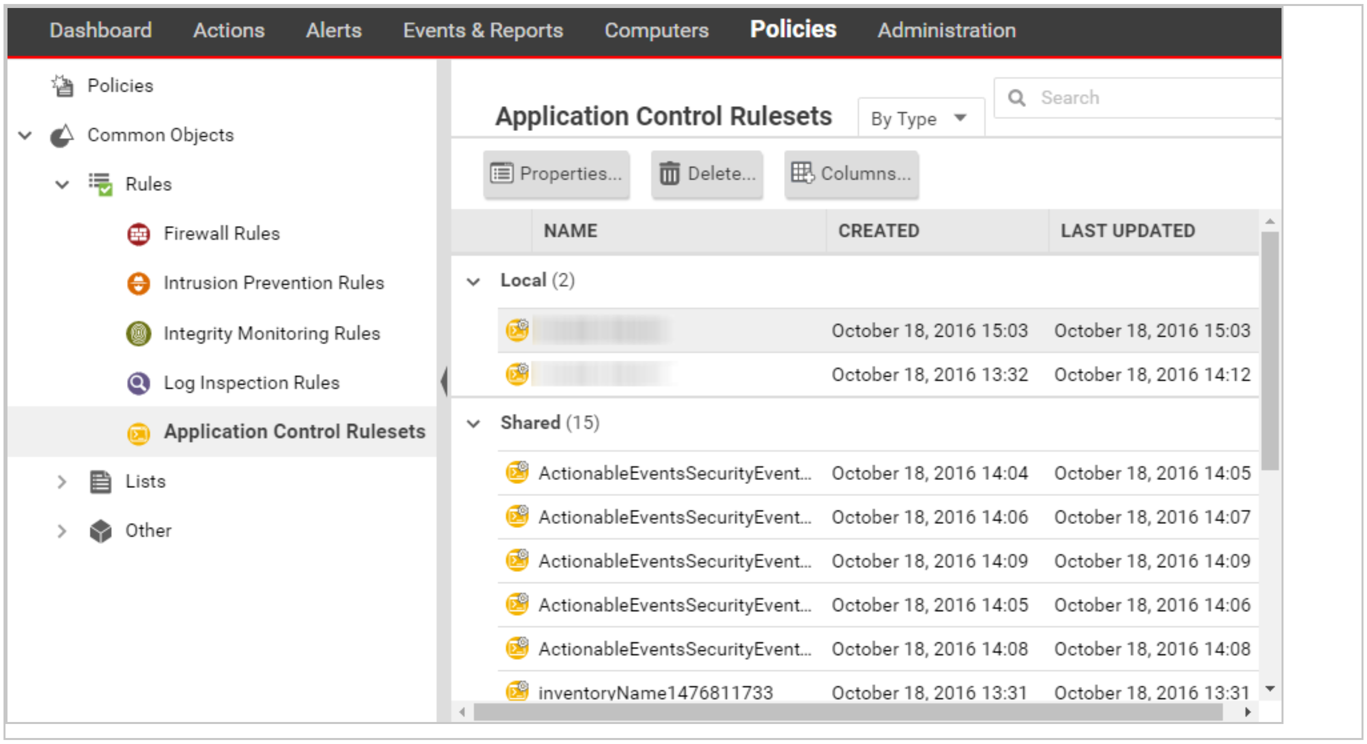
**SHA1:**
AB07FE450A4544C80CEDFC17AF1F59D6BD24B202

**MD5:**
02150914CD0A1C01030B65E88840BC6F

The **Application Control: Software Changes** page is displayed when you click **Actions** in Deep Security Manager. It displays all unrecognized software (software that isn't in a computer's inventory and doesn't have a corresponding application control rule). Software changes are allowed or blocked at the computer level, so if a particular piece of software is installed on fifty computers, it will appear on that page fifty times. However, if you know that a certain piece of software should be allowed or blocked everywhere, you can filter the **Actions** page to sort the changes by file hash and then click **Allow All** to allow it on all computers where the software is installed.

The policy applied to a computer specifies whether it will allow all unrecognized software to run by default, or block all unrecognized software, but no explicit application control rule is created until you click "Allow" or "Block" on the Actions page. When you click Allow or Block, a corresponding rule appears in the ruleset for the computer. The rulesets are displayed on the **Application Control Rulesets** page.

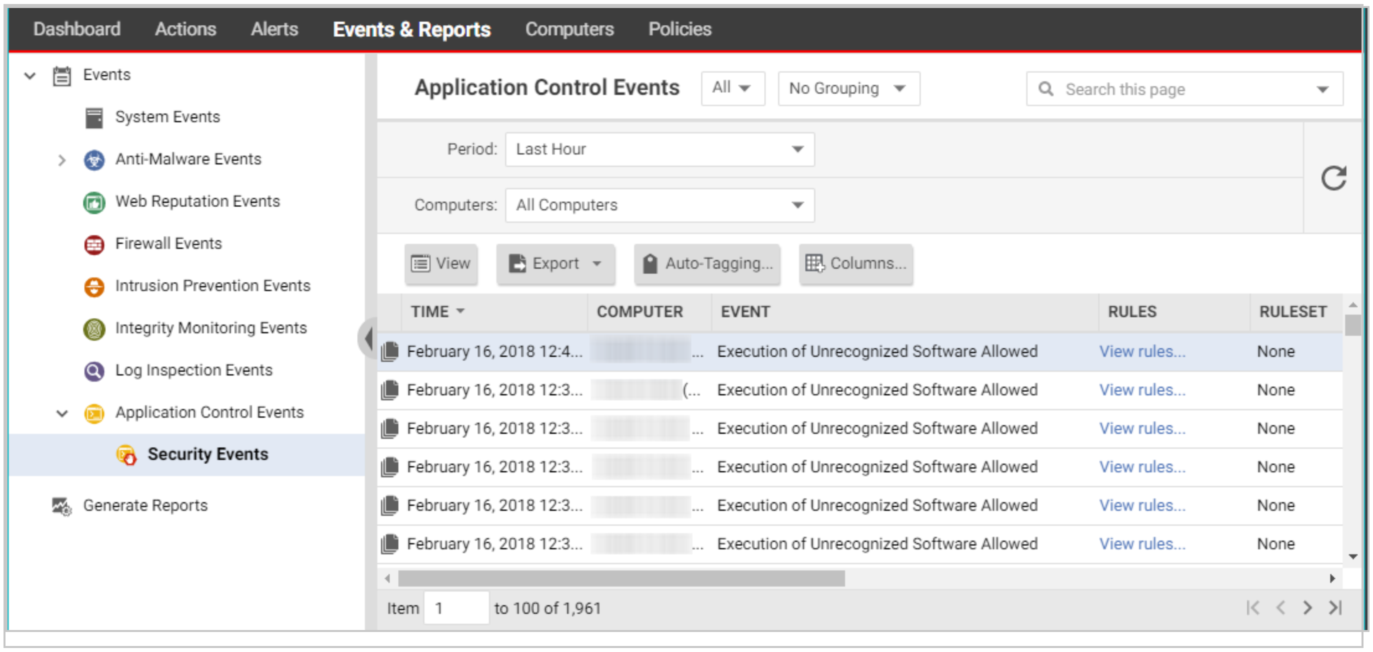
Application Control Rulesets



| NAME | CREATED | LAST UPDATED |
|---|---|---|
| **Local** (2) | | |
| [redacted] | October 18, 2016 15:03 | October 18, 2016 15:03 |
| [redacted] | October 18, 2016 13:32 | October 18, 2016 14:12 |
| **Shared** (15) | | |
| ActionableEventsSecurityEvent... | October 18, 2016 14:04 | October 18, 2016 14:05 |
| ActionableEventsSecurityEvent... | October 18, 2016 14:06 | October 18, 2016 14:07 |
| ActionableEventsSecurityEvent... | October 18, 2016 14:09 | October 18, 2016 14:09 |
| ActionableEventsSecurityEvent... | October 18, 2016 14:05 | October 18, 2016 14:06 |
| ActionableEventsSecurityEvent... | October 18, 2016 14:08 | October 18, 2016 14:08 |
| inventoryName1476811733 | October 18, 2016 13:31 | October 18, 2016 13:31 |

To see the ruleset for a computer, go to **Policies > Common Objects > Rules > Application Control Rulesets**. To see which rules are part of a ruleset, double-click the ruleset and go to the **Rules** tab. The Rules tab displays the pieces of software that have rules associated with them and enables you to change allow rules to block, and vice versa.

### Security Events



Application Control Events

Period: Last Hour

Computers: All Computers

| TIME | COMPUTER | EVENT | RULES | RULESET |
|---|---|---|---|---|
| February 16, 2018 12:4... | [redacted] | Execution of Unrecognized Software Allowed | View rules... | None |
| February 16, 2018 12:3... | [redacted] | Execution of Unrecognized Software Allowed | View rules... | None |
| February 16, 2018 12:3... | [redacted] | Execution of Unrecognized Software Allowed | View rules... | None |
| February 16, 2018 12:3... | [redacted] | Execution of Unrecognized Software Allowed | View rules... | None |
| February 16, 2018 12:3... | [redacted] | Execution of Unrecognized Software Allowed | View rules... | None |
| February 16, 2018 12:3... | [redacted] | Execution of Unrecognized Software Allowed | View rules... | None |

Item 1 to 100 of 1,961

**Events & Reports > Events > Application Control Events > Security Events** displays all unrecognized software that either has been run on a computer or has been prevented from running by a block rule. You can filter this list by time period and other criteria.

For each event (except aggregated events), you can click **View rules** to change the rule from Allow to Block or vice versa. Deep Security Agent 10.2 or later includes event aggregation logic to reduce the volume of logs when the same event occurs repeatedly.

## What does application control detect as a software change?

Unlike integrity monitoring, which monitors any file, application control looks only for software files when examining the initial installation and monitoring for change.

Software can be:

- Windows applications (.exe, .com, .dll, .sys), Linux libraries (.so) and other compiled binaries and libraries
- Java .jar and .class files, and other compiled byte code
- PHP, Python, and shell scripts, and other web apps and scripts that are interpreted or compiled on the fly
- Windows PowerShell scripts, batch files (.bat), and other Windows-specific scripts (.wsf, .vbs, .js)

For example, WordPress and its plug-ins, Apache, IIS, nginx, Adobe Acrobat, app.war, and /usr/bin/ssh would all be detected as software.

Application control checks a file's extension to determine whether it's a script. Additionally, on Linux, application control treats any file with execute permissions as if it's a script.

**Note:** On Windows computers, application control tracks changes on the local file system, but not on network locations, CD or DVD drives, or USB devices.

Application control is integrated with the kernel (on Linux computers) and file system, so it has permissions to monitor the whole computer, including software installed by root or administrator accounts. The agent watches for disk write activity on software files, and for attempts to execute software.

### Differences in how Deep Security Agent 10 and 11 compare files

To determine whether software is new or has changed, Deep Security 10 agents compare the file with the initially installed software's SHA-256 hash, file size, path, and file name (they have a "file-based" ruleset). Deep Security 11 (and newer) agents compare only the file's SHA-256 hash and file size (they have a "hash-based" ruleset). Because the rules created by Deep Security 11 (and newer) agents compare only the unique hash and file size, a rule will continue to be applied even if the software file is renamed or moved. As a result, using Deep Security 11 (and newer) agents reduces the number of software changes that you need to deal with.

A Deep Security 10 agent continues to use a file-based ruleset until it is upgraded to Deep Security 11.0 or newer. When you upgrade an agent to version 11.0 or newer, its ruleset is converted to use hash-based rules. If there are multiple file-based rules for the same hash value, they are consolidated into one hash-based rule. If the rules being consolidated conflict with each other (one rule blocks the file and another allows it), the new hash-based rule will be an "allow" rule.

## Set up Application Control

**Warning:** Application Control continuously monitors your server and logs an event whenever a software change occurs. It is not intended for environments with self-changing software or that normally creates executables, such as some web or mail servers. To ensure Application Control is appropriate for your environment, check "What does application control detect as a software change?" on the previous page.

For information about how Application Control works, see "About Application Control" on page 990.

To enable Application Control and monitor software changes:

1. "Turn on Application Control" below
2. "Monitor new and changed software" on the next page
3. "Turn on maintenance mode when making planned changes" on page 1001

This article also provides "Application Control tips and considerations" on page 1002 that you should be aware of when working with Application Control.

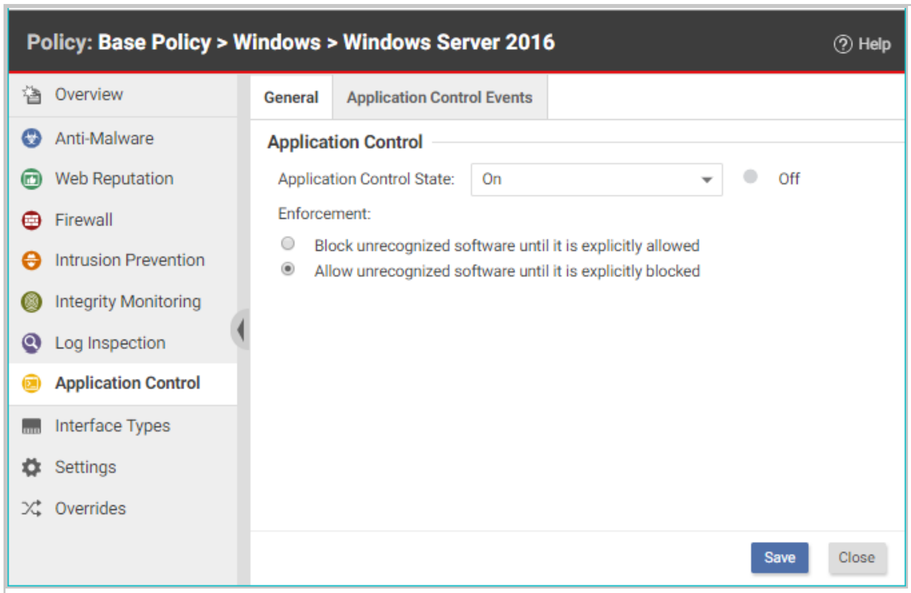
Once you've enabled Application Control, you can also learn how to:

- "View and change Application Control rulesets" on page 1007
- "Reset Application Control after too much software change" on page 1039
- "Monitor Application Control events" on page 1004
- "Use the API to create shared and global rulesets" on page 1040

## Turn on Application Control

You can enable Application Control in the settings for a computer or in policies:

1. Open the Computer or Policy editor and go to **Application Control > General**.
2. Set the **Application Control State** to "On" or "Inherited (On)".
3. Under **Enforcement**, select your targeted protection state:
   - **Block unrecognized software until it is explicitly allowed**
   - **Allow unrecognized software until it is explicitly blocked** (we recommend that you choose this option when initially setting up Application Control)
4. Click **Save**.



Application Control

Application Control State: On ○ Off

Enforcement:

○ Block unrecognized software until it is explicitly allowed

● Allow unrecognized software until it is explicitly blocked

The next time that the Deep Security Manager and agent connect, the agent scans and then generates an inventory of all software installed on the computer and creates rules that allow all the software that it finds. This initial inventory can take 15 minutes or longer, depending on your environment.

Warning: When generating an inventory, Application Control does not include software on remote file systems such as a CIFS (Common Internet File System) or NFS (Network File System). Software on remote file systems must be manually added to the inventory.

To check that Application Control is working as expected, follow the instructions in "Verify that Application Control is enabled" on page 1003.

## Monitor new and changed software

Once an inventory has been created on a protected computer, any software executable files that are added or changed are classified as a "software change" and appear on the **Actions** page in Deep Security Manager. When unrecognized software runs, or attempts to run and is blocked, the event is listed under **Events & Reports > Events > Application Control Events > Security Events**. For more information, see "Application Control events" on page 1284

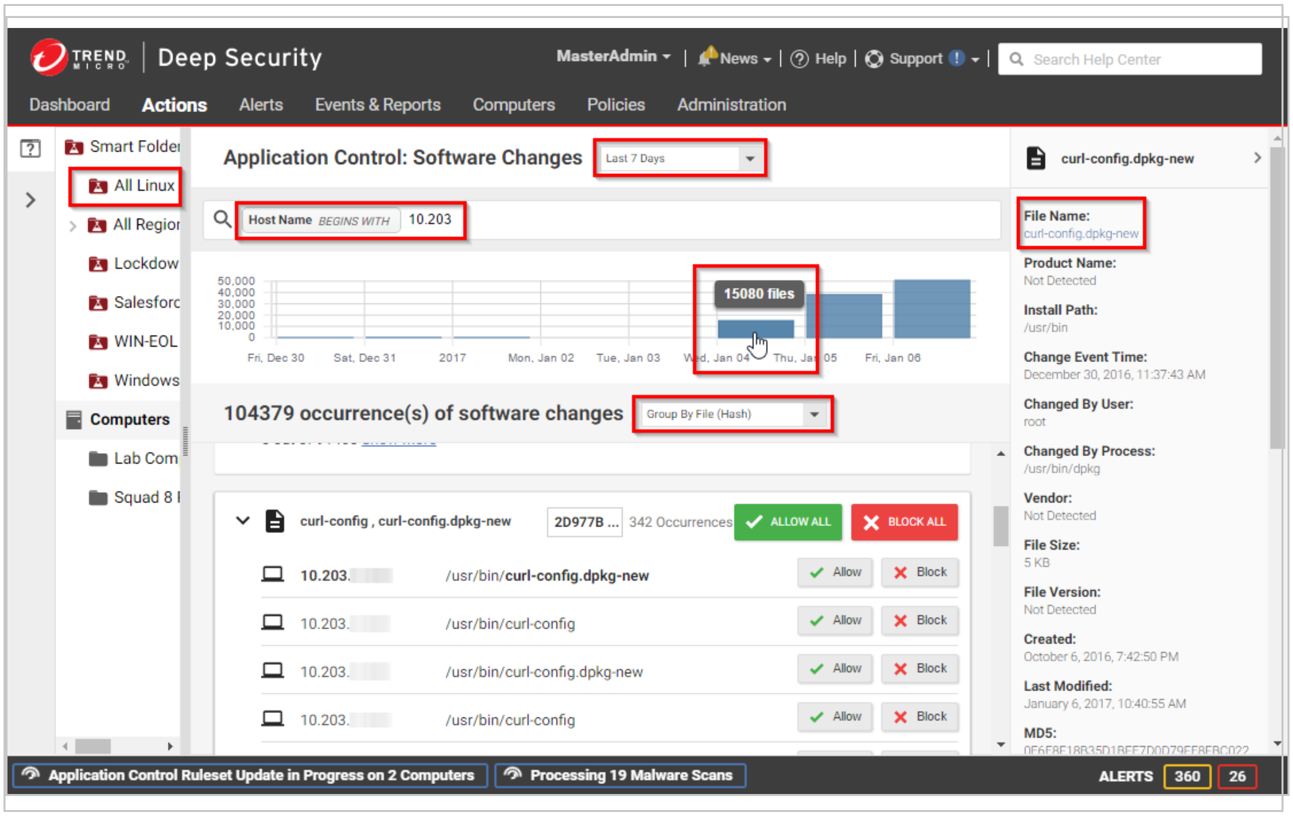
After you initially enable Application Control, you will likely see a lot of software changes on the **Actions** page. This can happen when allowed software creates new executables, renames files, or relocates files through the normal course of operation. As you add rules to tune Application Control, you should see fewer software changes.

To quickly find all software changes on all computers and easily create allow or block rules for them, use the **Actions** tab.

> Tip: You can automate the creation of allow or block rules using the Deep Security API. For more information, see the Allow or block unrecognized software guide in the Deep Security Automation Center.

1. In Deep Security Manager, go to **Actions**.
2. There are several ways you can filter to see only specific occurrences of unrecognized software.

> Tip: Instead of evaluating each software change on each computer individually, use the filters described below to find software changes that you know are good, and allow them in bulk.



File Name: curl-config.dpkg-new
Product Name: Not Detected
Install Path: /usr/bin
Change Event Time: December 30, 2016, 11:37:43 AM
Changed By User: root
Changed By Process: /usr/bin/dpkg
Vendor: Not Detected
File Size: 5 KB
File Version: Not Detected
Created: October 6, 2016, 7:42:50 PM
Last Modified: January 6, 2017, 10:40:55 AM
MD5: 0E6E8F18B35D1BEE7D0D79EE8EBC022

To reduce the number of software changes being displayed:

- From the drop-down list next to **Application Control: Software Changes**, select a time range such as **Last 7 Days**. You can also click a bar in the graph near the top of the page to display the changes for that time period.

- In the pane on the left, click **Computers** and select an individual computer or group, or click **Smart Folders** to display only the computers that are included in a particular smart folder (see "Group computers dynamically with smart folders" on page 1467).

  > **Note:** Unlike the **Computers** tab, the **Software Changes** pane usually does not show all computers. It only displays computers where Application Control has detected software changes that don't already have allow or block rules.

- Enter search terms and operators in the search filter field. You search for these attributes: Change By Process, Change By User, File Name, Host Name, Install Path, MD5, SHA1, and SHA256. For example, you could find all changes made by a particular user that you trust and click **Allow All** to allow all of their changes. Or if a particular software update was installed across your organization (while maintenance mode was not enabled), filter the page according to the hash value of the file and click **Allow All** to allow all occurrences.

  > **Tip:** Details about a software change are displayed in the right pane. You can click the file name or computer name in the details to add it to your search filter.

- Select whether to **Group by File (Hash)** or **Group by Computer**.

3. Click either **Allow** or **Block** to add an allow or block rule on that computer, for that software. If you need more information to decide whether to allow or block, click the software name, then use the details panel on the right side.

   The next time that the agent connects with the Deep Security Manager, it receives the new rules.

### Tips for handling changes

- For most environments, we suggest that you select the **Allow unrecognized software until it is explicitly blocked** option to allow software changes by default when you first enable Application Control and add allow and block rules for changes that you see on the **Actions** page. Eventually, the rate of software changes should decrease. At that point, you could consider blocking software changes by default and creating allow rules for the software that you know is good. Some organizations prefer to continue to allow changes by default and monitor the **Actions** page for software that should be blocked.
- You may prefer to start by evaluating security events, rather than dealing with unrecognized software first. Security events show you which unrecognized software has run (or attempted to run). For information on security events, see "Monitor Application Control events" on page 1004.

- When an unrecognized file is allowed to execute and you want to continue to allow it, create an Allow rule. In addition to allowing the file's execution, the event is no longer logged for that file, which reduces noise and makes important events easier to find.
- When a known file's execution is blocked, consider cleaning that file from the computer, especially for repeated occurrences.
- Keep in mind that software changes are listed for each computer where they occur. You must allow or block the software for each computer.
- Rules are assigned to computers, not to policies. For example, if `helloworld.py` is detected on three computers, when you click **Allow All** or **Block All**, this would affect only three computers. It won't affect future detections on other computers, because they have their own rulesets.
- If you see changes related to software updates that you can control, use the maintenance mode feature when performing those updates. See "Turn on maintenance mode when making planned changes" below.

## Turn on maintenance mode when making planned changes

Warning: With maintenance mode enabled, Application Control does not scan remote file systems such as a CIFS (Common Internet File System) or NFS (Network File System). Since software changes on remote file systems cannot be auto-authorized, we recommended that you manually add them to the software inventory as required.

When you install patches, upgrade software, or deploy web applications, Application Control will detect them. Depending on your setting for how to handle unrecognized software, this could block that software until you use the **Actions** tab to create allow rules.

To avoid extra down time and alerts during deployment and maintenance windows, you can put Application Control into a mode designed for maintenance windows. While maintenance mode is enabled, Application Control will continue to enforce rules that block software, but it will allow new or updated software to run and automatically add it to the computer's inventory.

Tip: You can automate maintenance mode using the Deep Security API. For more information, see the Configure maintenance mode during upgrades guide in the Deep Security Automation Center.

1. In Deep Security Manager, go to **Computers**.
2. Select one or more computers, then click **Actions > Turn On Maintenance Mode**.

3. Select the duration of your maintenance window.

   Maintenance mode will automatically disable itself when your maintenance window is scheduled to end. Alternatively, if you'd prefer to manually disable maintenance mode when updates are finished, select **Indefinite**.

   On the **Dashboard**, the **Application Control Maintenance Mode Status** widget indicates whether the command succeeded.

4. Install or upgrade software.
5. If you chose to disable maintenance mode manually, remember to disable maintenance mode in order to start to detect software changes again.

## Application Control tips and considerations

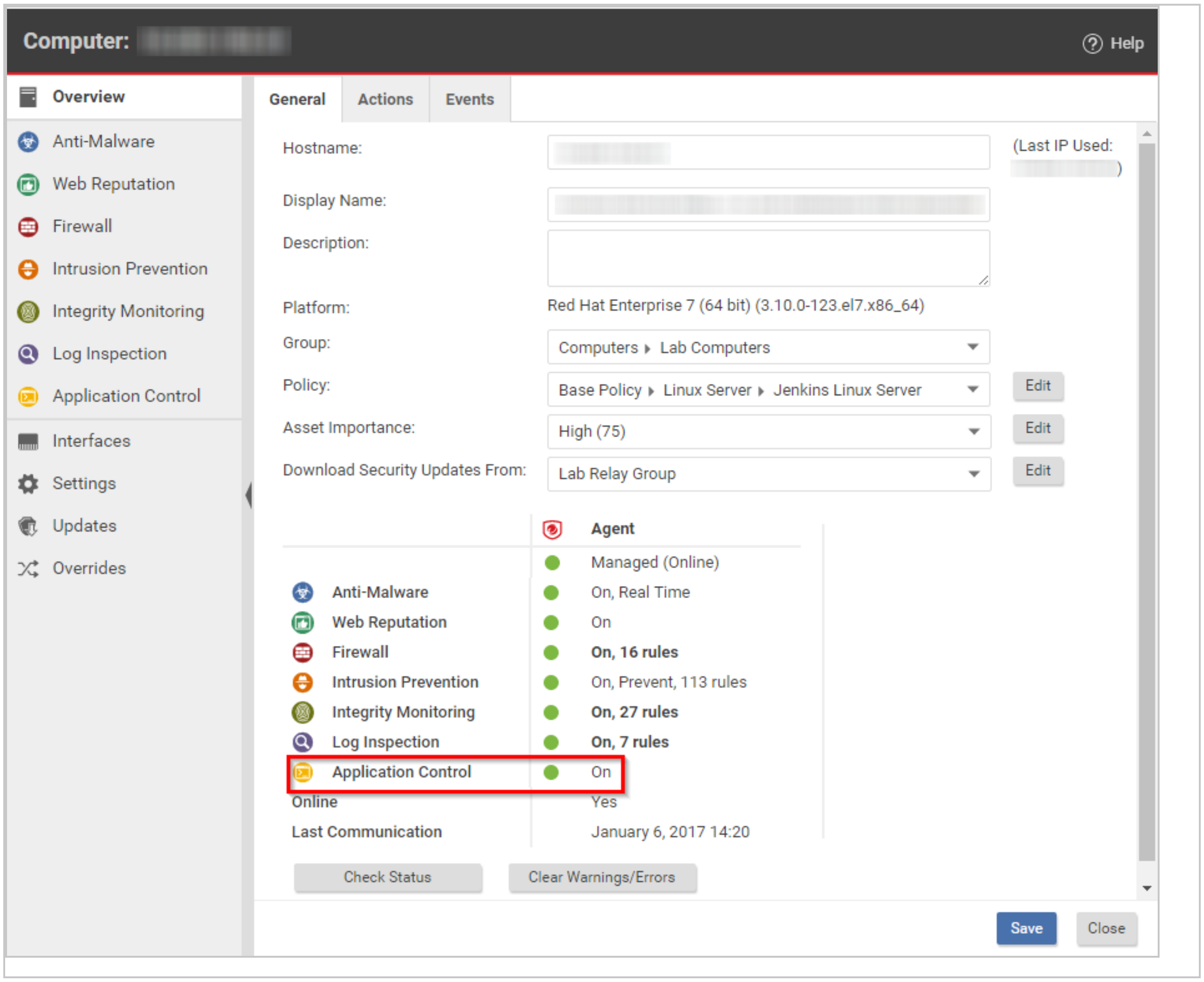
- For better performance with Application Control, use Deep Security anti-malware instead of Windows Defender. See "Coexistence of Deep Security Agent with Microsoft Defender Antivirus" on page 766.
- If you create a block rule for a batch file or PowerShell script, you will not be able to copy, move, or rename the file when using its associated interpreter (powershell.exe for PowerShell scripts or cmd.exe for batch files).
- If you add an allow or block rule, it is normally sent to the agent the next time the agent connects to Deep Security Manager. If you see an error saying that the ruleset upload was not successful, verify that network devices between the agent and the manager or relay allow communications on the heartbeat port number or relay port numbers.
- To verify that a block rule is working, try to run the software that you just blocked. (For details on how Deep Security Agent detects changes, see "What does application control detect as a software change?" on page 995)
- When blocked software remains installed, Application Control continues to record logs and show alerts when it blocks the software from running. To reduce the permission error logs on the computer and also reduce your attack surface, uninstall the software that Application Control is blocking. Once that is done, if you want to dismiss related alerts, either go to **Alerts** or go to **Dashboard**, click the alert, and then click **Dismiss Alert**. Not all alerts can be dismissed. For more information, see "Predefined alerts" on page 1196.
- For performance reasons, if the computer has too much software change, Application Control will continue to enforce existing rules, but stop detecting and displaying software changes. To resolve this, see "Reset Application Control after too much software change" on page 1039.

## Verify that Application Control is enabled

For an overview of Application Control, see "About Application Control" on page 990. For initial configuration instructions, see "Set up Application Control" on page 996.

When Application Control is enabled and has finished its initial software inventory scan:

- The **State** field indicates "On" or "On, Blocking unrecognized software".
- On **Computers**, the **Status** field changes from "Application Control Ruleset Build In Progress" to "Managed (Online)".
- **Events & Reports > Events > System Events** will record "Application Control Ruleset Build Started" and "Application Control Ruleset Build Completed". (If you don't see any logs, see "Choose which Application Control events to log" on page 1005.)



Hostname: [redacted]

(Last IP Used: [redacted])

Display Name: [redacted]

Description:

Platform: Red Hat Enterprise 7 (64 bit) (3.10.0-123.el7.x86_64)

Group: Computers ▸ Lab Computers

Policy: Base Policy ▸ Linux Server ▸ Jenkins Linux Server

Asset Importance: High (75)

Download Security Updates From: Lab Relay Group

| | Agent |
|---|---|
| | ● Managed (Online) |
| Anti-Malware | ● On, Real Time |
| Web Reputation | ● On |
| Firewall | ● **On, 16 rules** |
| Intrusion Prevention | ● On, Prevent, 113 rules |
| Integrity Monitoring | ● **On, 27 rules** |
| Log Inspection | ● **On, 7 rules** |
| Application Control | ● On |
| Online | Yes |
| Last Communication | January 6, 2017 14:20 |

To verify that Application Control is working:

1. Copy an executable to the computer or add execute permissions to a plain text file. Try to run the executable.

   Depending on your enforcement setting for unrecognized software, it should be either blocked or allowed. Once Application Control has built initial allow rules or downloaded a shared ruleset, if any change is detected, it should appear in the **Actions** tab, which you can use to create allow and block rules (see "Monitor new and changed software" on page 998). Depending on your alert configuration, you will also see an alert if unrecognized software is detected, or if Application Control blocks software from launching (see "Monitor Application Control events" below). The event should persist until the software change no longer exists, or until the oldest data has been removed from the database.

2. Add an allow or block rule for your test software and then try again. This time, Application Control should apply your allow or block rule.

   > Tip: If software is accidentally blocked because you've selected **Block unrecognized software until it is explicitly allowed** and the software isn't being recognized, the **Reason** column in Application Control event logs can help you to troubleshoot the cause.

## Monitor Application Control events

For an overview of Application Control, see "About Application Control" on page 990. For initial configuration instructions, see "Set up Application Control" on page 996.

By default, when you enable Application Control it logs events, such as when there are software changes or when it blocks software from executing. Application Control events appear on the **Actions** and **Events & Reports** pages. If configured, an alert appears on the **Alerts** page.

You can configure some of which Application Control event logs are recorded, and which are forwarded to external SIEM systems, or syslog servers.

To monitor for software changes on computers:

1. "Choose which Application Control events to log" on the next page
2. "View Application Control event logs" on the next page
3. "Interpret aggregated security events" on the next page
4. "Monitor Application Control alerts" on page 1006

## Choose which Application Control events to log

1. Go to **Administration > System Settings > System Events**.
2. Scroll down to the Application Control events such as Event ID 7000 "Application Control Events Exported".
3. If you want to record event logs for that type of event, select **Record**.

   When those events occur, they appear on **Events & Reports > Events > System Events**. Logs are kept until they meet maximum log age criteria. For details, see "About Deep Security event logging" on page 1046.

   > **Note:** Events that appear on **Computers > Details > Application Control > Events** are not configured here. They are always logged.
4. If you want to forward event logs to a SIEM, or syslog server, select **Forward**.
5. If you use an external SIEM, you may need to load the list of possible Application Control event logs, and indicate what action to take. For a list of Application Control events, see "System events" on page 1233 and "Application Control events" on page 1284.

## View Application Control event logs

Application Control generates system events and security events:

- **System event:** An audit event that provides a history of configuration changes or software updates. To see system events click **Events & Reports > Events > System Events**. For a list, see "System events" on page 1233.
- **Security event:** An event that occurs on the agent when Application Control blocks or allows unrecognized software, or blocks software due to a block rule. To see security events, click **Events & Reports > Events > Application Control Events > Security Events**. For a list, see "Application Control events" on page 1284.

## Interpret aggregated security events

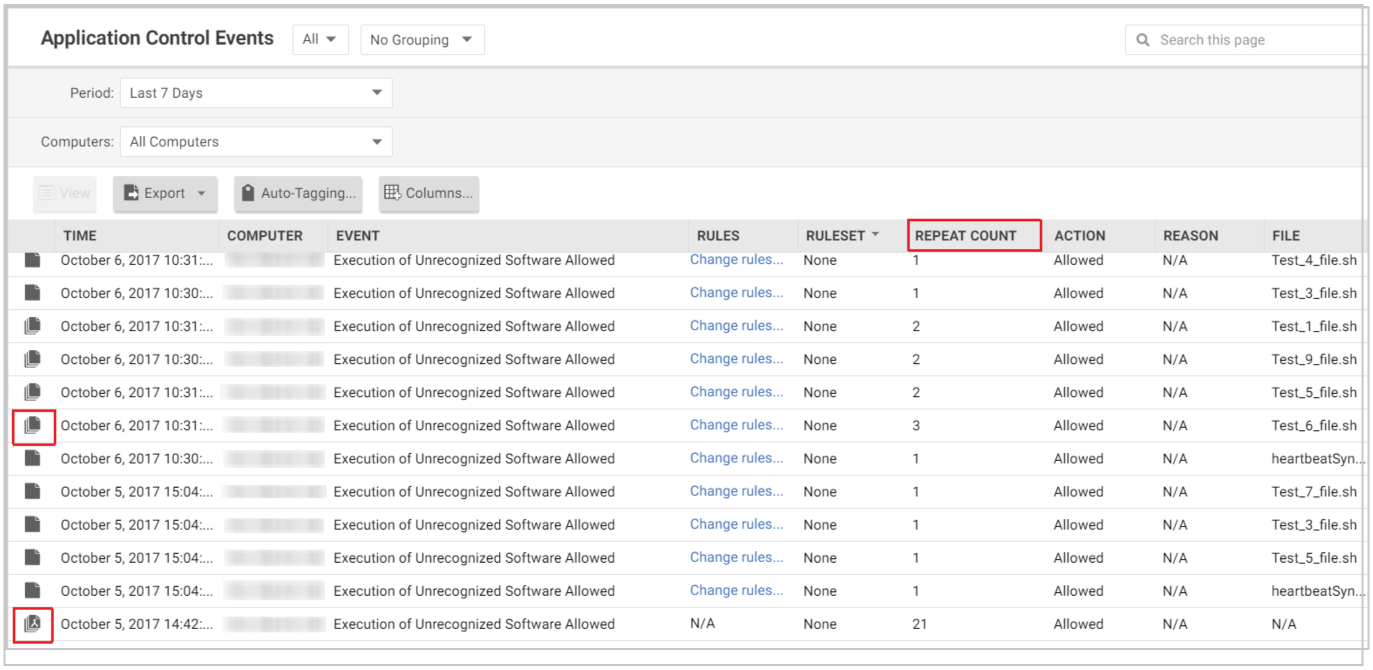
When an agent heartbeat includes several instances of the same security event, Deep Security aggregates the events in the Security Events log. Event aggregation reduces the number of items in the log, making it easier to find important events:

- When the event occurs for the same file, which is usually the case, the log includes the file name with the aggregated event. For example, a heartbeat includes 3 instances of the "Execution of Unrecognized Software Allowed" event for the Test_6_file.sh file, and no other instances of that event. Deep Security aggregates these 3 events for the file Test_6_file.sh.

- When the event occurs for many files, the log omits the rules link, path, file name, and user name. For example, a heartbeat includes 21 instances of the "Execution of Unrecognized Software Allowed" event that occurred for several different files. Deep Security aggregates the 21 events in a single event, but does not include a rules link, path, file name, or user name.

When aggregated events apply to multiple files, other occurrences of these events have likely been reported in other heartbeats. After you respond to other events where the file name is known, it is likely that no more aggregated events occur.

In the log, aggregated events use special icons, and the **Repeat Count** column indicates the number of events that are aggregated.



Period: Last 7 Days

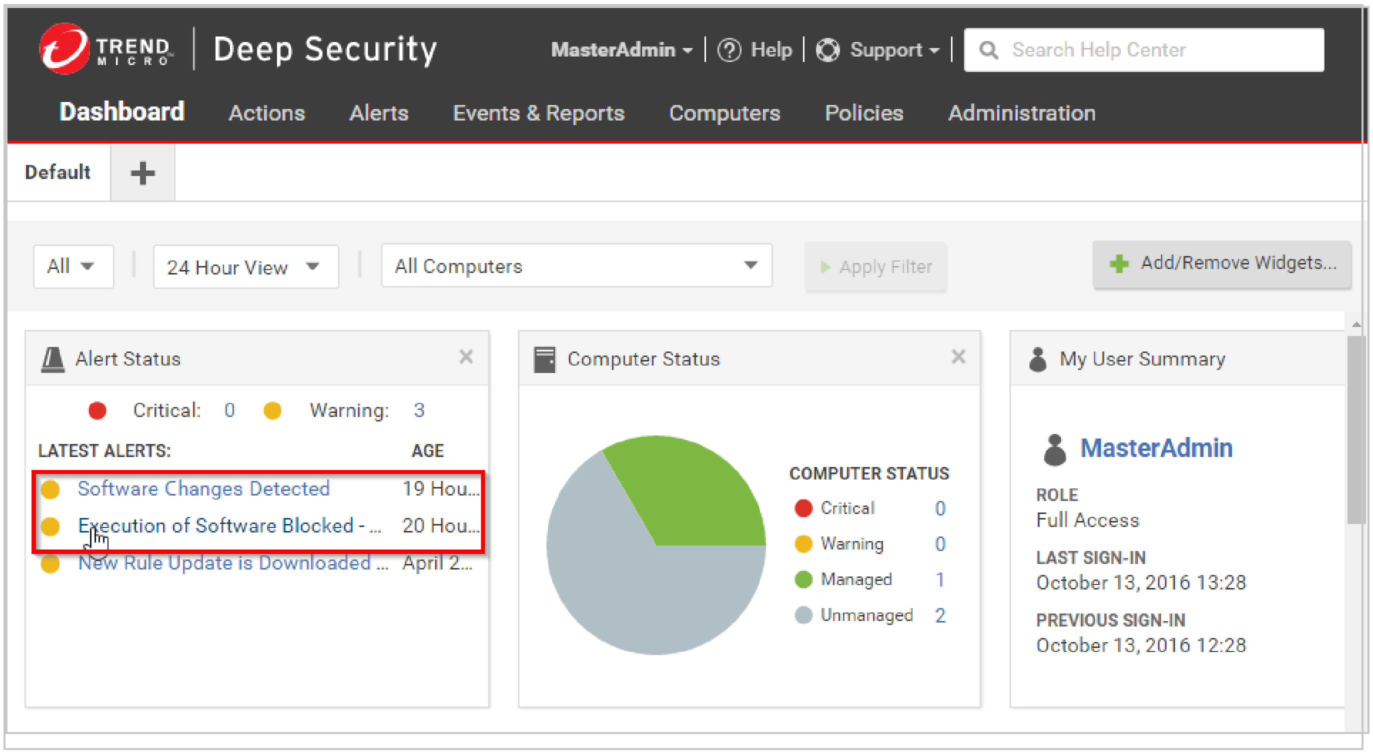
Computers: All Computers

| TIME | COMPUTER | EVENT | RULES | RULESET | REPEAT COUNT | ACTION | REASON | FILE |
|---|---|---|---|---|---|---|---|---|
| October 6, 2017 10:31:... | [redacted] | Execution of Unrecognized Software Allowed | Change rules... | None | 1 | Allowed | N/A | Test_4_file.sh |
| October 6, 2017 10:30:... | [redacted] | Execution of Unrecognized Software Allowed | Change rules... | None | 1 | Allowed | N/A | Test_3_file.sh |
| October 6, 2017 10:31:... | [redacted] | Execution of Unrecognized Software Allowed | Change rules... | None | 2 | Allowed | N/A | Test_1_file.sh |
| October 6, 2017 10:30:... | [redacted] | Execution of Unrecognized Software Allowed | Change rules... | None | 2 | Allowed | N/A | Test_9_file.sh |
| October 6, 2017 10:31:... | [redacted] | Execution of Unrecognized Software Allowed | Change rules... | None | 2 | Allowed | N/A | Test_5_file.sh |
| October 6, 2017 10:31:... | [redacted] | Execution of Unrecognized Software Allowed | Change rules... | None | 3 | Allowed | N/A | Test_6_file.sh |
| October 6, 2017 10:30:... | [redacted] | Execution of Unrecognized Software Allowed | Change rules... | None | 1 | Allowed | N/A | heartbeatSyn... |
| October 5, 2017 15:04:... | [redacted] | Execution of Unrecognized Software Allowed | Change rules... | None | 1 | Allowed | N/A | Test_7_file.sh |
| October 5, 2017 15:04:... | [redacted] | Execution of Unrecognized Software Allowed | Change rules... | None | 1 | Allowed | N/A | Test_3_file.sh |
| October 5, 2017 15:04:... | [redacted] | Execution of Unrecognized Software Allowed | Change rules... | None | 1 | Allowed | N/A | Test_5_file.sh |
| October 5, 2017 15:04:... | [redacted] | Execution of Unrecognized Software Allowed | Change rules... | None | 1 | Allowed | N/A | heartbeatSyn... |
| October 5, 2017 14:42:... | [redacted] | Execution of Unrecognized Software Allowed | N/A | None | 21 | Allowed | N/A | N/A |

## Monitor Application Control alerts

To configure which Application Control events or severity levels cause an alert, go to the **Alerts** tab, click the **Configure Alerts** button, and then select an event and double-click **Properties**. For details, see "Configure alerts" on page 1180.

When alerts are enabled for Application Control events, any software change that the Application Control engine detects and any software that it blocks from executing appear in the **Alerts** tab. If you have enabled the **Alert Status** widget, Application Control alerts also appear on the Dashboard.



Alert Status

Critical: 0 Warning: 3

| LATEST ALERTS: | AGE |
|---|---|
| Software Changes Detected | 19 Hou... |
| Execution of Software Blocked - ... | 20 Hou... |
| New Rule Update is Downloaded ... | April 2... |

Computer Status

| COMPUTER STATUS | |
|---|---|
| Critical | 0 |
| Warning | 0 |
| Managed | 1 |
| Unmanaged | 2 |

My User Summary

MasterAdmin

ROLE
Full Access

LAST SIGN-IN
October 13, 2016 13:28

PREVIOUS SIGN-IN
October 13, 2016 12:28

To monitor which computers are in maintenance mode, you can also click **Add/Remove Widgets** and enable the **Application Control Maintenance Mode** widget, which displays a list of the computers and their scheduled maintenance windows.

## View and change Application Control rulesets

Each computer has its own Application Control ruleset. You can:

- "View Application Control rulesets" on the next page and find out which rules they include.

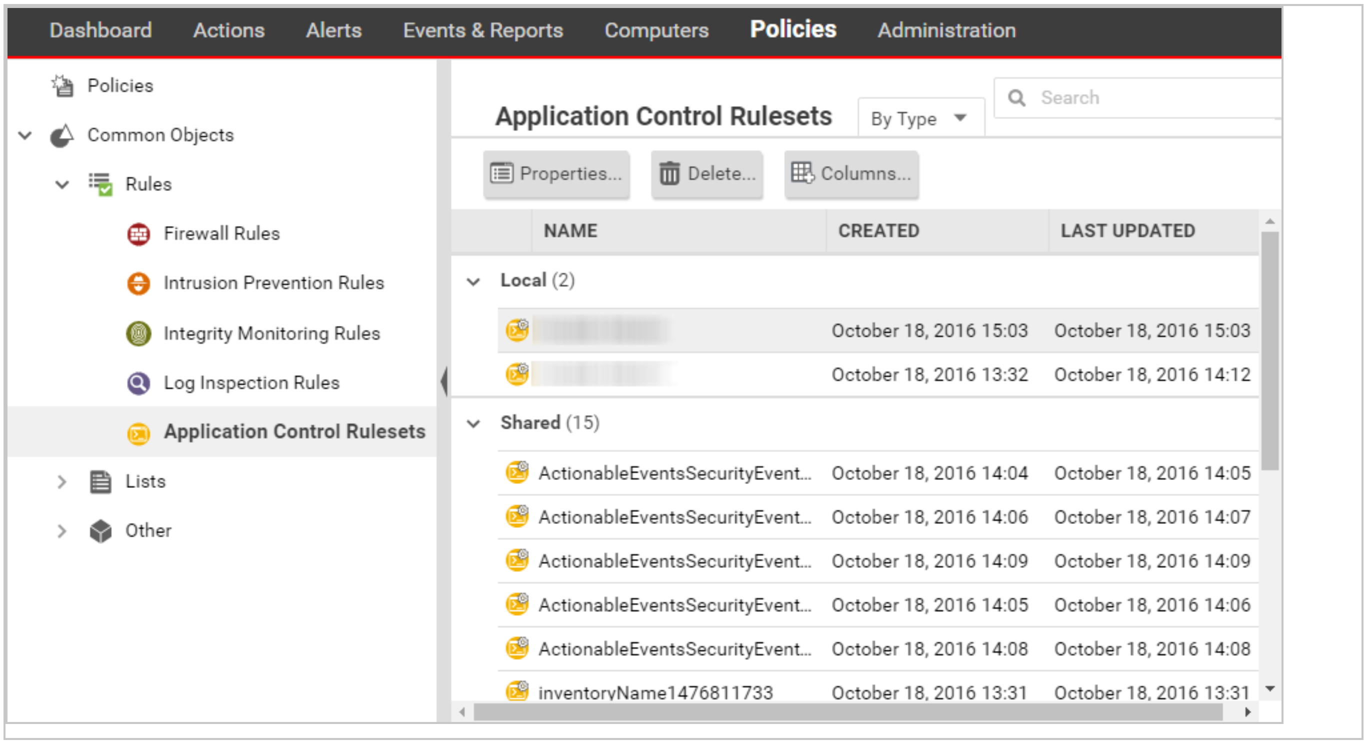
  Tip: When you first enable Application Control for a computer, the software installed on the computer is added to the computer's inventory and allowed to run. However, you cannot see the rules associated with the inventory from Deep Security Manager unless you use the Deep Security legacy REST API to do so (see "Use the API to create shared and global rulesets" on page 1040). In Deep Security Manager, a computer's ruleset appears empty until you create some allow/block rules for the computer.

- "Change the action for an Application Control rule" on the next page if a software file should no longer be allowed/blocked.
- "Delete an individual Application Control rule" on page 1010 if the software has been removed and isn't likely to return.
- "Delete an Application Control ruleset" on page 1011 if the computer associated with the ruleset has been removed.

Tip: If a user reports that Application Control is blocking software that they need to run on a particular computer, you can undo the block rule on that computer. Go to **Events & Reports > Application Control Events > Security Events**, find the computer, locate the block event, and then click **View Rules**. In the pop-up that appears, you can change the block rule to an allow rule.

## View Application Control rulesets

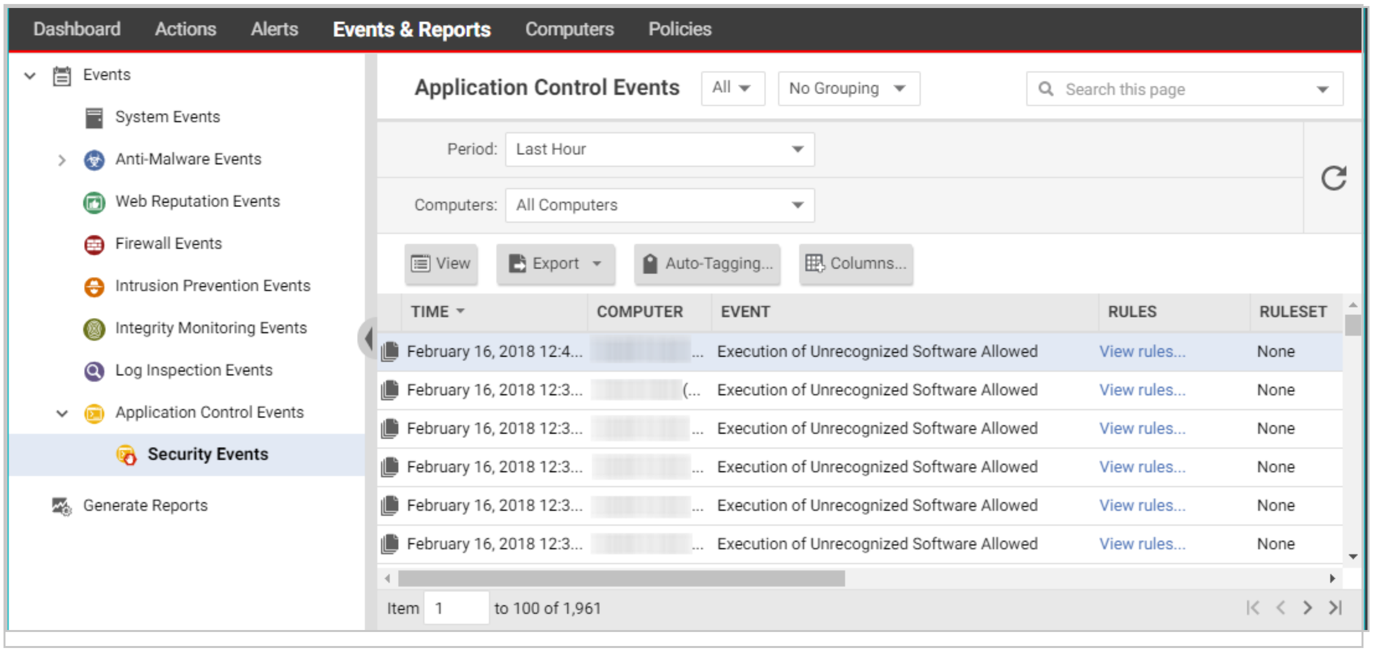
To view the list of Application Control rulesets, go to **Policies > Common Objects > Rules > Application Control Rulesets**.



| NAME | CREATED | LAST UPDATED |
|---|---|---|
| Local (2) | | |
| [redacted] | October 18, 2016 15:03 | October 18, 2016 15:03 |
| [redacted] | October 18, 2016 13:32 | October 18, 2016 14:12 |
| Shared (15) | | |
| ActionableEventsSecurityEvent... | October 18, 2016 14:04 | October 18, 2016 14:05 |
| ActionableEventsSecurityEvent... | October 18, 2016 14:06 | October 18, 2016 14:07 |
| ActionableEventsSecurityEvent... | October 18, 2016 14:09 | October 18, 2016 14:09 |
| ActionableEventsSecurityEvent... | October 18, 2016 14:05 | October 18, 2016 14:06 |
| ActionableEventsSecurityEvent... | October 18, 2016 14:08 | October 18, 2016 14:08 |
| inventoryName1476811733 | October 18, 2016 13:31 | October 18, 2016 13:31 |

To see which rules are part of a ruleset, double-click the ruleset and go to the **Rules** tab. The Rules tab displays the software files that have rules associated with them and enables you to change allow rules to block, and vice versa. (See "Change the action for an Application Control rule" below.)

### Security Events



Period: Last Hour

Computers: All Computers

| TIME | COMPUTER | EVENT | RULES | RULESET |
|---|---|---|---|---|
| February 16, 2018 12:4... | [redacted] ... | Execution of Unrecognized Software Allowed | View rules... | None |
| February 16, 2018 12:3... | [redacted] (... | Execution of Unrecognized Software Allowed | View rules... | None |
| February 16, 2018 12:3... | [redacted] ... | Execution of Unrecognized Software Allowed | View rules... | None |
| February 16, 2018 12:3... | [redacted] ... | Execution of Unrecognized Software Allowed | View rules... | None |
| February 16, 2018 12:3... | [redacted] ... | Execution of Unrecognized Software Allowed | View rules... | None |
| February 16, 2018 12:3... | [redacted] ... | Execution of Unrecognized Software Allowed | View rules... | None |

Item 1 to 100 of 1,961

**Events & Reports > Events > Application Control Events > Security Events** displays all unrecognized software that either was run on a computer or was actively blocked from running. You can filter this list by time period and other criteria. For more information, see "Application Control events" on page 1284.

For each event (except aggregated events), you can click **View rules** to change the rule from Allow to Block or vice versa.

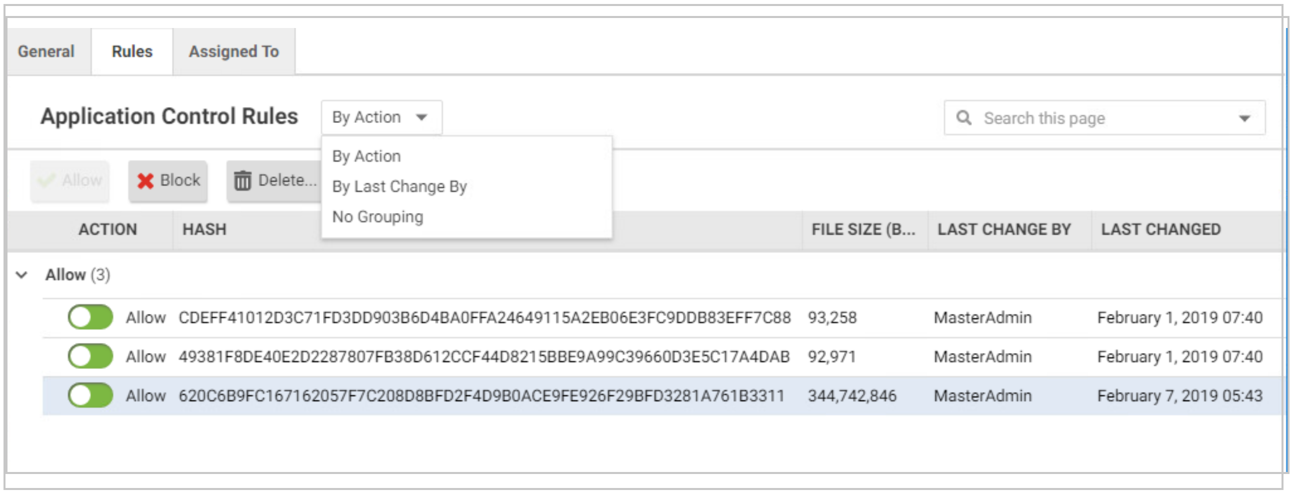
Deep Security Agent 10.2 or later includes event aggregation logic to reduce the volume of logs when the same event occurs repeatedly. (See "Interpret aggregated security events" on page 1005.)

## Change the action for an Application Control rule

If you want to allow a software that you previously blocked (or the opposite), you can edit the action in the rule. If you need to undo the rule so that the software is not recognized by Application Control (in other words, delete the rule, not only change its action), see "Delete an individual Application Control rule" on the next page instead.

1. Go to **Policies > Common Objects > Rules > Application Control Rulesets**.
2. Double-click to select the ruleset that contains the rule that you want to change.

3. On the pop-up window that appears, go to the **Rules** tab.
4. If you want to focus on software that was blocked (or allowed), then in the menu next to **Application Control Rules**, select **By Action** to group similar rules. Alternatively, you can use the search to filter the list.



| ACTION | HASH | FILE SIZE (B... | LAST CHANGE BY | LAST CHANGED |
|---|---|---|---|---|
| Allow (3) | | | | |
| Allow | CDEFF41012D3C71FD3DD903B6D4BA0FFA24649115A2EB06E3FC9DDB83EFF7C88 | 93,258 | MasterAdmin | February 1, 2019 07:40 |
| Allow | 49381F8DE40E2D2287807FB38D612CCF44D8215BBE9A99C39660D3E5C17A4DAB | 92,971 | MasterAdmin | February 1, 2019 07:40 |
| Allow | 620C6B9FC167162057F7C208D8BFD2F4D9B0ACE9FE926F29BFD3281A761B3311 | 344,742,846 | MasterAdmin | February 7, 2019 05:43 |

If you want to change the action for a software file, but it has multiple different file names , select **By File Name** to group related rules.

5. Find the row for the specific software that you want to allow or block.
6. In the **Action** column, change the setting to allow or block, then click **OK**.

   The next time that the agent connects with Deep Security Manager, the rule will be updated, and the version number will increase.

## Delete an individual Application Control rule

If you want to undo a rule that you created, go to **Policies > Common Objects > Rules > Application Control Rulesets**, double-click the ruleset that contains the rule, go to the **Rules** tab, select the rule and then click **Delete**.

Some things to keep in mind:

- When the rules are not needed anymore, you can delete them to reduce the size of the ruleset. This improves performance by reducing RAM and CPU usage.
- If you delete a rule, Application Control will not recognize the software anymore. If the software is installed again, it will appear again on the **Actions** tab.
- If a software update is unstable and you might need to downgrade, keep rules that allow rollback to the previous software version until you have completed testing.

- To find the oldest rules, go to **Policies > Rules > Application Control Rulesets**, then click **Columns**. Select **Date/Time (Last Change)**, click **OK**, and then click that column's header to sort by date.

### Delete an Application Control ruleset

If an Application Control ruleset is not being used anymore (for example, if the computer associated with the ruleset no longer exists), you can delete it.

To delete a ruleset, go to **Policies > Rules > Application Control Rulesets**, click a ruleset to select it, and click **Delete**.

## Application Control Trust Entities

Trust Entities auto-authorizes software changes that match the properties of "Trust rules" on page 1017 assigned to "Trust rulesets" on the next page. Each trust rule contains one or more "Types of trust rule properties" on page 1022 that define the parameters for auto-authorizing software changes.

By using the Trust Entities feature, you can proactively auto-authorize software changes on Deep Security Agent thus reducing the number of software change events sent to Deep Security Manager. For example, any agent undergoing regular OS updates creates several new software changes each time a patch is applied. By configuring appropriate trust rules and applying them to those agents, you can auto-authorize the software changes on the agent, and avoid having to manually manage them from the Deep Security Manager **Actions** tab or as Application Control security events.

To auto-authorize software changes using Trust Entities, you need to configure "Trust rules" on page 1017, assign them to "Trust rulesets" on the next page, and "Assign or unassign a trust ruleset" on page 1014 to policies or computers.

For information on how to allow or block software changes that are not being auto-authorized with the Trust Entities feature, see "View and change Application Control rulesets" on page 1007.

In this document, *source* refers to the process that creates a software change, whereas *target* is used when referring to the software change itself.

Tip: API documentation is available for trust rulesets.

Currently, some trust rule properties only apply to agents on supported Windows platforms and are not yet available on Linux. For details, see "Trust rule property limitations for Linux" on page 1038.

## Trust rulesets

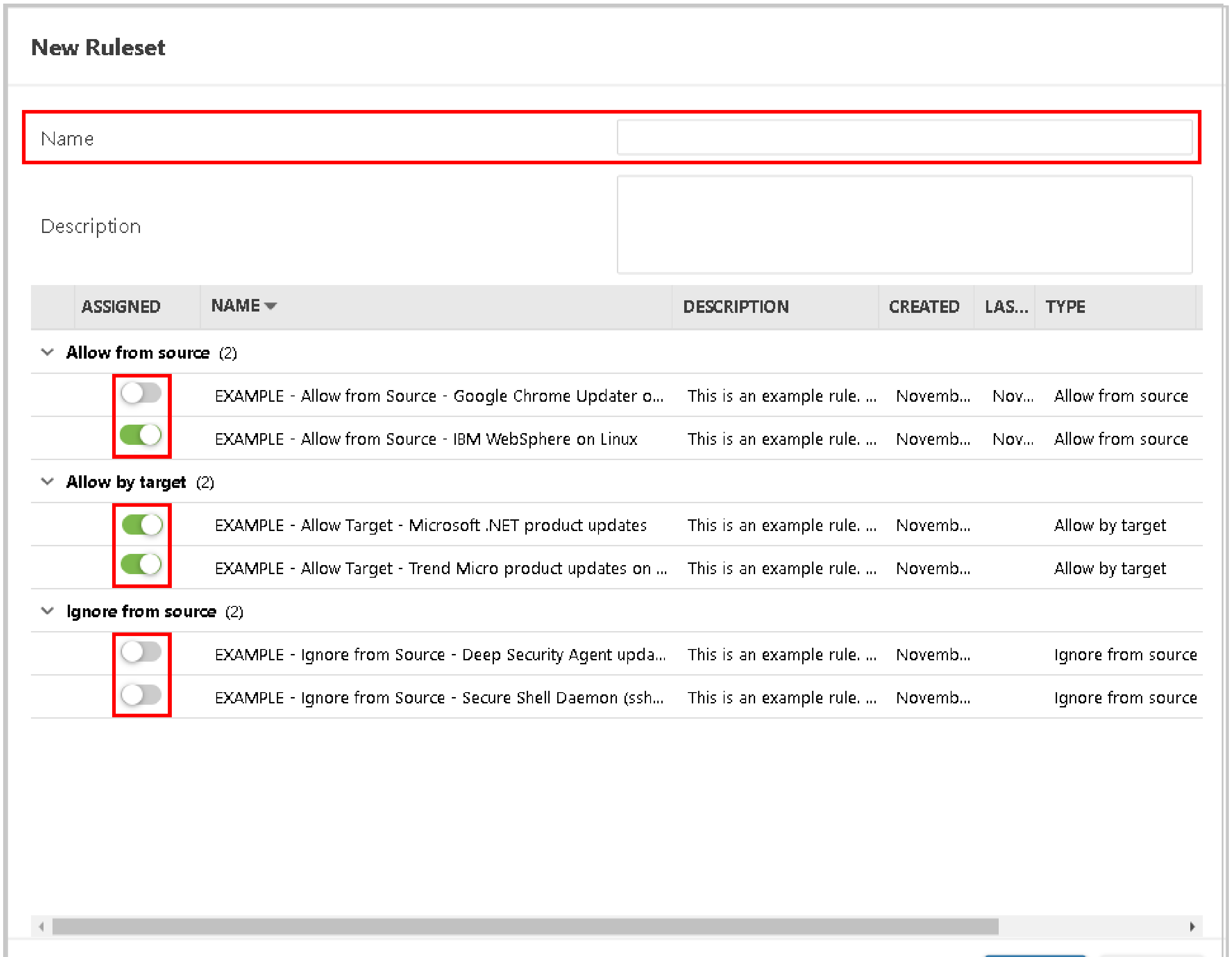
A trust ruleset consists of one or more user-configured "Trust rules" on page 1017. If you "Assign or unassign a trust ruleset" on page 1014 to a policy or computer in Deep Security Manager, the rules contained in that ruleset are applied to the related workloads and will auto-authorize any software changes that meet its rule property requirements.

### Create a trust ruleset

To create a new trust ruleset, do one of the following:

From the Deep Security Manager **Policies** tab:

1. Go to **Common Objects > Rules > Application Control Rules > Trust Entities**.
2. In the Trust Rulesets section, select **New**.
3. In the New Ruleset window, provide a name and (optionally) a description for the new ruleset.
4. Select one or more of the trust rules in the list to assign them to your trust ruleset.



**New Ruleset**

Name

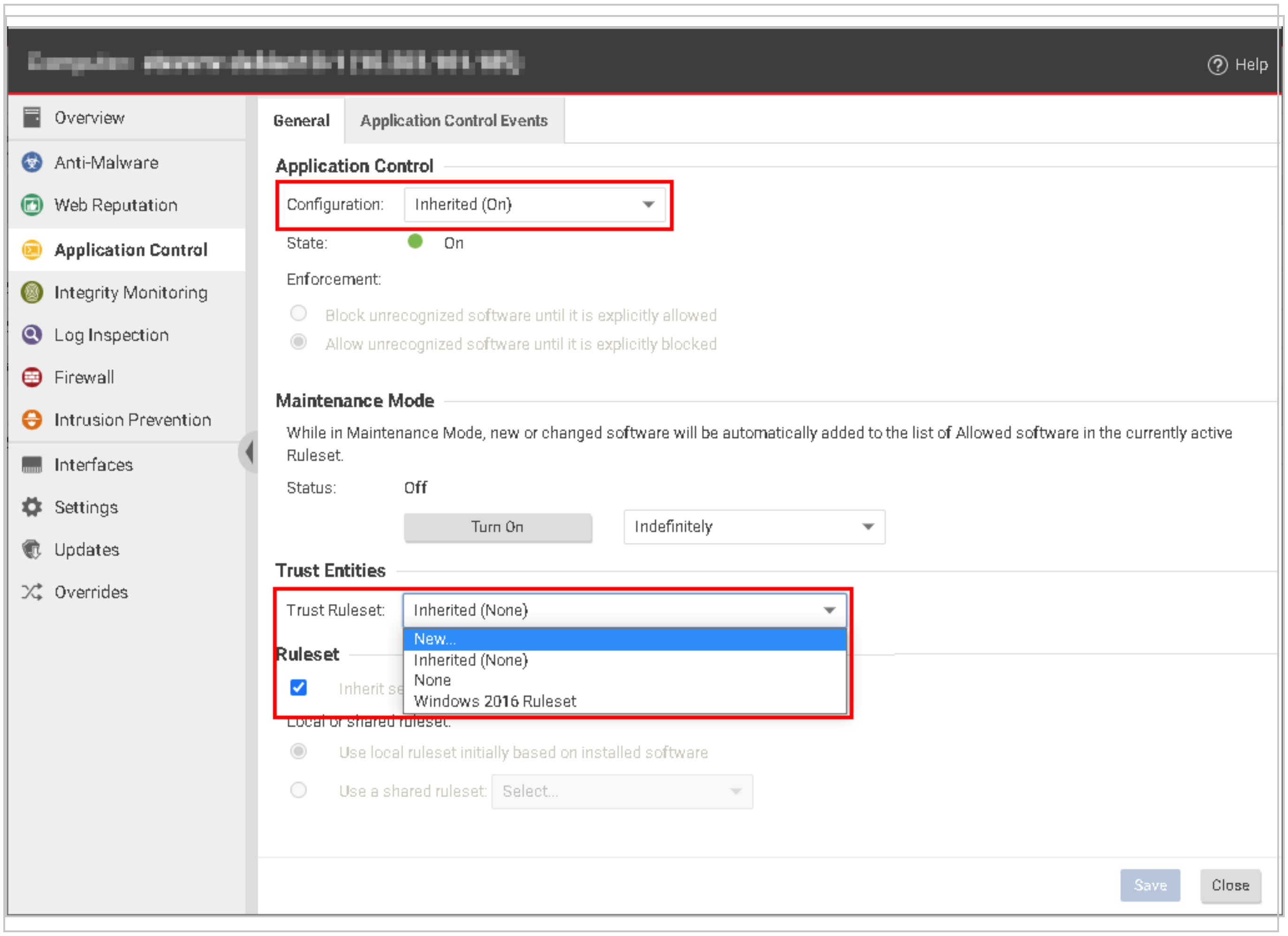
Description

| ASSIGNED | NAME ▾ | DESCRIPTION | CREATED | LAS... | TYPE |
|---|---|---|---|---|---|
| **Allow from source** (2) | | | | | |
| ○ | EXAMPLE - Allow from Source - Google Chrome Updater o... | This is an example rule. ... | Novemb... | Nov... | Allow from source |
| ● | EXAMPLE - Allow from Source - IBM WebSphere on Linux | This is an example rule. ... | Novemb... | Nov... | Allow from source |
| **Allow by target** (2) | | | | | |
| ● | EXAMPLE - Allow Target - Microsoft .NET product updates | This is an example rule. ... | Novemb... | | Allow by target |
| ● | EXAMPLE - Allow Target - Trend Micro product updates on ... | This is an example rule. ... | Novemb... | | Allow by target |
| **Ignore from source** (2) | | | | | |
| ○ | EXAMPLE - Ignore from Source - Deep Security Agent upda... | This is an example rule. ... | Novemb... | | Ignore from source |
| ○ | EXAMPLE - Ignore from Source - Secure Shell Daemon (ssh... | This is an example rule. ... | Novemb... | | Ignore from source |

The trust ruleset is created, containing any rules you assigned.

From the Deep Security Manager **Computers** or **Policies** tab:

1. Double-click a computer or policy (or right-click and select **Details**).
2. Go to **Application Control** and make sure the Configuration is set to On or Inherited (On).
3. In the **Trust Ruleset** dropdown list, select **New**.



[redacted]

Application Control

Configuration: Inherited (On)

State: On

Enforcement:

○ Block unrecognized software until it is explicitly allowed

● Allow unrecognized software until it is explicitly blocked

Maintenance Mode

While in Maintenance Mode, new or changed software will be automatically added to the list of Allowed software in the currently active Ruleset.

Status: Off

Indefinitely

Trust Entities

Trust Ruleset: Inherited (None)

New...
Inherited (None)
None
Windows 2016 Ruleset

Ruleset

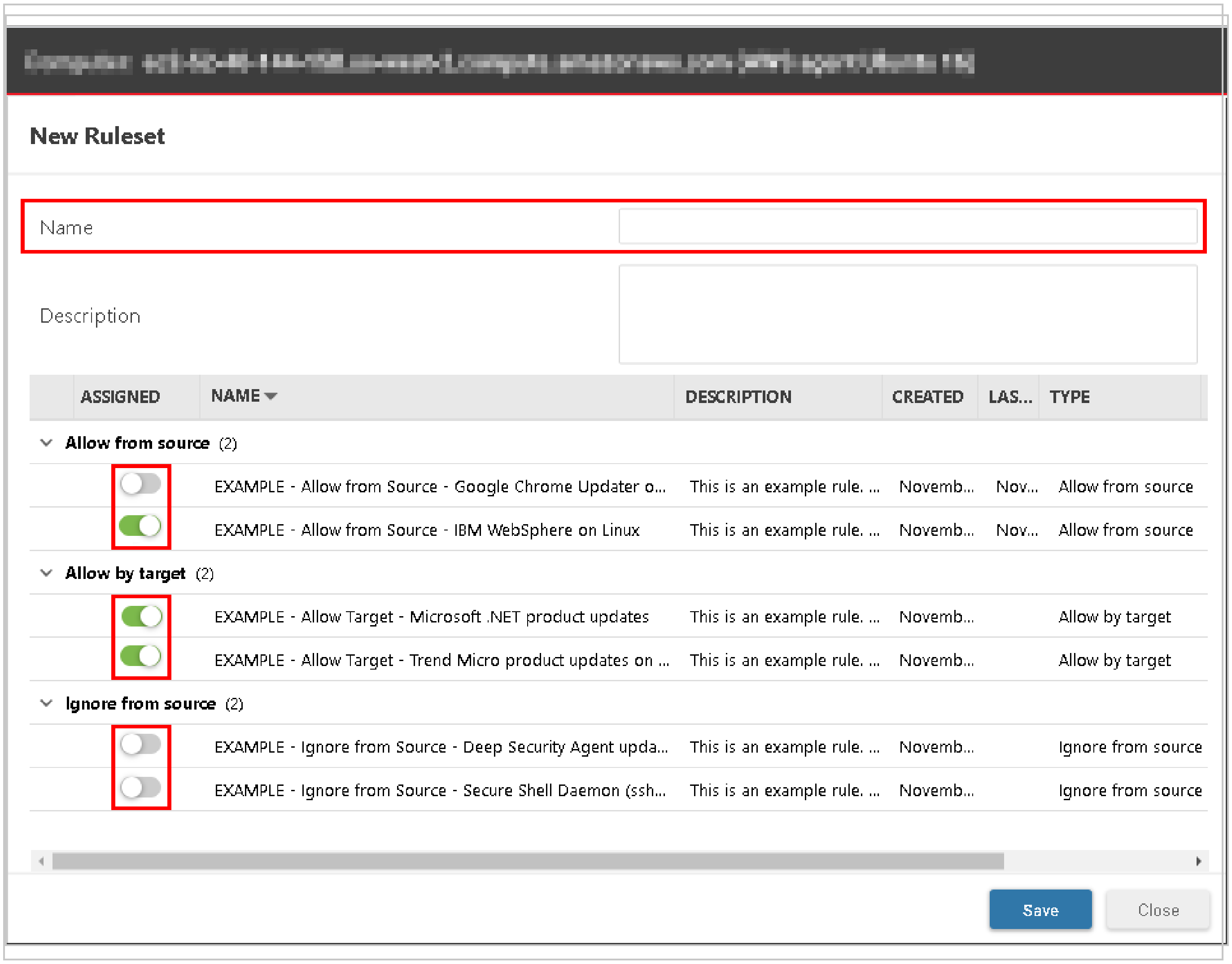
☑ Inherit se

Local or shared ruleset:

● Use local ruleset initially based on installed software

○ Use a shared ruleset: Select...

4. In the New Ruleset window, provide a name and (optionally) a description for the new ruleset.



[redacted]

New Ruleset

Name

Description

|  | ASSIGNED | NAME ▾ | DESCRIPTION | CREATED | LAS... | TYPE |
|---|---|---|---|---|---|---|
| ⌄ Allow from source (2) |  |  |  |  |  |  |
|  | ○ | EXAMPLE - Allow from Source - Google Chrome Updater o... | This is an example rule. ... | Novemb... | Nov... | Allow from source |
|  | ● | EXAMPLE - Allow from Source - IBM WebSphere on Linux | This is an example rule. ... | Novemb... | Nov... | Allow from source |
| ⌄ Allow by target (2) |  |  |  |  |  |  |
|  | ● | EXAMPLE - Allow Target - Microsoft .NET product updates | This is an example rule. ... | Novemb... |  | Allow by target |
|  | ● | EXAMPLE - Allow Target - Trend Micro product updates on ... | This is an example rule. ... | Novemb... |  | Allow by target |
| ⌄ Ignore from source (2) |  |  |  |  |  |  |
|  | ○ | EXAMPLE - Ignore from Source - Deep Security Agent upda... | This is an example rule. ... | Novemb... |  | Ignore from source |
|  | ○ | EXAMPLE - Ignore from Source - Secure Shell Daemon (ssh... | This is an example rule. ... | Novemb... |  | Ignore from source |

5. Select one or more of the trust rules in the list to assign them to your trust ruleset and select **Save** to create the trust ruleset, containing any rules you assigned.

6. (Optional) To assign the new trust ruleset to the computer or policy, select **Save**.

> **Tip:** Instead of creating a trust ruleset from scratch, you can use the **Duplicate** button from the Trust Entity Management window (**Policies > Common Objects > Rules > Application Control Rules > Trust Entities**) to create a copy of an existing ruleset and then configure it to meet your needs.

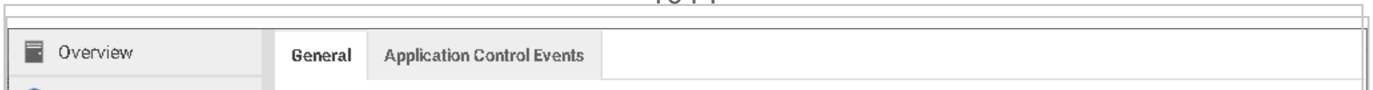
### Assign or unassign a trust ruleset

To assign a trust ruleset:

1. From the Deep Security Manager **Computers** or **Policies** tab, double-click a computer or policy (or right-click and select **Details**).

2. Go to **Application Control** and make sure **Configuration** is set to On or Inherited (On).

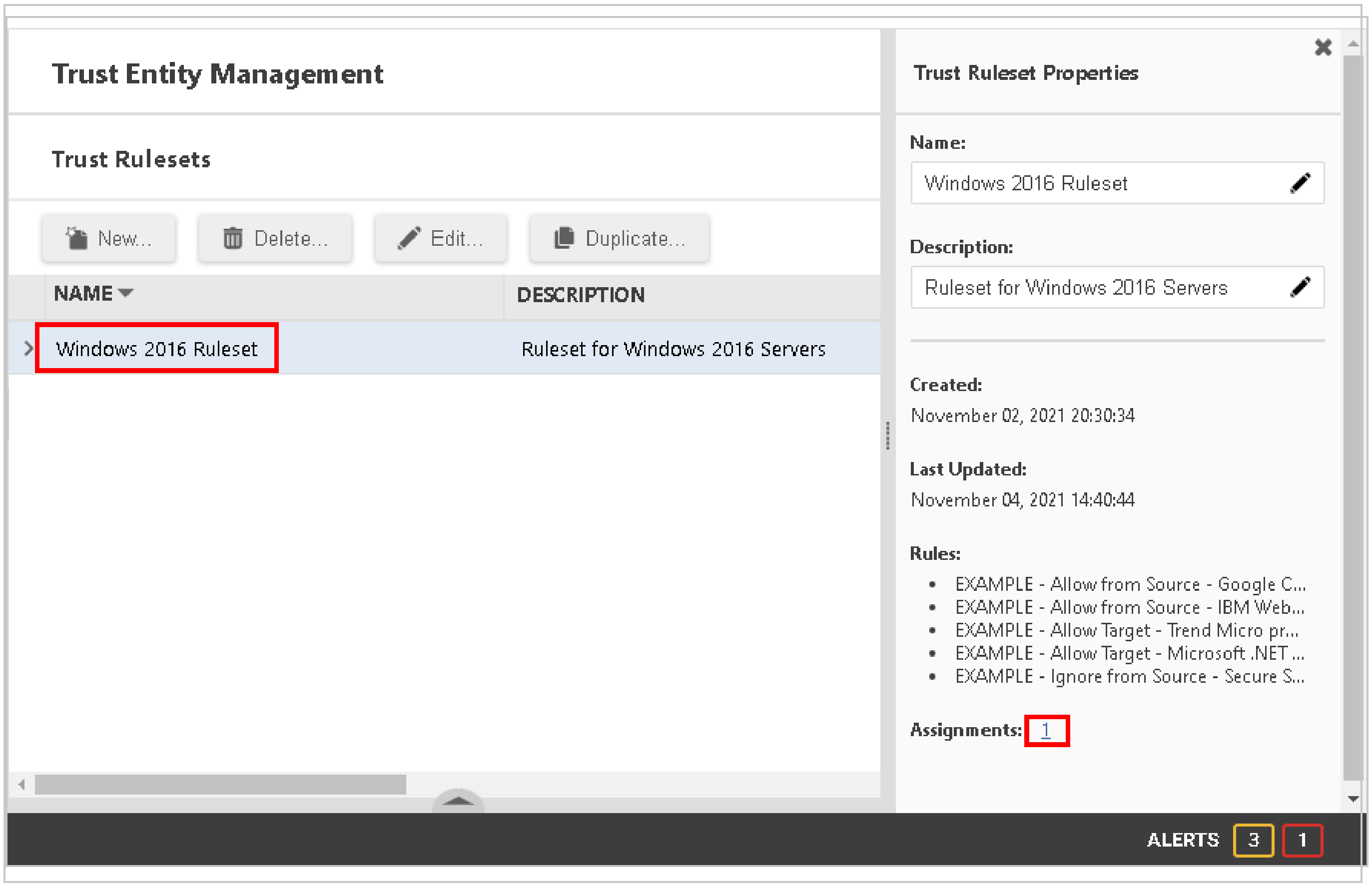
3. Select a **Trust Ruleset** from the dropdown list.



The trust ruleset you selected is now assigned to the computer or policy.

To unassign a trust ruleset:

1. Go to **Common Objects > Rules > Application Control Rules > Trust Entities** and select the trust ruleset.
2. In the Trust Ruleset Properties window displayed on the right, select the number next to Assignments.



Trust Entity Management

Trust Rulesets

| NAME | DESCRIPTION |
|---|---|
| Windows 2016 Ruleset | Ruleset for Windows 2016 Servers |

Trust Ruleset Properties

Name: Windows 2016 Ruleset

Description: Ruleset for Windows 2016 Servers

Created: November 02, 2021 20:30:34

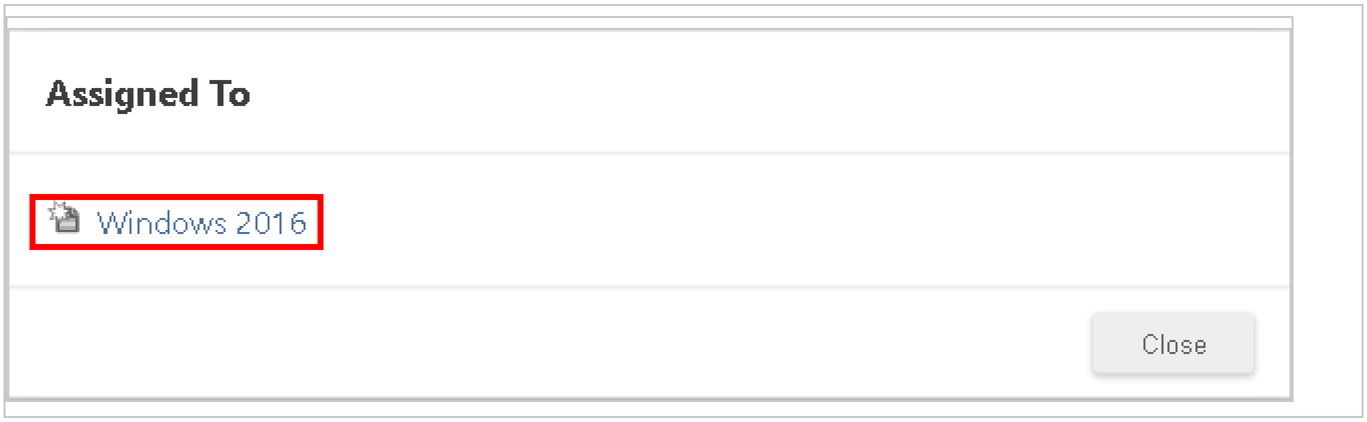
Last Updated: November 04, 2021 14:40:44

Rules:

- EXAMPLE - Allow from Source - Google C...
- EXAMPLE - Allow from Source - IBM Web...
- EXAMPLE - Allow Target - Trend Micro pr...
- EXAMPLE - Allow Target - Microsoft .NET ...
- EXAMPLE - Ignore from Source - Secure S...

Assignments: 1

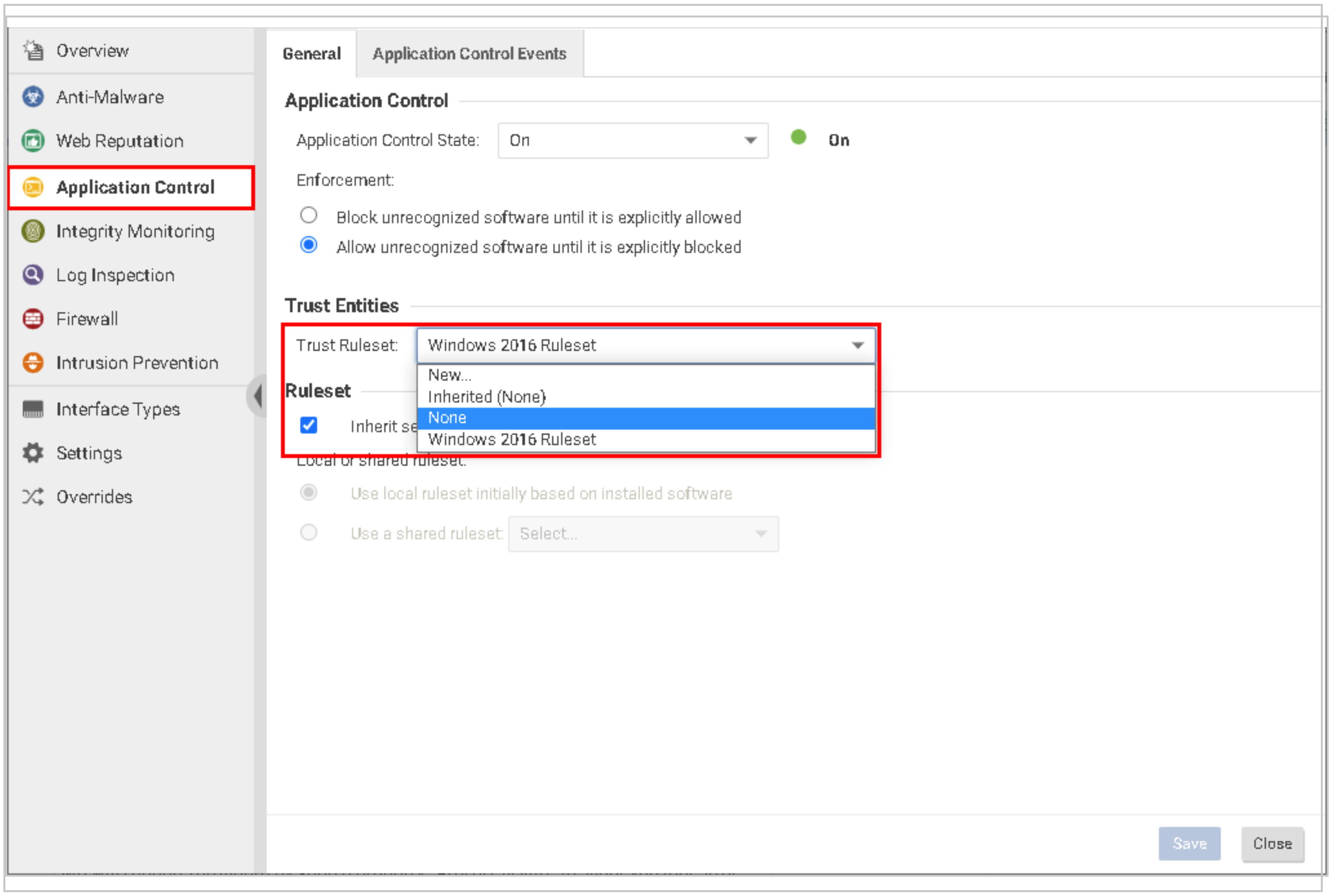
3. In the Assigned To window, select a computer or policy.



Assigned To

Windows 2016

4. From the **Application Control** tab of the computer or policy window, unassign the ruleset by selecting None from the Trust Ruleset dropdown list.



Application Control

Application Control State: On ● On

Enforcement:

○ Block unrecognized software until it is explicitly allowed

● Allow unrecognized software until it is explicitly blocked

Trust Entities

Trust Ruleset: Windows 2016 Ruleset

New...
Inherited (None)
None
Windows 2016 Ruleset

Ruleset

☑ Inherit se

Local or shared ruleset:

● Use local ruleset initially based on installed software

○ Use a shared ruleset: Select...

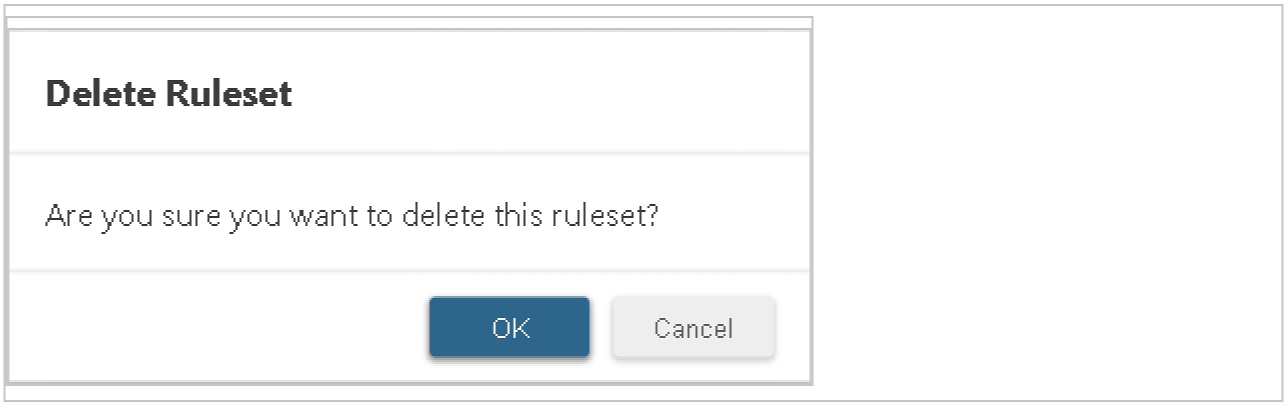
5. Select **Save**.

The trust ruleset is no longer assigned to the computer or policy.

### Delete a trust ruleset

1. Go to **Common Objects > Rules > Application Control Rules > Trust Entities**.
2. In the Trust Rulesets section, select the ruleset you want to delete and select **Delete**.

3. From the Delete Ruleset confirmation window, select **OK**.



Delete Ruleset

Are you sure you want to delete this ruleset?

The trust ruleset is deleted.

Note that you cannot delete a trust ruleset if it is currently inherited by or assigned to a computer or policy. You must "Assign or unassign a trust ruleset" on page 1014 before it can be deleted.

## Trust rules

A trust rule contains one or more properties that determine which software changes are auto-authorized by Application Control. Software changes that match the properties of a trust rule are auto-authorized and will not create events in Deep Security Manager.

> Warning: Any empty trust rule properties are treated as wildcards. While this gives you freedom in how you customize trust rules, it could also impact the security of your system. To maximize system security and prevent any unwanted software changes from being authorized, try to fill in as many properties as possible when creating trust rules. If you are unsure of the security impact a trust rule might have, check with someone who has a good knowledge of system security or contact Trend Micro before adding it to a trust ruleset.

### Types of trust rules

- **Allow from source** rule permits a trusted updater or installer process to install new software on the system. Authorized executable files created by the trusted updater are automatically approved. To use this rule, you need to specify the properties of the source, such as a process or installer, in the rule. In addition, you need to restrict the process to only creating authorized software in specified directories using the "Paths" on page 1023 attribute. Applying this rule minimizes software change events on the **Actions** page. The Allow from source rule is evaluated during software creation and must be in place prior to running the installer.

- **Allow by target** rule permits an executable file to run if it matches the specified properties. The properties you specify in the rule must match the properties of the target, such as an executable file. This rule is evaluated at the time of execution, therefore it can be applied after a security event is detected for the file on the **Alerts** page.
- **Block by target** rule prevents an executable file from running if it matches the specified properties. The properties you specify in the rule must match the properties of the target, such as an executable file. This rule is evaluated at the time of execution, therefore it can be applied after a security event is detected for the file on the **Alerts** page.

  > **Note:** Block by target rules are supported for Deep Security Agent 20.0.0-3288 or later.

- **Ignore from source** rule sets up a process exclusion, enabling the specified process to execute or create software in designated directories without being monitored by Application Control. When the exclusion rule is removed, the exclusion is immediately lifted. If you only specify the paths with Ignore by source rules, any process can execute or create software in those directories without being monitored by Application Control. This option should only be used if Application Control scanning is causing compatibility problems (for example, performance issues or sharing violations) with some of the processes or paths. The Ignore from source rule overrides any global rules created using the Workload Security API. For more information on global rules, see "Use the API to create shared and global rulesets" on page 1040.

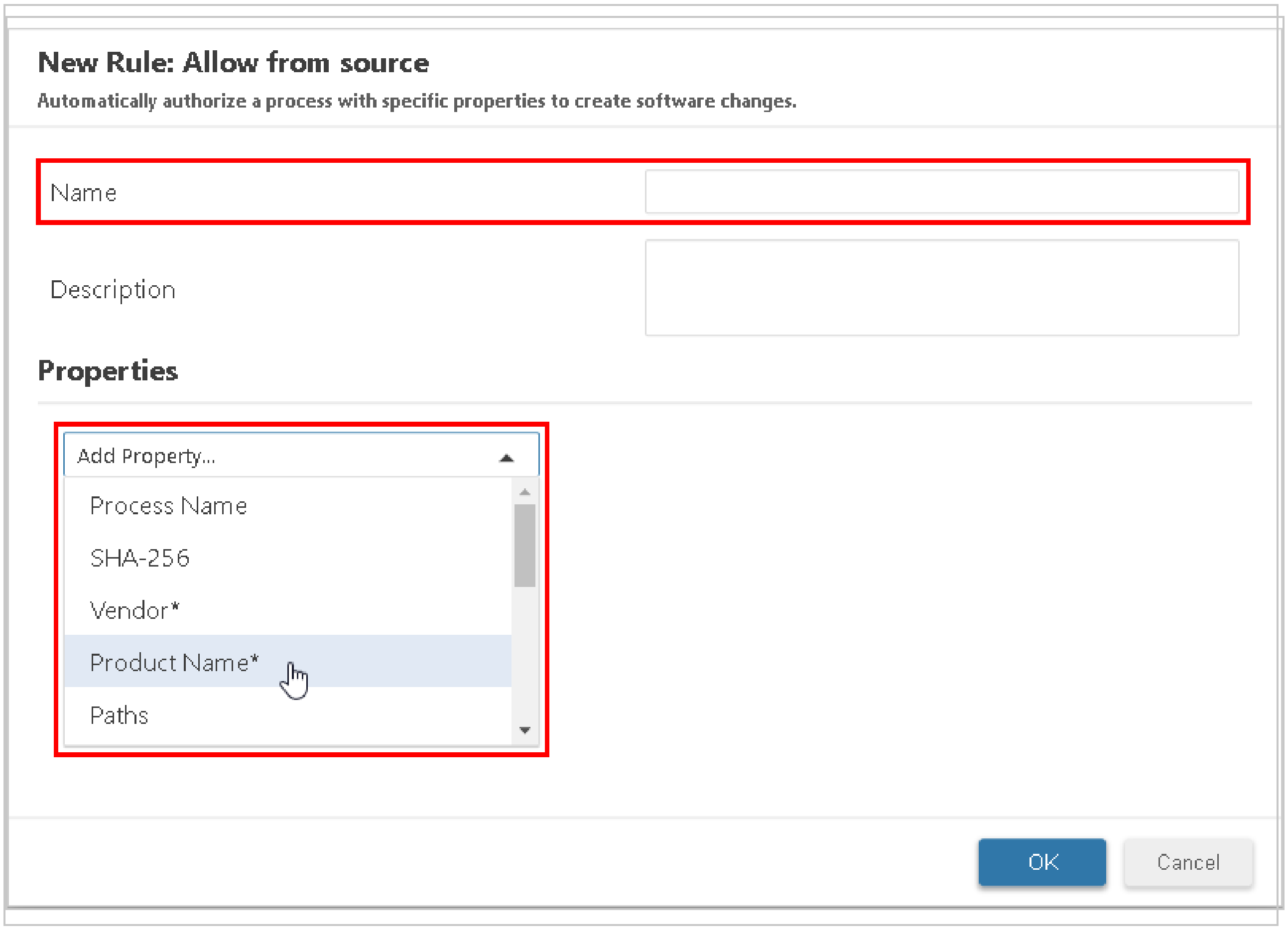
Every time an Allow from source rule auto-authorizes a software change, an entry is added to the local inventory of the agent where the change occurred. This does not occur for Ignore from source rules.

> **Warning:** When used in an Ignore by source rule, the "Process Name" on page 1023 property is only supported for for Deep Security Agent 20.0.0-3165 or later.

### Create a trust rule

1. Go to **Common Objects > Rules > Application Control Rules > Trust Entities**.
2. In the Trust Rules section, select **New** and select one of the "Types of trust rules" on the previous page from the dropdown list.
3. In the New Rule window, provide a name and (optionally) a description for the new rule.

4. Select a property from the Add Property dropdown list to add it to the new rule.



**New Rule: Allow from source**

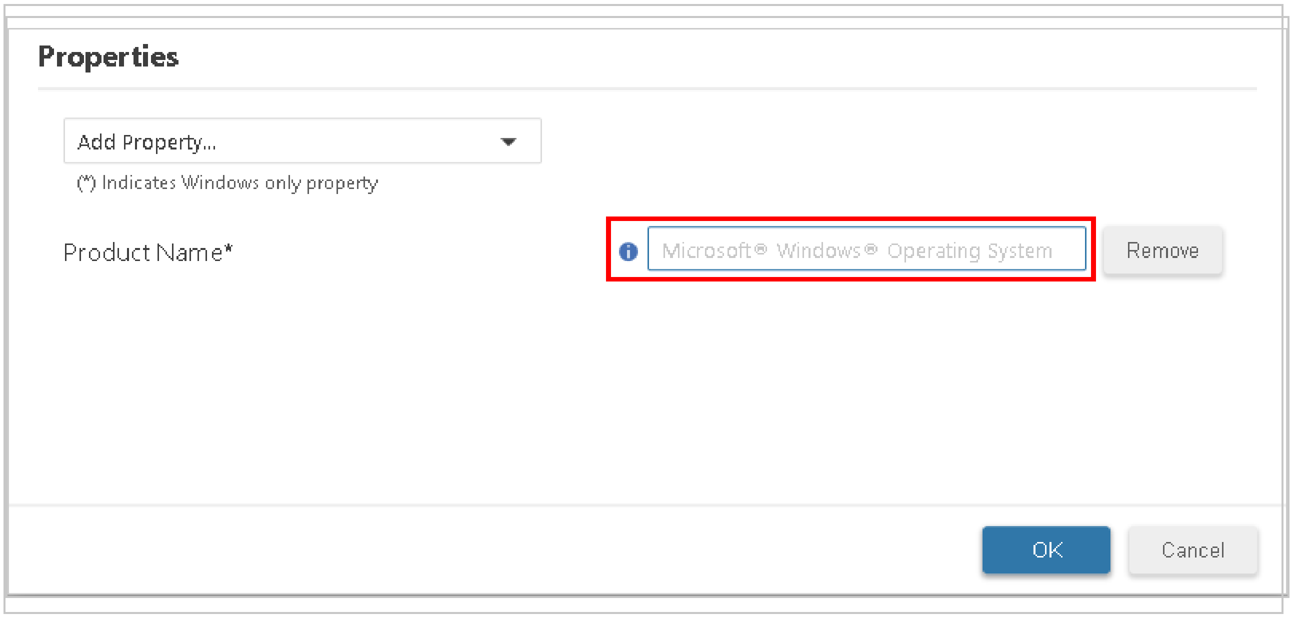
Automatically authorize a process with specific properties to create software changes.

Name

Description

**Properties**

5. Type the value for the property in the box provided.


Properties
Add Property...
(*) Indicates Windows only property
Product Name*
Microsoft® Windows® Operating System
Remove
OK
Cancel

6. (Optional) To add more properties to this trust rule, repeat steps 4 and 5.
7. Click **OK**.

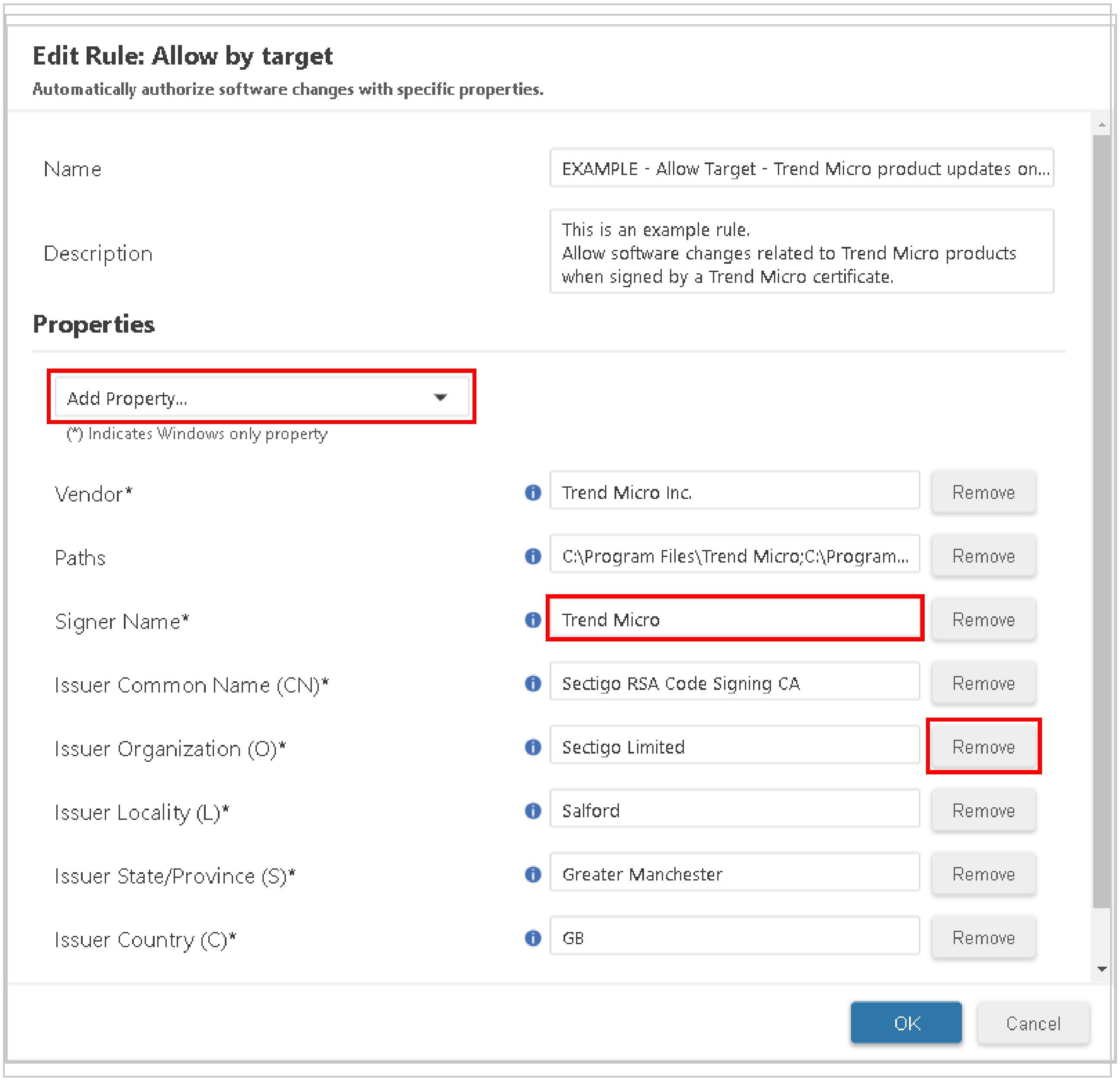
The new trust rule is created and ready to assign to a trust ruleset.

Tip: For help configuring trust rule property values, see "Types of trust rule properties" on page 1022.

Tip: Select a trust rule (from **Policies > Common Objects > Rules > Application Control Rules > Trust Entities**) and use **Assign/Unassign** to choose which trust rulesets to include it in. This can be especially useful if you want to quickly assign or unassign a new rule across many rulesets.

### Change trust rule properties

1. From the Deep Security Manager **Trust Entities** tab (**Policies > Common Objects > Rules > Application Control Rules > Trust Entities**), select a rule and select **Edit** (or double-click a rule).



**Edit Rule: Allow by target**

Automatically authorize software changes with specific properties.

| | |
|---|---|
| Name | EXAMPLE - Allow Target - Trend Micro product updates on... |
| Description | This is an example rule.<br>Allow software changes related to Trend Micro products when signed by a Trend Micro certificate. |

**Properties**

Add Property...

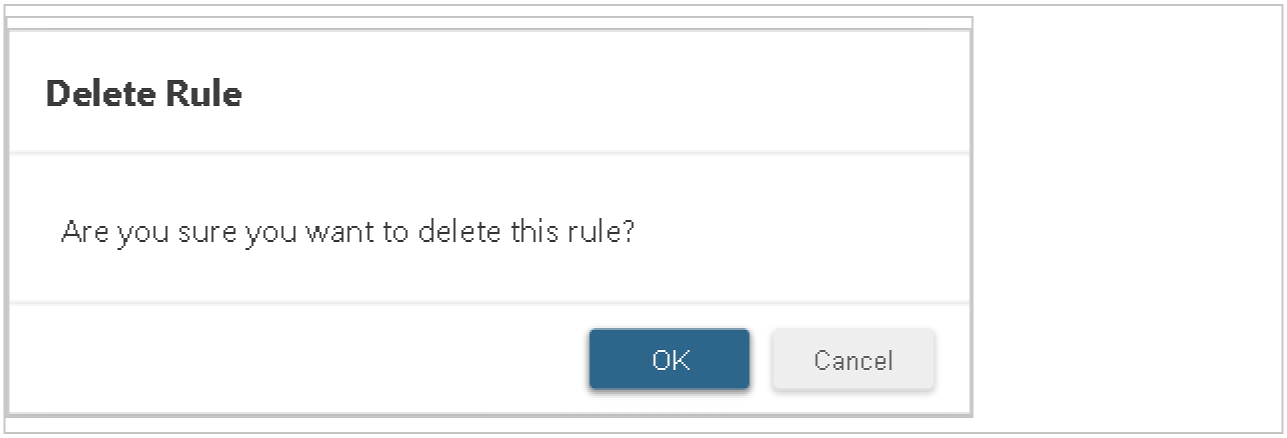
(*) Indicates Windows only property

| | |
|---|---|
| Vendor* | Trend Micro Inc. |
| Paths | C:\Program Files\Trend Micro;C:\Program... |
| Signer Name* | Trend Micro |
| Issuer Common Name (CN)* | Sectigo RSA Code Signing CA |
| Issuer Organization (O)* | Sectigo Limited |
| Issuer Locality (L)* | Salford |
| Issuer State/Province (S)* | Greater Manchester |
| Issuer Country (C)* | GB |

2. In the Edit Rule window, do one of the following:
   - To add a new property, select one from the **Add Property** dropdown list and fill in its value.
   - To edit an existing property, change the value in its text field.
   - To remove an existing property, select **Remove**.
3. Click **OK**.

### Delete a trust rule

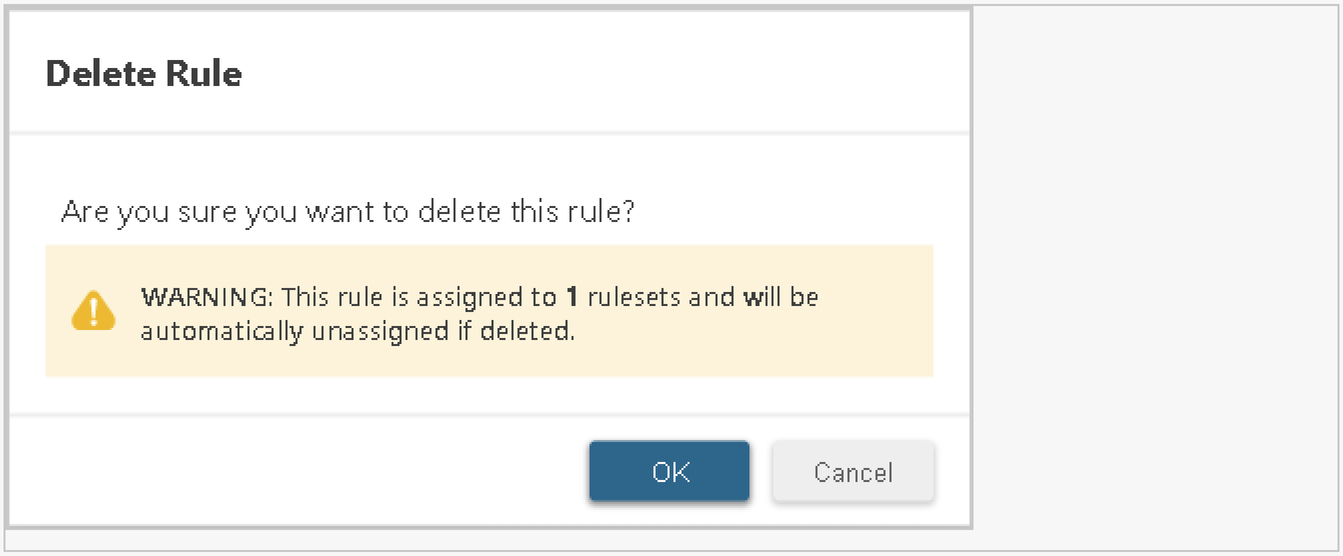
1. From the Deep Security Manager **Trust Entities** tab (**Policies > Common Objects > Rules > Application Control Rules > Trust Entities**), select a rule and select **Delete**.
2. Click **OK** to confirm the deletion.



Delete Rule

Are you sure you want to delete this rule?

**Note:** If you delete a trust rule that is currently assigned to any trust rulesets, it will automatically be unassigned from them following a warning prompt



Delete Rule

Are you sure you want to delete this rule?

WARNING: This rule is assigned to **1** rulesets and will be automatically unassigned if deleted.

## Types of trust rule properties

The properties and values included in a trust rule define which software changes are auto-authorized by that rule. The following sections detail the trust rule property types you can use to configure trust rules, including steps to help you find the information required to configure the property values.

### Process Name

> **Warning:** When used in an "Types of trust rules" on page 1017 rule, the process name property is only supported for Deep Security Agent 20.0.0-3165 or later.

This property specifies the name of the process creating software changes. The process name must use the absolute path of the process, including its file name.

To find a process name of a software change:

1. Go to Deep Security Manager's **Actions** tab.
2. Find and select the software change.

The process displays on the right under Changed By Process along with other details.

Deep Security Agent uses wildcards for process names. When a process name includes the full path to the process:
- the globstar `**` in a path matches any number of additional characters within the process name;
- the globstar `**` matches any number of additional characters within the process name; - a single asterisk or star `*` matches any number of additional characters with the current directory only; - a `?` matches a single character.

The `*` character stops its search at directory path delimiters (`/` and `\`). The `?` character does not match match directory path delimiters. Drive letters are treated like any other characters in the target path and hold no special significance for matching.

### Paths

This property specifies the target paths applied to a trust rule. Application Control automatically authorizes software changes if they occur within a path entered for this property, including all subdirectories and file names. You can set multiple paths separated by a semicolon. For example, `C:\Windows\;C:\Program Files\`.

When entering values for paths, consider how the last slash (`\` or `/`) in a path affects which directories are included:

- A path ending with a slash matches all subdirectories under that full path. For example, `C:\Windows\System\` would match any subdirectories in the `System` directory.

- A value specified after the last slash is treated as a regular expression wild card and matches the specific directory, as well as any other directories that start with the same value. For example, `C:\Windows\System` would include all directories and subdirectories that match "C:\Windows\System*" including `C:\Windows\System\`, `C:\Windows\System32\`, `C:\Windows\SystemApps\`, and so on.

Deep Security Agent version 20.0.0-5137 and later supports globstar (`**`) wildcard. Using globstar `**` in a path matches any number of additional characters within the current directory and its subdirectories, a single asterisk (`*`) matches any number of additional characters within the current directory only, and a question mark (`?`) matches a single additional character. Drive letters or drive delimiters (`/` or `\`) are treated like any other characters in the target path and hold no special significance for matching, except for `*` which stops at forward slash (`/`) or back slash (`\`) characters.

### SHA-256

When used in an Allow from source rule, this specifies the checksum (SHA-256) of the source process creating a software change. When used in an Allow by target rule, it is the checksum (SHA-256) of the software change itself.

To find the SHA256, do one of the following:

**From Windows PowerShell (for source or target)**:

Follow instructions in the Windows PowerShell command Get-FileHash.

**From Deep Security Manager (for target only)**:

From Deep Security Manager's **Actions** tab, find and select the software change.

The SHA256 will be displayed on the right along under SHA256 along with other details.

### Vendor

This property, which is currently supported only on Windows, specifies the software vendor.

To find the vendor, do one of the following:

**From File Explorer**:

1. From the directory containing the process or file, right-click on one of the properties displayed at the top of File Explorer (Name, Date modified, etc.) and select **More**.
2. Select **Company** and click **OK**.

   The vendor will be displayed in the File Explorer window.

**From Deep Security Manager**:

From Deep Security Manager's **Actions** tab, find and select the software change.

The vendor will be displayed on the right under Vendor along with other details.

**Product Name**

This property, which is currently supported only on Windows, specifies the software product name.

To find the product name, do one of the following:

**From file properties**:

1. From the directory containing the file, right-click the process or file and select **Properties**.
2. From the **Details** tab, look at the value for Product Name.

**From File Explorer**:

1. From the directory containing the file, right-click on one of the properties displayed at the top of File Explorer (Name, Date modified, etc) and click **More**.
2. Select **Product name** and click **OK**.

The product name will be displayed in the **Product name** column.

**From Deep Security Manager**:

From Deep Security Manager's **Actions** tab, find and select the software change.

The product name will be displayed on the right under Product Name along with other details.

**Signer Name**

When used in an Allow from source rule, this specifies the signer name of the source process creating a software change. When used in an Allow by target rule, it is the signer name in the certificate that signed the target file.

This property, which is currently supported on Windows only, specifies the name of the company that signed the software certificate.

To find the certificate signer name:

1. Right-click the process or file and select **Properties**.
2. On the **Digital Signatures** tab, find the name of the signer in **Signature list**.

The signer name is displayed under **Signer Name**

To eliminate the maximum amount of software change events or security events, use the signer name rule property to match all events from a specific signer.

#### Issuer Common Name

This property, which is currently supported only on Windows, specifies the issuer common name (CN) of the signing software certificate.

To find the issuer common name:

1. Right-click the process or file and click **Properties**.
2. From the **Digital Signatures** tab, select the first certificate you see on the **Signature** list.
3. Select the certificate and click **Details**.
4. Select **View Certificate**.
5. Go to the **Details** tab and select **Issuer**.

If included in the certificate, the issuer CN is displayed under Issuer.

#### Issuer Organizational Unit

This property, which is currently supported only on Windows, specifies the issuer organizational unit (OU) of the software certificate.

To find the issuer organizational unit:

1. Right-click the process or file and select **Properties**.
2. From the **Digital Signatures** tab, select the first certificate you see on the signature list.
3. Select the certificate and click **Details**.
4. Click **View Certificate**.
5. Go to the **Details** tab and select **Issuer**.

If included in the certificate, the issuer OU is displayed.

#### Issuer Organization

This property, which is currently supported only on Windows, specifies the issuer organization (O) of the software certificate.

To find the issuer organization:

1. Right-click the process or file and click **Properties**.
2. From the **Digital Signatures** tab, select the first certificate you see on the signature list.
3. Select the certificate and click **Details**.
4. Click **View Certificate**.
5. Go to the **Details** tab and select **Issuer**.

If included in the certificate, the issuer O is displayed.

### Issuer Locality

This property, which is currently supported only on Windows, specifies the issuer locality (L) of the software certificate.

To find the issuer locality:

1. Right-click the process or file and click **Properties**.
2. From the **Digital Signatures** tab, select the first certificate you see on the signature list.
3. Select the certificate and click **Details**.
4. Click **View Certificate**.
5. Go to the **Details** tab and select **Issuer**.

If included in the certificate, the issuer L is displayed.

### Issuer State or Province

This property, which is currently supported only on Windows, specifies the issuer state or province (S) of the software certificate.

To find the issuer state or province:

1. Right-click the process or file and click **Properties**.
2. From the **Digital Signatures** tab, select the first certificate you see on the signature list.
3. Select the certificate and click **Details**.
4. Click **View Certificate**.
5. Go to the **Details** tab and select **Issuer**.

If included in the certificate, the issuer S is displayed.

#### Issuer Country

This property, which is currently supported only on Windows, specifies the issuer country (C) of the software certificate.

To find the issuer country:

1. Right-click the process or file and click **Properties**.
2. From the **Digital Signatures** tab, select the first certificate you see on the signature list.
3. Select the certificate and click **Details**.
4. Click **View Certificate**.
5. Go to the **Details** tab and select **Issuer**.

If included in the certificate, the issuer C is displayed.

## Application Control event aggregation and analysis

Dynamic software updates on a server can cause thousands of drift events (**Action** page) and security events (**Application Control Events** page). This presents a challenge in the use of Application Control, as it is difficult to know what to approve after the fact. To mitigate the situation while using Deep Security Agent 20.0.0.5761 or later, you can create trust rules that allow you to only see atypical drift and security events. This also allows you to put your server in lockdown to prevent any unauthorized software from being executed.

Drift events are aggregated based on the process name and target path. Security events are aggregated based on the SHA256 hash and target path. For example, if the same process creates 10,000 drift items at the same path, the drift would be aggregated to a single trust rule with the `processName` and `paths` attributes.

When diagnostics are requested for the agent, the aggregated drift events and security events are stored in a trust rule format in a JSON file and included in the diagnostics. The JSON file can then be used by the **Trust Rule** editor to add the trust rules for the server.

#### Drift events

A drift event in the JSON format has the following attributes:

```
{"time":1615999592250,"eventType":"ApplicationControl","uid":1063,"g
id":1064,"operationType":"create","user":"ribapp","group":"ribapp",
"md5":"57579EF7681147B84774F69F44783A67","sha256":"90B0418DCB3B29440
EE6F69FEE05BD54265CEE3BCFABDA8ED355E257FECC2939",

"processName":"/opt/IBM/WebSphere/AppServer/java/jre/bin/java","type
":4,"rdev":0,"lastModificationTime":1615999090000,"mode":33188,"size
":3984617,

"sha1":"B226BDB9DB39AD38C4BEB6FE4F1C1C7151207848","nlink":1,"procUse
r":"ribapp","isAuthorized":1,"pid":10223,"fileExtension":"jar",

"operationDate":1615999591534,"procUid":1063,"procGroup":"ribapp","p
ath":"/opt/IBM/WebSphere/AppServer/profiles/devmiesAppSrv/installedA
pps/devdmrhx01-
cell02/IESHSRIDEVM.ear/","fileName":"DC.jar","recordTime":1615999592
215,"fileSystemType":"ext4","procGid":1063,"dev":64775,"source":4,"i
no":3801778}
```

- `processName` is the name of the process that created or updated the target file. In the preceding example, it is set to `/opt/IBM/WebSphere/AppServer/java/jre/bin/java`.
- `path` is the location in which the process updated or created the executable file. In the preceding example, it is set to `/opt/IBM/WebSphere/AppServer/profiles/devmiesAppSrv/installedApps/devdmrhx01-cell02/IESHSRIDEVM.ear/`.

## Trust rules for drift events

You can create a trust rule to auto-authorize the drift for an event. A trusted updater can be defined via setting `trustType` to 1 for this rule, and you are trusting the process to create software in any path listed in `paths`:

```
        "trustrules": [{
            "trustType":"1",

"processName":"/opt/IBM/WebSphere/AppServer/java/jre/bin/java",
"paths":"/opt/IBM/WebSphere/AppServer/profiles/devmiesAppSrv/install
edApps/devdmrhx01-cell02/IESHSRIDEVM.ear/"
        }, ]
```

Processing drift events to create trust rules can be a many-to-one operation. For example, if the process named `/opt/IBM/WebSphere/AppServer/java/jre/bin/java` creates thousands of JAR files in path `/opt/IBM/WebSphere/AppServer/profiles/devmiesAppSrv/installedApps/devdmrhx01-cell02/IESHSRIDEVM.ear/`, the preceding trust rule will eliminate drift for all of these JAR files, which makes trust rules efficient at aggregating the drift.

A trust rule consists of an array of rules, with one unique process per rule. Each trust rule can have multiple paths defined in its `paths` attribute. For example, if a process named `process1` has created drift at three distinct locations `path1`, `path2`, `path3`, one trust rule can capture all drift created by `process1` at all of these locations:

```
        "trustrules": [{
            "trustType":"1",
            "processName":"process1",
            "paths":"path1;path2;path3"
        }, ]
```

There is an additional attribute called `hitcount` whose purpose is a process hit count. You can use this attribute to determine how many times a specific trust rule has been hit.

There is also an extension hit count: extensions are tracked by incrementing each time the process updates a file with a particular extension:

```
        "trustrules": [{
            "trustType":"1",
            "processName":"process1",
            "paths":"path1;path2;path3",
            "hitcount":12342,
            ".jar":1234,
            ".py":323,
            ".":456
        }, ]
```

The preceding example shows a process that has updated JAR files 1234 times, pi files 323 times, and files with no extensions 456 times.

### Security events

A security event in the JSON format has the following attributes:

```
        "
  {time":1492100772165,"eventType":"ApplicationControl","sha1":"066A02
  D230F3B16439396B049DC

  912DB376B96CE","fileName":"svchost.exe","operationType":"detectOnly"
  ,"blockReason":2,"size":31

  1544,"sha256":"62EFB22F6853D73374761A0B8ED2CE40BF09AA401EC7D4AAAA0CE
  4D5C3380EEA","type":1,
        "path":"C:\\Windows\System32\\","pid":1832,"operationDate":

  1492100772149,"processName":"\\device\\harddiskvolume2\\windows\\sys
  tem32\\cmd.exe","md5":
        "5F7B8544F7A20800069107FC93384F0E"},

  {"time":1492100772165,"eventType":"ApplicationControl","blockReason"
  :2,"sha256":"62EFB22F6

  853D73374761A0B8ED2CE40BF09AA401EC7D4AAAA0CE4D5C3380EEA","size":3115
  44,"processName":"\\de

  vice\\harddiskvolume2\\windows\\system32\\cmd.exe","sha1":"066A02D23
  0F3B16439396B049DC912D
```

```
B376B96CE","operationType":"detectOnly","pid":1832,"md5":"5F7B8544F7
A20800069107FC93384F0E
        ","path":"C:\\Program Files\\Trend Micro\\Deep Security
Agent\\","operationDate":149210077}
```

In the preceding example, `sha256` is set to `62EFB22F6853D73374761A0B8ED2CE40BF09AA401EC7D4AAAA0CE4D5C3380EEA` and `path` is set to `C:\\Windows\System32\\`.

## Trust rules for security events

You can create a trust rule to auto-authorize the drift for a security event. A trusted target can be defined via setting `trustType` to 2 for this rule, based on SHA256 hash, in any path listed in `paths`:

```
        "trustrules": [{
            "trustType":"2",

"sha256":"62EFB22F6853D73374761A0B8ED2CE40BF09AA401EC7D4AAAA0CE4D5C3
380EEA",
            "paths":"C:\\Windows\System32\\"
        }, ]
```

Processing security events to create trust rules is a complex operation. A trust rule consists of an array of rules, with one unique SHA256 per rule. Each trust rule can have multiple paths defined in its `paths` attribute. For example, if a file is executed with a `sha256` content hash `AAAAAAAABBBBBBBBCCCCCCCCDDDDDDDDD` from distinct locations `path1`, `path2`, `path3`, one trust rule can represent this as follows:

```
        "trustrules": [{
            "trustType":"2",
            "sha256":"AAAAAAAABBBBBBBBCCCCCCCCDDDDDDDDD",
            "paths":"path1;path2;path3"
        }, ]
```

There is an additional attribute called `hitcount` whose purpose is a SHA256 hit count. You can use this attribute to determine how many times a specific trust rule has been hit.

There is also a file name hit count: files with different names can have the same SHA256 content hash. You can use this attribute to count the number of times a file with a specific name has been used to execute the same SHA256. In the following example, SHA256 `AAAAAAAABBBBBBBBCCCCCCCCDDDDDDDDEEEEEEEE` has been executed 12342 times, `filename1` has been used 2342 times, and `filename2` has been used 10000 times. Both `filename1` and `filename2` have the same content hash.

Since processes with different names can execute the same target with the same SHA256 content hash, you can also count the number of times that the process name was used to execute the same SHA256. In the following example, SHA256 `AAAAAAAABBBBBBBBCCCCCCCCDDDDDDDDEEEEEEEE` has been executed 12342 times, `filename1` has been used 2342 times, and `filename2` has been used 10000 times. Both `filename1` and `filename2` have the same content hash. Process name `/opt/process1` was used to execute the target 12000 times and `/opt/process2` was used to execute the target 342 times.

```
"trustrules": [{
    "trustType":"2",
    "sha256":"AAAAAAAABBBBBBBBCCCCCCCCDDDDDDDDEEEEEEEE",

    "paths":"path1;path2;path3",
    "hitcount":12342,
    "filename1":2342,
    "filename2":10000
    "/opt/process1":12000,
    "/opt/process2":342
}, ]
```

Note that a process is represented with a full path, while the file name is included in a relative path to one of the paths.

#### Event analysis output

The Application Control event analysis output is directed to a file called `ac_event_analysis.txt`. This file has a trust rule format with additional hit count attributes and extension hit count attributes:

```
trustrules": [{
    "trustType":"1",
    "processName":"process1",
    "paths":"path11;path12;path13",
    "hitcount":12342,
    ".jar":12342
}
{
    "trustType":"1",
    "processName":"process2",
    "paths":"path21;path22;path23",
    "hitcount":23232,
    ".py":23232
}
{
    "trustType":"1",
    "processName":"process3",
    "paths":"path31;path32;path33",
    "hitcount":34332,
    ".exe":34322
}
{
    "trustType":"1",
    "processName":"process4",
    "paths":"path41;path42;path43",
    "hitcount":12312,
    ".":12312
}, ]
```

The file locations are as follows:

- On Windows: `C:\ProgramData\Trend Micro\Deep Security Agent\diag\ac_event_analysis.txt`.

- On Linux: `/var/opt/ds_agent/diag/ac_event_analysis.txt`.
- In the diagnostics: `agent/ac/ac_event_analysis.txt`.

The analysis is loaded from this file on restart so that the state is maintained after an agent restart. The analysis is cleared when Application Control is enabled after having been disabled. To view the `ac_event_analysis.txt` file, either use JQ or an online JSON formatter.

### Debug trust rules

You can debug trust rules as follows:

1. Apply new trust rules to Deep Security Manager.
2. Stop Deep Security Agent.
3. Delete the `ac_event_analysis.txt` file.
4. Start Deep Security Agent.
5. Wait a few minutes to see if the `ac_event_analysis.txt` file reappears:
   - If the file no longer appears, then the trust rules are working and suppressing the event generation.
   - If the file still appears, inspect the `ac_event_analysis.txt` file for the new event information and add new trust rules accordingly. Trust type 1 rules are Allow by source rules for auto-approving drift events, whereas trust type 2 rules are Allow by target rules to allow execution of the target file.
6. To configure new trust rules, repeat the procedure starting from step 1.

To see how often the trust rules are being hit, execute `sendCommand` on the agent, as follows:

- Linux: `/opt/ds_agent/sendCommand --get TrustRules`
- Windows: `\program files\trend micro\deep security agent\sendCommand --get TrustRules`

### Consult metrics

The drift analysis and event analysis are added to the Application Control metrics, where top ten processes with the highest hit counts are included in the `drift_analysis` object and the top ten SHA256 with the highest counts are stored in the `event_analysis` object:

```
"AC": {
    "eventReportInQueue":"0",
    "evtPreCreateProcessHandled":"17",
                "acProcessHashCount":"0",
                "acProcessBlockUnrecognized":"0",
                "engFlushDbBufferError":"0",
                "acFileProcessImgPath":"0",
                "evtFilePostClose":"249",
                "acFileErrorHash":"0",
                "acFileAllowImportingRuleset":"0",
                "evtFilePreCreateFromContainer":"0",
                "evtFilePostChmodFromContainer":"0",
                "engStopError":"0",
                "evtFilePreCreateHandled":"0",
                "ctrlInterpreterMatched":"0",
                "engPurgeDb":"0",
                "importCount":"0",
                "inventoryAdsVisited":"0",
                "engGetInventory":"1",
                "acFileAllow":"5",
                "acFileAllowBuilding":"0",
                "engSetConfigError":"0",
                "ctrlMsiInstallationMatched":"0",
                "ctrlDropProcessEvtReportQueueFull":"0",
                "importFail":"0",
                "eventReportDropped":"0",
                "evtFilePostChmod":"3",
                "acFileBlock":"0",
                "acFileDrift":"3",
                "engGetMetricsError":"0",
                "ctrlDropFileEvtReportQueueFull":"0",
                "inventoryFolderVisited":"0",
                "engStartError":"0",
                "evtFileCloudFileIgnore":"0",
                "engSetConfig":"1",
                "engFlushDbBuffer":"0",
               "engPurgeDbError":"0",
               "inventoryBytesInventoried":"433695822",
               "evtPreCreateProcessWithCmdLine":"0",
               "inventoryDriveVisited":"0",
               "importSuccess":"0",
               "engSetRuleset":"0",
               "eventReportSent":"3",
               "drift_analysis": [
                   {
                   "trusttype":"1",
                   "processName":"/usr/bin/bash",
                   "hitcount":2,
                   "paths":"/im1"
                   },
                   {
                   "trusttype":"1",
                   "processName":"/usr/bin/cp",
                   "hitcount":1,
                   "paths":"/im1"
                   }
               ],
               "event_analysis": [
                   {
                   "trusttype":"2",
                   "sha256":"AAAAAAAABBBBBBBBCCCCCCCCDDDDDDDDEEEEEEEE",
                   "hitcount":2,
                   "paths":"/im1"
                   },
                   {
                   "trusttype":"2",

   "sha256":"EEEEEEEEDDDDDDDDCCCCCCCCBBBBBBBBAAAAAAAA",
                   "hitcount":1,
                   "paths":"/im1"
                   }
               ],
```

### View signer information

When trust rules are enabled, both the file signer information and process signer information are included in trust rules for the drift events analysis. For security event analysis, the file signer information is included.

Trust rules are enabled (the file signer information along with the process signer information is visible in the `ac_event_analysis.txt` file) when a trust entity ruleset is applied to the host.

## Trust rule property limitations for Linux

> **Warning:** Adding trust rules that are not currently supported on Linux will result in the rules not applying for any software changes.

The following trust rule properties are not currently supported for Linux:

- Signer Name
- Product Name
- Issuer Common Name
- Issuer Organizational Unit
- Issuer Organization
- Issuer Locality
- Issuer State or Province
- Issuer Country
- Vendor

Only the following trust rule properties are currently supported for Linux:

- Process Name
- Paths
- SHA-256

## Reset Application Control after too much software change

For an overview of Application Control, see "About Application Control" on page 990.

Application Control is intended for use on stable servers that are not updated frequently, and not for workstations or servers that undergo a lot of software changes.

Too many changes make large rulesets that consume more RAM, unless you remove old rules. If you don't use maintenance mode during authorized software updates, too many changes can also result in high administrator workload because they must manually create allow rules for each change.

**If unrecognized software changes exceed the maximum, Application Control will stop detecting and displaying all of the computer's software changes.** This stoppage is designed to prevent out-of-memory and disk space errors that can occur if the ruleset grows too large.

When a stoppage occurs, Deep Security Manager will notify you through an alert ("Unresolved software change limit") and an event log ("Unresolved software change limit reached"). You must resolve the issue to continue detecting software changes.

1. Examine the computer's processes and security events. Verify that the computer has not been compromised. If you are not sure, or do not have enough time, the safest and fastest way is to restore the system from a backup or VM snapshot.

   > Warning: If you don't remove any unauthorized software (including zero-day malware), Application Control will ignore it when you reset Application Control. It won't appear on the Actions tab anymore and if its process has already executed and it is in RAM, Application Control won't log any events or alerts about it until you reboot the computer.

2. If the computer was running software updates, including auto-updates (for example, browser, Adobe Reader, or yum auto-updates), disable them or schedule them so that they occur only when you have enabled Application Control's maintenance mode (see "Turn on maintenance mode when making planned changes" on page 1001).
3. Reset Application Control. To do this, disable Application Control in the **Computer editor**[1]. Once the agent has acknowledged it and cleared the error status, enable Application Control again. The agent generates a new software inventory list.

[1] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

## Use the API to create shared and global rulesets

For an overview of Application Control, see "About Application Control" on page 990. For initial configuration instructions, see "Set up Application Control" on page 996.

Using the Deep Security Manager API on the Automation Center, you can create shared rulesets and global rules. You can use one type of ruleset, or a combination. For more information, see Create a shared ruleset and Add global rules.

- **Local ruleset:** Rules that are added as part of a computer's software inventory or when in maintenance mode are stored only on the protected computer and are not visible in Deep Security Manager. Allow or block rules that you configure in Deep Security Manager are sent to the agent and stored in both places. Because agents don't transfer their inventory information to the manager, local rulesets offer better performance than shared rulesets.

  To determine whether software is new or has changed, Deep Security Agent 10 compares the file with the initially installed software's SHA-256 hash, file size, path, and file name (they have a "file-based" local ruleset). Deep Security Agent 11 and newer compares only the file's SHA-256 hash and file size (they have a "hash-based" local ruleset). Because the rules created by Deep Security 11 (and newer) agents compare only the unique hash and file size, a rule will continue to be applied even if the software file is renamed or moved. As a result, using Deep Security Agent 11 or newer reduces the number of software changes that you need to deal with. Deep Security Agent 10 continues to use a file-based local ruleset until it is upgraded to Deep Security Agent 11.0 or newer. When you upgrade, its local ruleset is converted to use hash-based rules.

  > **Note:** If there are multiple file-based rules for the same hash value, they are consolidated into one hash-based rule. If the rules being consolidated conflict with each other (one rule blocks the file and another allows it), the new hash-based rule will be an "allow" rule.

- **Shared ruleset:** Syncs all of its rule data onto both agents and manager (and also relays, if enabled). This increases network and disk space usage. However, it may be easier if you need to verify the rules from the initial inventory scan or maintenance mode, or if you manage a server farm with many computers that should be identical. For example, if you have a server pool of identical LAMP web servers, or if they are virtual machines (VMs) that are part of an auto-scaling group, shared rulesets can be useful. It can also reduce administrator workload.

> **Warning:** Don't use a shared ruleset if you enabled **Block unrecognized software until it is explicitly allowed**, and if computers are merely similar (but not identical). It will block all software on other computers that isn't in the first computer's ruleset. If those include critical files, it could break the OS. If that happens, you may be required to reinstall, revert to a backup, or use the OS recovery mode.

When you create a new shared ruleset using Deep Security Agent 11.1 or newer, it can only contain hash-based rules (rules that compare only a file's hash and size). If you created a shared ruleset using Deep Security Agent 11.0 or earlier, it contains file-based rules (rules that compare a file's name, path, size, and hash). Older shared rulesets will continue to use file-based rules until all agents using the shared ruleset are upgraded to Deep Security Agent 11.0 or newer. Then the shared ruleset will be converted to use hash-based rules.

> **Warning:** Don't create a new shared ruleset until all agents are upgraded to Deep Security Agent 11.0 or newer. New shared rulesets are hash-based and are not compatible with Deep Security Agent 10.3 or earlier, which supports only file-based rulesets.

> **Note:** If there are multiple file-based rules for the same hash value, they are consolidated into one hash-based rule. If the rules being consolidated conflict with each other (one rule blocks the file and another allows it), the new hash-based rule will be an "allow" rule.

To create shared rules, see Create a shared ruleset on the Automation Center.

- **Global rules:** Like shared rulesets, global rules are distributed to agents by the manager (and also relays, if enabled). This increases network and disk space usage. However, because they are global, you don't need to spend time selecting them in each policy. Global rules aren't part of the rulesets you can see in Deep Security Manager. Global rules can only contain block rules, not allow rules.

  Global rules require Deep Security Agent 10.2 or newer. The manager will not send the global rules to older agents. Global rules take precedence over all other Application Control rules and are enforced on all computers where Application Control is enabled. The rules in global rules are based on a file's MD5, SH-1 or SHA-256 hash. Because a software file's hash is unique, you can block specific software everywhere – regardless of file path, policy, or computer group, and regardless of whether Application Control has detected the software before.

> **Note:** In a multi-tenant deployment, each tenant has a separate global rules. To block software for all tenants, create the same global rules for each tenant.

To create global rules, see Add global rules on the Automation Center.

In this article:

- "Create a shared ruleset" below
- "Change from shared to computer-specific allow and block rules" on the next page
- "Deploy Application Control shared rulesets via relays" on the next page
- "Considerations when using relays with shared rulesets" on page 1045

## Create a shared ruleset

You can use the API to create shared allow or block rules and apply the ruleset to other computers. This can be useful if you have many identical computers (such as a load balanced web server farm). **Shared rulesets should be applied only to computers with the exact same inventory.**

1. Use the API to build a computer's shared allow and block rules. For more information, see Create a Shared Ruleset. If you want to examine the shared ruleset before you deploy it, see "View and change Application Control rulesets" on page 1007.
2. Go to **Computer or Policy editor**[1] **> Application Control**.
3. In the ruleset section, make sure **Inherit settings** is not selected and then select **Use a shared ruleset**. Indicate which shared rules to use.

   > **Note:** These settings are hidden until you use the API to create at least one shared ruleset. If you haven't created any shared rulesets, or if you keep the default settings, each computer will keep its own allow and block rules locally. Changes to local rules don't affect other computers.

4. Click **Save**.

   The next time that the Deep Security Agent on the computer connects with Deep Security Manager, the agent applies those rules.

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

If you see an error saying that the ruleset upload was not successful, verify that network devices between the agent and the manager or relay allow communications on the heartbeat port or relay port numbers.

## Change from shared to computer-specific allow and block rules

If the computer is currently using shared allow or block rules created via the API, you can change it to use local rules. Application control scans the file system for all currently-installed software and creates an initial ruleset for it, similar to when you first enabled Application Control.

**Warning:** Before you start, verify that only good software is currently installed. Rebuilding the ruleset will allow all currently installed software, even if it is insecure or malware. If you are not sure what is installed, the safest approach is to make a clean install and then enable Application Control.

The steps below configure a computer's agent to use a local ruleset. If you want all computers to use local rules, edit the setting in the **Policies** tab instead.

1. Go to **Computer editor**[1] **> Application Control**.
2. In the ruleset section, deselect **Inherit settings** (if necessary), and then select **Use local ruleset initially based on installed software**.
3. Click **Save**.

   To verify the change, the next time the agent and Deep Security Manager connect, look for event log messages about building the Application Control ruleset.

## Deploy Application Control shared rulesets via relays

Each time you create an Application Control ruleset or change it, it must be distributed to all computers that use it. Shared rulesets are bigger than local rulesets. Shared rulesets are also often applied to many servers. If they all downloaded the ruleset directly from the manager at the same time, high load could cause slower performance. Global rulesets have the same considerations.

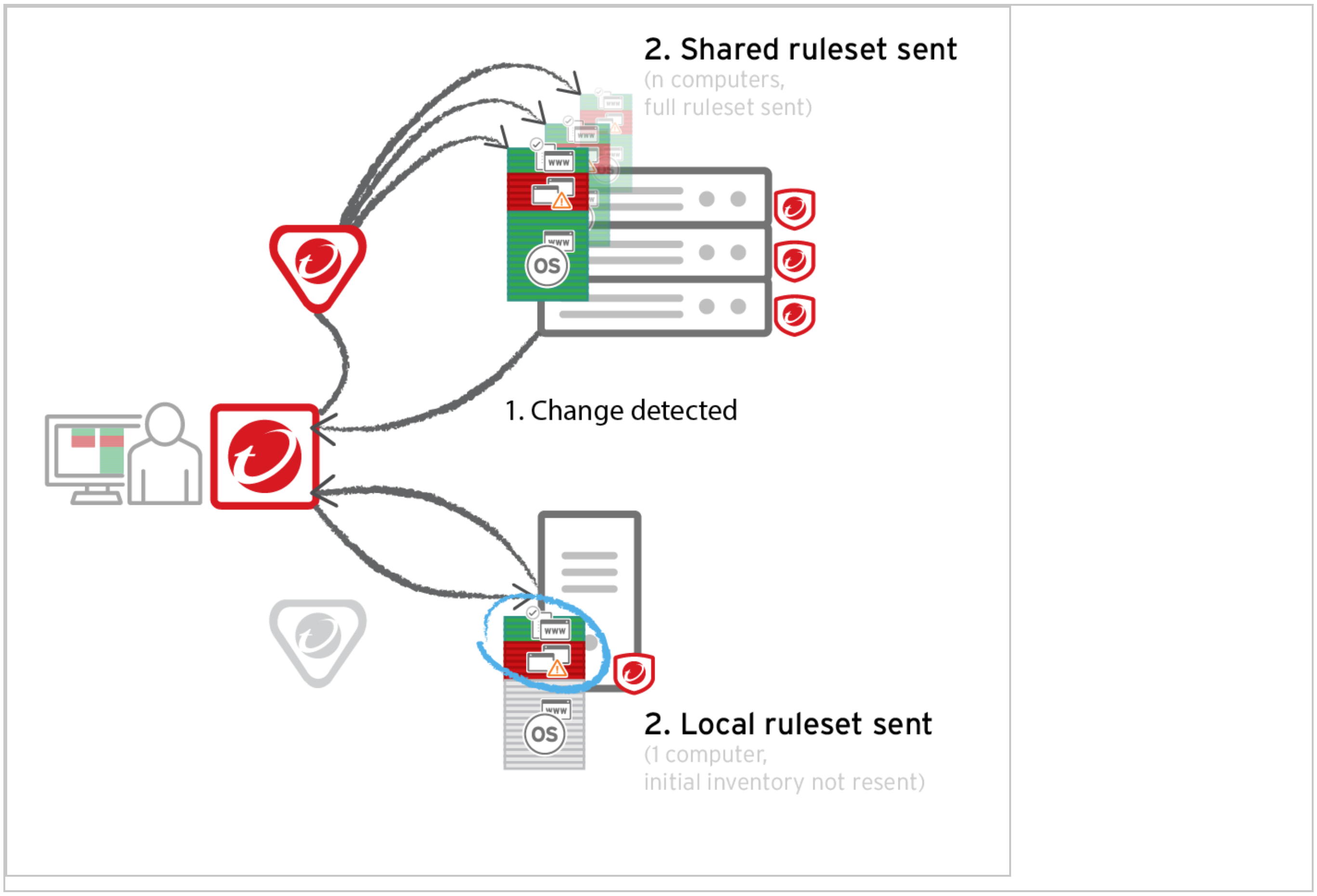
Using Deep Security Relays can solve this problem. (For information on configuring relays, see "Deploy additional relays" on page 1345.)

Steps vary depending whether or not you have a multi-tenant deployment.

[1] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

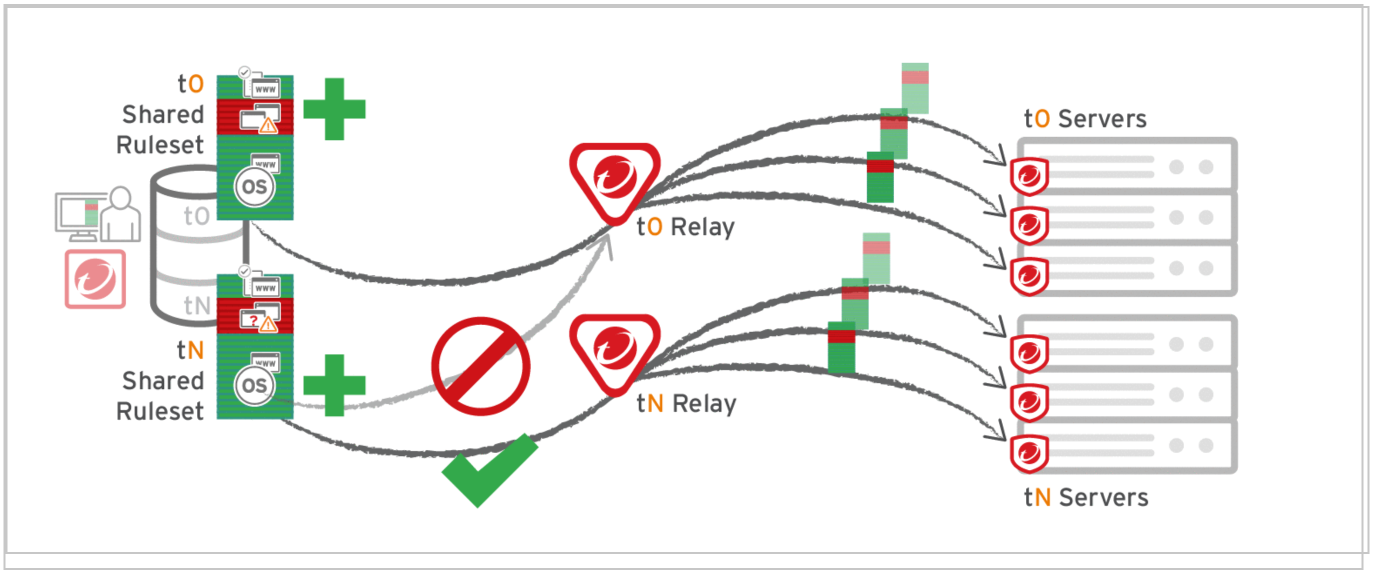
### Single tenant deployments

Go to **Administration > System Settings > Advanced** and then select **Serve Application Control rulesets from relays**.



### Multi-tenant deployments

The primary tenant (t0) can't access other tenants' (tN) configurations, so t0 relays don't have tN Application Control rulesets. Other tenants (Tn) must create their own relay group, then select **Serve Application Control rulesets from relays**.



## Considerations when using relays with shared rulesets

Before using relays, verify that they are compatible with your deployment. If the agent doesn't have any previously downloaded ruleset currently in effect, and **if it doesn't receive new Application Control rules, then the computer won't be protected by Application Control.** If Application Control ruleset download fails, a ruleset download failure event will be recorded on the manager and on the agent.

- If you are using a proxy to connect agents to a manager, you must use a relay.

  > **Note:** In Deep Security Agent 10.0 and earlier, agents didn't have support for connections through a proxy to relays. If a ruleset download fails due to a proxy, and if your agents require a proxy to access the relay or manager, then you must either:
  > - update agents' software, then configure the proxy
  > - bypass the proxy
  > - add a relay and then select **Serve Application Control rulesets from relays**

- If you are using shared or global rulesets, a relay can result in faster performance.
- If you are using local rulesets, a relay can cause slower performance,
- Do not use a relay with multi-tenant configurations when non-primary tenants (tN) use the default, primary (t0) relay group.

# Configure events and alerts

## About Deep Security event logging

Deep Security Agents record when a protection module rule or condition is triggered (a "security event"). Agents and Deep Security Manager also records when administrative or system-related events occur (a "system event"), such as an administrator logging in, or agent software being upgraded. Event data is used to populate the various reports and graphs in Deep Security Manager.

To view events, go to **Events & Reports** in Deep Security Manager.

### Where are event logs on the agent?

Location varies by the computer's operating system. On Windows, event logs are stored in this location:

```
C:\Program Data\Trend Micro\Deep Security Agent\Diag
```

On Linux, event logs are stored here:

```
/var/opt/ds_agent/diag
```

**Note:** These locations only contain standard-level logs; diagnostic debug-level logs have a different location. For performance reasons, debug-level logging is not enabled by default. You should only enable debug logging if diagnosing an issue with Trend Micro technical support, and make sure to disable debug logging when you are done. For more information, see Enabling detailed logging on Deep Security Agent (DSA).

### When are events sent to the manager?

Most events that take place on a computer are sent to the Deep Security Manager during the next heartbeat operation except the following, which will be sent right away if communication settings allow relays/agents to initiate communication:

- Smart Scan Server is offline
- Smart Scan Server is back online
- Integrity Monitoring scan is complete

- Integrity Monitoring baseline created
- Unrecognized elements in an Integrity Monitoring Rule
- Elements of an Integrity Monitoring Rule are unsupported on the local platform
- Abnormal restart detected
- Low disk space warning
- Log Inspection offline
- Log Inspection back online
- Reconnaissance scan detected (if the setting is enabled in **Computer or Policy editor**[1] **> Firewall > Reconnaissance**

## How long are events stored?

Once collected by the Deep Security Manager, events are kept for a period of time, which is specified on the **Administration** > **System Settings** > **Storage** page. For details, see "Log and event storage best practices" on page 1050.

## System events

All the Deep Security system events are listed and can be configured on the **Administration > System Settings > System Events** tab. You can set whether to record the individual events and whether to forward them to a SIEM system. For details on system events, see "System events" on page 1233.

## Security events

Each protection module generates events when rules are triggered or other configuration conditions are met. Some of this security event generation is configurable. For information on specific types of security events, refer to these articles:

- "Anti-malware events" on page 1285
- "View and restore identified malware" on page 780
- "Application Control events" on page 1284

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

- "Firewall events" on page 1289
- "Integrity monitoring events" on page 1303
- "Intrusion prevention events" on page 1297
- "Log inspection events" on page 1306
- "Web reputation events" on page 1308
- "Device Control events" on page 1288

The firewall stateful configuration in effect on a computer can be modified to enable or disable TCP, UDP, and ICMP event logging. To edit the properties of a stateful firewall configuration, go to **Policies > Common Objects > Other > Firewall Stateful Configurations**. The logging options are in the **TCP**, **UDP**, and **ICMP** tabs of the firewall stateful configuration's **Properties** window. For more information about firewall events, see "Firewall events" on page 1289.

## See the events associated with a policy or computer

The **Policy editor**[1] and the**Computer editor** [2]both have **Events** tabs for each protection module. The policy editor displays events associated with the current policy. The computer editor displays events specific to the current computer.

## View details about an event

To see details about an event, double-click it.

The **General** tab displays:

- **Time:** The time according to the system clock on the computer hosting the Deep Security Manager.
- **Level:** The severity level of event that occurred. Event levels include **Info**, **Warning**, and **Error**.
- **Event ID:** The event type's unique identifier.
- **Event:** The name of the event (associated with the event ID.)
- **Target:** The system object associated with the event will be identified here. Clicking the object's identification will display the object's properties sheet.

[1] To open the Policy editor, go to the Policies page and double-click the policy that you want to edit (or select the policy and click Details).

[2] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

- **Event Origin:** The Deep Security component from which the event originated.
- **Action Performed By:** If the event was initiated by a user, that user's username will be displayed here. Clicking the username will display the **User Properties** window.
- **Manager:** The hostname of the Deep Security Manager computer.
- **Description:** If appropriate, the specific details of what action was performed to trigger this event are displayed here.

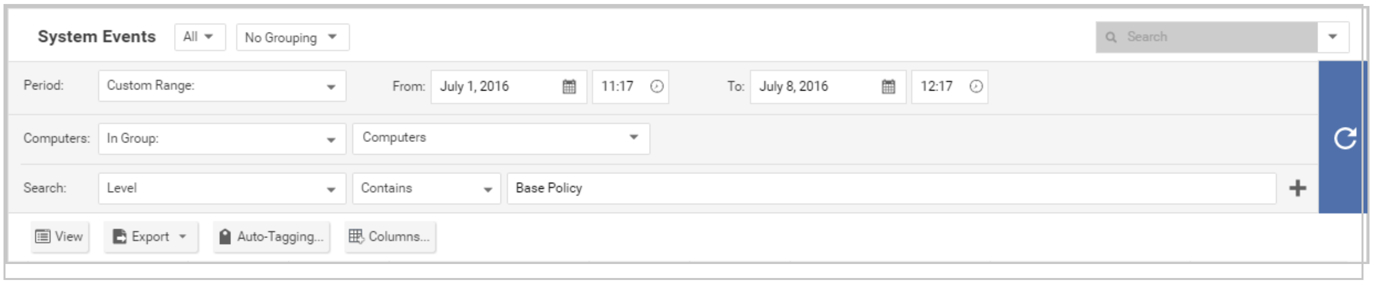
The **Tags** tab displays tags that have been attached to this event. For more information on event tagging, see **Policies > Common Objects > Other > Tags**, and "Apply tags to identify and group events" on page 1057.

## Filter the list to search for an event

The **Period** toolbar lets you filter the list to display only those events that occurred within a specific timeframe.

The **Computers** toolbar lets you organize the display of event log entries by computer groups or computer policies.

Clicking **Search > Open Advanced Search** toggles the display of the advanced search bar.


System Events: All, No Grouping

Period: Custom Range: From: July 1, 2016 11:17 To: July 8, 2016 12:17

Computers: In Group: Computers

Search: Level Contains Base Policy

Clicking the "Add Search Bar" button (+) to the right of the search bar will display an additional search bar so you can apply multiple parameters to your search. When you are ready, press the "Submit Request" button (at the right of the toolbars with the right-arrow on it).

## Export events

You can export displayed events to a CSV file. (Paging is ignored, all pages will be exported.) You have the option of exporting the displayed list or the selected items.

## Improve logging performance

Here are some suggestions to help maximize the performance of event collection:

- Reduce or disable log collection for computers that are not of interest.
- Consider reducing the logging of firewall rule activity by disabling some logging options in the firewall stateful configuration **Properties** window. For example, disabling the UDP logging will eliminate the "Unsolicited UDP" log entries.

# Log and event storage best practices

Best practices for log and event data storage depend on the data compliance regulations you must meet, such as PCI and HIPAA. Also consider optimizing the use of your database. Storing too much data may affect database performance and size requirements.

If you're storing too much data in your database, these symptoms may occur:

- Error messages that systems may be experiencing loss of database activity
- Inability to import software updates
- General slow-down in Deep Security

To avoid those symptoms:

1. Store system events according to the compliance standard requirement.
2. Forward system and security events to external storage. See "Forward Deep Security events to a Syslog or SIEM server" on page 1067. Then you can reduce how long events are kept in the local database.
3. Set thresholds in the log inspection module for event storage or event forwarding. **Severity clipping** allows you to send events to a Syslog server (if enabled) or to store events based on the severity level of the log inspection rule. See "Configure log inspection event forwarding and storage" on page 963.

Default local storage settings are in the table below. To change these settings, go to **Administration > System Settings > Storage**. To delete software versions or older rule updates, go to **Administration > Updates > Software > Local** or **Administration > Updates > Security > Rules**.

**Tip:** To reduce database disk space usage, forward events to an external Syslog server or SIEM and reduce the local event retention time. Only keep counters locally.

| Data type settings | Data pruning default setting |
|---|---|
| Automatically delete Anti-Malware Events older than | 7 Days |
| Automatically delete Web Reputation Events older than: | 7 Days |
| Automatically delete Firewall Events older than: | 7 Days |
| Automatically delete Intrusion Prevention Events older than: | 7 Days |
| Automatically delete Integrity Monitoring Events older than: | 7 Days |
| Automatically delete Log Inspection Events older than: | 7 Days |
| Automatically delete Application Control Events older than: | 7 Days |
| Automatically delete Device Control Events older than: | 7 Days |
| Automatically delete System Events older than: | 53 Weeks |
| Automatically delete Server Logs older than: | 7 Days |
| Automatically delete Counters older than: | 13 Weeks |
| Number of older software versions to keep per platform:* | 5 |
| Number of older Rule Updates to keep: | 10 |

* If multi-tenancy is enabled, this setting will not be available.

**Note:** If using a PostgreSQL database, old events might not be pruned immediately. PostgreSQL maintenance jobs periodically remove the old events' database partitions. Pruning will occur during the next scheduled job.

*Events* are records of individual events. They populate the **Events** pages.

*Counters* are the number of times individual events have occurred. They populate the dashboard widgets (number of firewall events over the last 7 days, etc.) and the reports.

*Server log files* are from Deep Security Manager's web server. They don't include event logs from agents installed on your network's web servers.

## Troubleshooting

During troubleshooting, it may be useful to increase the logging level and record more detailed events.

Increased logging can significantly increase disk space usage. Reduce the logging level again when you have finished troubleshooting.

1. Open the Computer or Policy editor[1].
2. Go to **Settings > General > Logging Level**.
3. Choose whether to inherit the logging override settings from the policy assigned to this computer (**Inherited**), to not override logging settings (**Do Not Override**), to log all triggered firewall rules (**Full Firewall Event Logging**), to log all triggered intrusion prevention rules (**Full Intrusion Prevention Event Logging**), or to log all triggered rules (**Full Logging**).
4. Click **Save** .

## Limit log file sizes

You can set the maximum size of each individual log file and how many of the most recent files are kept. Event log files will be written to until they reach the maximum allowed size, at which point a new file will be created and written to until it reaches the maximum size and so on. Once the maximum number of files is reached, the oldest will be deleted before a new file is created. Event log entries usually average around 200 bytes in size and so a 4 MB log file will hold about 20,000 log entries. How quickly your log files fill up depends on the number of rules in place.

1. Open the Computer or Policy editor[2] for the policy that you want to configure.
2. Go to **Settings > Advanced > Events**.
3. Configure these properties:

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

- **Maximum size of the event log files (on Agent/Appliance):** Maximum size that the log file can reach before a new log file is created.
- **Number of event log files to retain (on Agent/Appliance):** Maximum number of log files that will be kept. Once the maximum number of log files is reached, the oldest file will be deleted before a new one is created.
- **Do Not Record Events with Source IP of:** This option is useful if you don't want Deep Security to make record events for traffic from certain trusted computers.

  > **Note:** The following three settings let you fine tune event aggregation. To save disk space, Deep Security Agents and Appliances will take multiple occurrences of identical events and aggregate them into a single entry and append a "repeat count", a "first occurrence" timestamp, and a "last occurrence" timestamp. To aggregate event entries, Deep Security Agents and Appliances need to cache the entries in memory and then write them to disk.

- **Cache Size:** Determines how many types of events to track at any given time. Setting a value of 10 means that 10 types of events will be tracked (with a repeat count, first occurrence timestamp, and last occurrence timestamp). When a new type of event occurs, the oldest of the 10 aggregated events will be flushed from the cache and written to disk.
- **Cache Lifetime:** Determines how long to keep a record in the cache before flushing it to disk. If this value is 10 minutes and nothing else causes the record to be flushed, any record that reaches an age of 10 minutes gets flushed to disk.
- **Cache Stale time:** Determines how long to keep a record whose repeat count has not been recently incremented. If Cache Lifetime is 10 minutes and Cache Staletime is 2 minutes, an event record which has gone 2 minutes without being incremented will be flushed and written to disk.

  > **Note:** Regardless of the above settings, the cache is flushed whenever events are sent to the Deep Security Manager.

4. Click **Save**.

## Event logging tips

- On computers that are less important, modify the amount of logs collected. This can be done in the **Events** and **Advanced Network Engine Options** areas on the Computer or

Policy editor[1] > **Settings > Advanced** tab.

- Consider reducing the event logging of firewall rule activity by disabling the event logging options in the firewall stateful configuration. (For example, if you disable UDP logging, it will eliminate unsolicited UDP log entries.)
- For intrusion prevention rules, the best practice is to log only dropped packets. If you log packet modifications, it may cause too many log entries.
- For intrusion prevention rules, only include packet data (an option in the intrusion prevention rule's **Properties** window) when you are interested in examining the behavior of a specific attack. Packet data increases log sizes, so it shouldn't be used for everything.

# Anti-Malware scan failures and cancellations

Anti-Malware scans can fail or be cancelled for several reasons, which have different recommended actions.

**Note:** These events can occur for manual, quick, or scheduled scans.

## Anti-Malware scan failure events

This table provides possible reasons for system events 793, 795, and 1543 (Malware Scan Failure).

| Event reason | Reason ID * | Description | Recommended action |
|---|---|---|---|
| Empty configuration | 31 | Malware Scan could not be started. This is caused by an empty Malware Scan configuration. | 1. From the Computer or Policy editor, go to **Anti-Malware > General**.<br>2. Make sure a Malware Scan configuration is assigned to the Scheduled scan.<br>3. Rerun the scan. |
| Anti-Malware module is off | 30 | Malware Scan could not be started. This is because the Anti-Malware module is turned off. | 1. From the Computer or Policy editor, go to **Anti-Malware >** |

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

| Event reason | Reason ID * | Description | Recommended action |
|---|---|---|---|
| | | | **General**.<br>2. Make sure the Anti-Malware state is "On" or "Inherited (On)."<br>3. Rerun the scan. |
| Anti-Malware service stops | 7 | Malware Scan failed because the Anti-Malware service is being terminated. | 1. From the Computer or Policy editor, go to **Overview > General**, and click **Check Status**.<br>2. If the Anti-Malware Status is "Anti-Malware Engine Offline," follow the procedure to solve the "Error: Anti-Malware Engine Offline" on page 1314 issue.<br>3. Rerun the scan. |
| Anti-Malware engine is offline | 9 | Malware Scan failed because the Anti-Malware engine is offline. | 1. Follow the procedure to solve the "Error: Anti-Malware Engine Offline" on page 1314 issue.<br>2. Rerun the scan. |
| Fail to access configuration | -2 | Malware Scan failed because of an inaccessible Anti-Malware configuration. (This may be due to an unexpected internal error or timing issue.) | 1. From the Computers page, right-click the target computer and go to **Actions > Assign Policy**.<br>2. Rerun the scan. |
| Other scan task is running | -16 | Malware Scan failed because another scan task is in progress. (This may be due to an unexpected internal error or timing issue.) | 1. From the Computers page, check the Task(s) column for the target computer to see if another Malware Scan is in progress.<br>2. If yes, either wait for the current scan task to complete or right-click the target computer and go to **Actions >** |

| Event reason | Reason ID * | Description | Recommended action |
|---|---|---|---|
| | | | **Cancel Malware Scan**.<br>3. Rerun the scan. |
| Unknown reason on agent | 10 | Malware Scan failed for an unknown reason. | 1. Collect the system event information and follow the procedure to "Create a diagnostic package" on page 1723.<br>2. Contact support. |

* The reason ID is included in events forwarded to an external Syslog, SIEM server, or to Amazon SNS. It is not displayed in Deep Security Manager.

## Anti-Malware scan cancellation events

This table provides possible reasons for system events 1526, 1528, and 1540 (Malware Scan Cancellation Completed).

| Event reason | Reason ID * | Description | Recommended action |
|---|---|---|---|
| Cancel by user | 1 | Anti-Malware scan was canceled manually or an Anti-Malware scheduled scan was terminated after exceeding its timeout limit. | Run the scan again. |
| Server reboot | 32 | Anti-Malware scan was canceled, possibly because the computer being scanned was shut down or restarted. | Check that the computer is on and run the scan again. |
| Anti-Malware service restart | 7 | Anti-Malware scan was cancelled because the Anti-Malware service was being restarted. | 1. From the Computer or Policy editor, go to **Anti-Malware > General**.<br>2. Make sure the Anti-Malware state is "On" or "Inherited (On)."<br>3. Rerun the scan. |
| Deep Security Agent restart | 6 | Anti-Malware scan was cancelled because the agent was being restarted. Check that the Anti-Malware module is online and run the scan again. | 1. From the Computer or Policy editor, go to **Anti-Malware > General**.<br>2. Make sure the Anti-Malware |

| Event reason | Reason ID * | Description | Recommended action |
|---|---|---|---|
| | | | state is "On" or "Inherited (On)."<br>3. Rerun the scan.<br>Also make sure there is no agent upgrade or policy change taking place during scanning because these tasks may cause the agent to restart. |
| Unknown reason | -1 | Anti-Malware scan was cancelled for an unknown reason. | 1. Collect the system event information and follow the procedure to "Create a diagnostic package" on page 1723.<br>2. Contact support. |

* The reason ID is included in events forwarded to an external Syslog, SIEM server, or to Amazon SNS. It is not displayed in Deep Security Manager.

## Apply tags to identify and group events

Deep Security enables you to create tags that you can use to identify and sort events. For example, you might use tags to separate events that are benign from those that require further investigation. You can use tags to create customized dashboards and reports.

Although you can use event tagging for a variety of purposes, it was designed to ease the burden of event management. After you have analyzed an event and determined that it is benign, you can look through the event logs of the computer (and any other similarly configured and tasked computers) to find similar events and apply the same label to them, eliminating the need to analyze each event individually.

To view tags that are currently in use, go to **Policies > Common Objects > Other > Tags**.

Tags do not alter the data in the events themselves, nor do they allow users to delete events. They are simply extra attributes provided by the manager.

You can perform tagging in the following ways:

- "Manual tagging" below lets you tag specific events as needed.
- "Auto-tagging" below lets you use an existing event as the model for auto-tagging similar events on the same or other computers. You define the parameters for similarity by selecting which event attributes have to match the model event attributes for a tag to be applied.
- "Trusted source tagging" on page 1060 lets you auto-tag integrity monitoring events based on their similarity to known-good events from a trusted source.

An important difference between standard tagging and trusted source tagging is that Run on Existing Events Now can only be done with standard event tagging

## Manual tagging

1. Go to **Events & Reports > Events** and select an event list. Right-click the event (or select multiple events and right-click) and select **Add Tag(s)**.
2. Type a name for the tag. Deep Security Manager will suggest matching names of existing tags as you type.
3. Select **The Selected [Event Type] Event**. Click **Next**.
4. Enter some optional comments and click **Finish**.

In the events list, you can see your tag in the **TAG(S)** column.

## Auto-tagging

Deep Security Manager enables you to define rules that apply the same tag to similar events automatically. To view existing saved auto-tagging rules, click **Auto-Tagging** in the menu bar on any **Events** page. You can run saved rules manually from this page.

1. Go to **Events & Reports > Events** and select an event list. Right-click a representative event and select **Add Tag(s)**.
2. Type a name for the tag. Deep Security Manager will suggest matching names of existing tags as you type.
3. Select **Apply to selected and similar [Event Type] Events** and click **Next**.
4. Select the computers where you want to auto-tag events and click **Next**. When applying tags to system events, this page is skipped.
5. Select which attributes will be examined to determine whether events are similar. For the most part, the attribute options are the same as the information displayed in the columns of the **Events** list pages. When you have selected which attributes to include in the event selection process, click **Next**.

6. On the next page, specify when events should be tagged. If you select **Existing [Event Type] Events**, you can select **Apply Auto-Tag Rule now** to apply the auto-tagging rule immediately, or **Apply Auto-Tag Rule in the background** to have it run in the background at a lower priority. Select **Future [Event Type] Events** to apply the auto-tagging rule to events that will happen in the future. You can also save the auto-tagging rule by selecting **Save Auto-Tag Rule** and optionally entering a name. Click **Next**.
7. Review the summary of your auto-tagging rule and click **Finish**.

In the events list, you can see that your original event and all similar events have been tagged

Event tagging only occurs after events have been retrieved from the agents or appliances to the Deep Security Manager database.

## Set the precedence for an auto-tagging rule

Once an auto-tagging rule is created, you can assign it a **Precedence** value. If the auto-tagging rule has been configured to run on future events, the rule's precedence determines the order in which all auto-tagging rules are applied to incoming events. For example, you can have a rule with a precedence value of 1 that tags all User Signed In events as "suspicious", and a rule with a precedence value of 2 that removes the "suspicious" tag from all User Signed In events where the target (user) is you. This results in a "suspicious" tag being applied to all future User Signed In events where the user is not you.

1. In an events list, click **Auto-Tagging** to display a list of saved auto-tagging rules.
2. Right-click an auto-tagging rule and select **Details**.
3. In the **General** tab, select a **Precedence** for the rule.

## Auto-tagging log inspection events

Log inspection events are auto-tagged based upon their grouping in the log file structure. This simplifies and automates the processing of log inspection events within Deep Security Manager. You can use auto-tagging to automatically apply tags for the log inspection groups. Log inspection rules have groups associated with them in the rules. For example:

```
<rule id="18126" level="3">
 <if_sid>18101</if_sid>
 <id>^20158</id>
 <description>Remote access login success</description>
 <group>authentication_success,</group>
 </rule>

 <rule id="18127" level="8">
 <if_sid>18104</if_sid>
 <id>^646|^647</id>
 <description>Computer account changed/deleted</description>
<group>account_changed,</group>
 </rule>
```

Each group name has a friendly name string associated with it. In the preceding example, `authentication_success` would be `Authentication Success`, `account_changed` would be `Account Changed`. When this is enabled, the friendly names are automatically added as a tag for that event. If multiple rules trigger, multiple tags will be attached to the event.

## Trusted source tagging

Trusted source event tagging can only be used with events generated by the Integrity Monitoring protection module.

The Integrity Monitoring module allows you to monitor system components and associated attributes on a computer for changes (changes include creation and deletion, as well as edits.) Among the components that you can monitor for changes are files, directories, groups, installed software, listening port numbers, processes, registry keys, and so on.

Trusted source event tagging is designed to reduce the number of events that need to be analyzed by automatically identifying events associated with authorized changes.

In addition to auto-tagging similar events, the integrity monitoring module allows you to tag events based on their similarity to events and data found on **Trusted Sources**. A trusted source can be one of the following:

- A **local trusted computer**
- The **Trend Micro Certified Safe Software Service**
- A **trusted common baseline**, which is a set of file states collected from a group of computers.

### Local trusted computer

A trusted computer is a computer to be used as a model computer that you know can only generate benign or harmless events. A target computer is a computer that you are monitoring for unauthorized or unexpected changes. The auto-tagging rule examines events on target computers and compares them to events from the trusted computer. If any events match, they are tagged with the tag defined in the auto-tagging rule.

You can establish auto-tagging rules that compare events on protected computers to events on a trusted computer. For example, a planned rollout of a patch can be applied to the trusted computer. The events associated with the application of the patch can be tagged as Patch X. Similar events raised on other systems can be auto-tagged and identified as acceptable changes and filtered out to reduce the number of events that need to be evaluated.

## Event matching algorithm

Integrity monitoring events contain information about transitions from one state to another. In other words, events contain *before* and *after* information. When comparing events, the auto-tagging engine will look for matching before and after states; if the two events share the same before and after states, the events are judged to be a match and a tag is applied to the second event. This also applies to creation and deletion events.

Remember that when using a trusted computer for trusted source event tagging, the events being tagged are events generated by integrity monitoring rules. This means that the integrity monitoring rules that are generating events on the target computer must also be running on the trusted source computer.

Trusted source computers must be scanned for malware before applying trusted source event tagging.

Utilities that regularly make modifications to the content of files on a system (prelinking on Linux, for example) can interfere with trusted source event tagging.

## Tag events based on a local trusted computer

1. Make sure the trusted computer is free of malware by running a full anti-malware scan.
2. Make sure the computers on which you want to auto-tag events are running the same (or some of the same) integrity monitoring rules as the trusted source computer.
3. In Deep Security Manager, go to **Events & Reports > Integrity Monitoring Events** and click **Auto-Tagging** in the toolbar.
4. In the **Auto-Tag Rules (Integrity Monitoring Events)** window, click **New Trusted Source** to display the **Tag Wizard**.
5. Select **Local Trusted Computer** and click **Next**.
6. From the list, select the computer that will be the trusted source and click **Next**.
7. Specify one or more tags to apply to events on target computers when they match events on this trusted source computer. Click **Next**.

   **Note:** You can enter the text for a new tag or select from a list of existing tags.

8. Identify the target computers whose events will be matched to those of the trusted source. Click **Next**.
9. Optionally, give the rule a name and click **Finish**.

## Tag events based on the Trend Micro Certified Safe Software Service

The Certified Safe Software Service is an allow list of known-good file signatures maintained by Trend Micro. This type of trusted source tagging will monitor target computers for file-related integrity monitoring events. When an event has been recorded, the file's signature (after the change) is compared to Trend Micro's list of known good file signatures. If a match is found, the event is tagged.

1. In Deep Security Manager, go to **Events & Reports > Integrity Monitoring Events** and click **Auto-Tagging** in the toolbar.
2. In the **Auto-Tag Rules (Integrity Monitoring Events)** window, click **New Trusted Source** to display the **Tag Wizard**.
3. Select **Certified Safe Software Service** and click **Next**.
4. Specify one or more tags to apply to events on target computers when they match the Certified Safe Software Service. Click **Next**.
5. Identify the target computers whose events will be matched to the Certified Safe Software Service. Click **Next**.
6. Optionally, give the rule a name and click **Finish**.

## Tag events based on a trusted common baseline

The trusted common baseline method compares events within a group of computers. A group of computers is identified and a common baseline is generated based on the files and system states targeted by the integrity monitoring rules in effect on the computers in the group. When an integrity monitoring event occurs on a computer within the group, the signature of the file after the change is compared to the common baseline. If the file's new signature has a match elsewhere in the common baseline, a tag is applied to the event. In trusted computer method, the before and after states of an integrity monitoring event are compared, but in the trusted common baseline method, only the after state is compared.

This method relies on all the computers in the common group being secure and free of malware. A full anti-malware scan should be run on all the computers in the group before the common baseline is generated.

When an integrity monitoring baseline is generated for a computer, Deep Security first checks if that computer is part of a trusted common baseline group. If it is, the computer's baseline data is included in the trusted common baseline for that group. For this reason, the trusted common baseline auto-tagging rule must be in place before any integrity monitoring rules have been applied to the computers in the common baseline group.

1. Make sure all the computers that will be in the group that will make up the trusted common baseline are free of malware by running a full anti-malware scan on them.
2. In Deep Security Manager, go to **Events & Reports > Integrity Monitoring Events** and click **Auto-Tagging** in the toolbar.
3. In the **Auto-Tag Rules (Integrity Monitoring Events)** window, click **New Trusted Source** to display the **Tag Wizard**.
4. Select **Trusted Common Baseline** and click **Next**.
5. Specify one or more tags to apply to events when they have a match in the trusted common baseline and click **Next**.
6. Identify the computers to include in the group used to generate the trusted common baseline. Click **Next**.
7. Optionally, give this rule a name and click **Finish**.

**Note:** Due to performance issues related to large amounts of baseline data, in the latest version of Deep Security Manager, **View Baseline** is not visible in the UI. For more information, see Database performance issue due to lots of Integrity Monitoring baseline data.

## Delete a tag

1. In an events list, right-click the events with the tag you want to delete, and select **Remove Tags**.
2. Select the tag you want to remove from **The Selected [Event Type] Event** or **Apply to selected similar [Event Type] Events**, and then click **Next**.
3. Optionally, add comments and click **Finish**.

# Reduce the number of logged events

To reduce the number of events being logged, the Deep Security Manager can be configured to operate in one of several **Advanced Logging Policy** modes. These modes are set in the **Computer or Policy editor**[1] on the **Settings > Advanced > Advanced Network Engine Settings** area.

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

The following table lists the types of events that are ignored in four of the more complex Advanced Logging Policy modes:

| Mode | Ignored Events |
|---|---|
| **Stateful and Normalization Suppression** | Out Of Connection<br>Invalid Flags<br>Invalid Sequence<br>Invalid ACK<br>Unsolicited UDP<br>Unsolicited ICMP<br>Out Of Allowed Policy<br>Dropped Retransmit |
| **Stateful, Normalization, and Frag Suppression** | Out Of Connection<br>Invalid Flags<br>Invalid Sequence<br>Invalid ACK<br>Unsolicited UDP<br>Unsolicited ICMP<br>Out Of Allowed Policy<br>CE Flags<br>Invalid IP<br>Invalid IP Datagram Length<br>Fragmented<br>Invalid Fragment Offset<br>First Fragment Too Small<br>Fragment Out Of Bounds<br>Fragment Offset Too Small<br>IPv6 Packet<br>Max Incoming Connections<br>Max Outgoing Connections<br>Max SYN Sent<br>License Expired<br>IP Version Unknown<br>Invalid Packet Info<br>Maximum ACK Retransmit<br>Packet on Closed Connection<br>Dropped Retransmit |
| **Stateful, Frag, and Verifier Suppression** | Out Of Connection<br>Invalid Flags<br>Invalid Sequence<br>Invalid ACK<br>Unsolicited UDP<br>Unsolicited ICMP<br>Out Of Allowed Policy<br>CE Flags<br>Invalid IP<br>Invalid IP Datagram Length |

| Mode | Ignored Events |
|---|---|
| | Fragmented<br>Invalid Fragment Offset<br>First Fragment Too Small<br>Fragment Out Of Bounds<br>Fragment Offset Too Small<br>IPv6 Packet<br>Max Incoming Connections<br>Max Outgoing Connections<br>Max SYN Sent<br>License Expired<br>IP Version Unknown<br>Invalid Packet Info<br>Invalid Data Offset<br>No IP Header<br>Unreadable Ethernet Header<br>Undefined<br>Same Source and Destination IP<br>Invalid TCP Header Length<br>Unreadable Protocol Header<br>Unreadable IPv4 Header<br>Unknown IP Version<br>Maximum ACK Retransmit<br>Packet on Closed Connection<br>Dropped Retransmit |
| **Tap Mode** | Out Of Connection<br>Invalid Flags<br>Invalid Sequence<br>Invalid ACK<br>Maximum ACK Retransmit<br>Packet on Closed Connection<br>Dropped Retransmit |

## Rank events to quantify their importance

The ranking system provides a way to quantify the importance of events. By assigning "asset values" to computers, and assigning severity or risk values to rules, the importance ("rank") of an event is calculated by multiplying the two values together. This allows you to sort events by rank.

**Note:** Unlike the other modules, Anti-Malware does not use asset values to rank event importance.

## Web Reputation event risk values

Risk values for Web Reputation events are linked to the three levels of risk used by the Web Reputation settings on the **General** tab of the **Web Reputation** page:

- **Dangerous:** corresponds to "A URL that has been confirmed as fraudulent or a known source of threats."
- **Highly Suspicious:** corresponds to "A URL that is suspected to be fraudulent or a known source of threats."
- **Suspicious:** corresponds to "A URL that is associated with spam or possibly compromised."
- **Blocked by Administrator:** A URL that is on the Web Reputation Service **Blocked** list.
- **Untested:** A URL that does not have a risk level.

## Firewall rule severity values

Severity values for Firewall rules are linked to their actions: Deny, Log Only, and Packet Rejection. (The latter refers to packets rejected because of a Firewall stateful configuration setting.) Use this panel to edit the severity values which will be multiplied by a computer's asset value to determine the rank of a Firewall event. (A Firewall rule's actions can be viewed and edited in the rule's **Properties** window.)

## Intrusion Prevention rule severity values

Intrusion Prevention rule severity values are linked to their severity levels: Critical, High, Medium, Low, or Error. Use this panel to edit their values which will be multiplied by a computer's asset value to determine the rank of an Intrusion Prevention event. An Intrusion Prevention rule's severity setting can be viewed in the rule's **Properties** window.

## Integrity Monitoring rule severity values

Integrity Monitoring rule severity values are linked to their severity levels: Critical, High, Medium, or Low. Use this panel to edit their values which will be multiplied by a computer's asset value to determine the rank of an Integrity Monitoring event. An Integrity Monitoring rule's severity can be viewed in the rule's **Properties** window.

### Log Inspection rule severity values

Log Inspection rule severity values are linked to their severity levels: Critical, High, Medium, or Low. Use this panel to edit their values which will be multiplied by a computer's asset value to determine the rank of a Log Inspection event. A Log Inspection rule's severity level can be viewed and edited from the rule's **Properties** window.

### Asset values

Asset values are not associated with any of their other properties like Intrusion Prevention rules or Firewall rules. Instead, asset values are properties in themselves. A computer's asset value can be viewed and edited from the computer's **Details** window. To simplify the process of assigning asset values, you can predefine some values that will appear in the **Asset Importance** list in the first page of the computer's **Details** window. To view existing predefined computer asset values, click the **View Asset Values** button in this panel. The **Asset Values** window displays the predefined settings. These values can be changed, and new ones can be created. (New settings will appear in the list for all computers.)

# Forward events to a Syslog or SIEM server

## Forward Deep Security events to a Syslog or SIEM server

You can send events to an external Syslog or Security Information and Event Management (SIEM) server. This can be useful for centralized monitoring, custom reporting, or to free local disk space on Deep Security Manager.

Even if you enable event forwarding to an external server, Deep Security Manager still records system and security events locally in order to display them in reports and graphs. Therefore, if you need to reduce disk space usage, event forwarding is not enough; you should also configure how long to keep events locally.

Alternatively, if you want to publish events to Amazon SNS, see "Set up Amazon Simple Notification Service" on page 1130.

Basic steps include the following:

1. "Allow event forwarding network traffic" on the next page
2. "Request a client certificate" on the next page

3. "Define a Syslog configuration" below
4. "Forward system events" on page 1071 and/or "Forward security events" on page 1071

## Allow event forwarding network traffic

All routers, firewalls, and security groups must allow inbound traffic from Deep Security Manager (and, for direct forwarding of security events, inbound traffic from agents) to your Syslog server. See also "Port numbers, URLs, and IP addresses" on page 478.

## Request a client certificate

If you want to forward events securely (over TLS), and if your Syslog server requires client authentication, then you must generate a *client* (not server) certificate signing request (CSR). Deep Security Manager uses this certificate to identify and authenticate itself when it connects as a client to the Syslog server. For details on how to request a client certificate, contact your certificate authority (CA).

Some Syslog servers do not accept self-signed server certificates (such as Deep Security Manager's default). A CA-signed client certificate is required.

Use either a CA that the Syslog server trusts, or an intermediate CA whose certificate was signed, directly or indirectly, by a trusted root CA (this is also known as a trust chain or signing chain).

Once you receive the signed certificate from your CA, to upload it to Deep Security Manager, continue with "Define a Syslog configuration" below.

## Define a Syslog configuration

Syslog configurations define the destination and settings that can be used when forwarding system or security events.

If you configured SIEM or Syslog settings before January 26th, 2017, they have been converted to Syslog configurations. Identical configurations were merged.

1. Go to **Policies > Common Objects > Other > Syslog Configurations**.
2. Click **New > New Configuration**.
3. On the **General** tab, configure the following:
   - **Name:** Unique name that identifies the configuration.
   - **Description:** Optional description of the configuration.

- **Log Source Identifier**: Optional identifier to use instead of Deep Security Manager's hostname.

  If Deep Security Manager is multi-node, each server node has a different hostname. Log source IDs can therefore be different. If you need the IDs to be the same regardless of hostname (for example, for filtering purposes), you can configure their shared log source ID here.

  This setting does not apply to events sent directly by Deep Security Agent, which always uses its hostname as the log source ID.

- **Server Name:** Hostname or IP address of the receiving Syslog or SIEM server.

- **Server Port:** Listening port number on the SIEM or Syslog server. For UDP, the IANA standard port number is 514. For TLS, it is usually port 6514. See also "Port numbers, URLs, and IP addresses" on page 478.

- **Transport:** Whether the transport protocol is secure (TLS) or not (UDP).

  With UDP, Syslog messages are limited to 64 KB. If the message is longer, data may be truncated.

  With TLS, the manager and Syslog server must trust each other's certificates. The connection from the manager to the Syslog server is encrypted with TLS 1.2, 1.1, or 1.0.

  TLS requires that you set **Agents should forward logs** to **Via the Deep Security Manager** (indirectly). Agents do not support forwarding with TLS.

- **Event Format:** Whether the log message's format is LEEF, CEF, or basic Syslog. See "Syslog message formats" on page 1073

  LEEF format requires that you set **Agents should forward logs** to **Via the Deep Security Manager** (indirectly).

  Basic Syslog format is not supported by Deep Security Anti-Malware, Web Reputation, Integrity Monitoring, and Application Control.

- **Include time zone in events:** Whether to add the full date (including year and time zone) to the event.

Example (selected): 2018-09-14T01:02:17.123+04:00.

Example (deselected): Sep 14 01:02:17.

Full dates require that you set **Agents should forward logs** to **Via the Deep Security Manager** (indirectly).

- **Facility:** Type of process with which the events will be associated. Syslog servers may prioritize or filter based on a log message's facility field. See also What are Syslog Facilities and Levels?

- **Agents should forward logs:** Whether to send events **Directly to the Syslog server** or **Via the Deep Security Manager** (indirectly).

  When forwarding logs directly to the Syslog server, agents use clear text UDP. Logs contain sensitive information about your security system. If logs will travel over an untrusted network such as the Internet, consider adding a VPN tunnel or similar to prevent reconnaissance and tampering.

  If you forward logs via the manager, they do not include Firewall and Intrusion Prevention packet data unless you configure Deep Security Manager to include it. For instructions, see Sending packet data to syslog via Deep Security Manager (DSM).

4. If the Syslog or SIEM server requires TLS clients to do client authentication (also called bilateral or mutual authentication; see "Request a client certificate" on page 1068), then on the **Credentials** tab, configure the following:
   - **Private Key:** Paste the private key of Deep Security Manager's client certificate.
   - **Certificate:** Paste the **client** certificate that Deep Security Manager will use to identify itself in TLS connections to the Syslog server. Use PEM, also known as Base64-encoded format.
   - **Certificate Chain:** If an intermediate CA signed the client certificate, but the Syslog server doesn't know and trust that CA, then paste CA certificates which prove a relationship to a trusted root CA. Press Enter between each CA certificate.
5. Click **Apply**.
6. If you selected the TLS transport mechanism, verify that both Deep Security Manager and the Syslog server can connect and trust each other's certificates.

   a. Click **Test Connection**.

      Deep Security Manager tries to resolve the hostname and connect. If that fails, an error message appears.

      If the Syslog or SIEM server certificate is not yet trusted by Deep Security Manager, the connection fails and an **Accept Server Certificate?** message should appear. The message shows the contents of the Syslog server's certificate.

   b. Verify that the Syslog server's certificate is correct, and then and click **OK** to accept it.

      The certificate is added to the manager's list of trusted certificates on **Administration > System Settings > Security**. Deep Security Manager can accept self-signed certificates.

   c. Click **Test Connection** again.

      Now the TLS connection should succeed.

7. Continue by selecting the events to forward. See "Forward system events" below and/or "Forward security events" below.

## Forward system events

Deep Security Manager generates system events, such as administrator logins or upgrading agent software.

1. Go to **Administration > System Settings > Event Forwarding**.
2. From **Forward System Events to a remote computer (via Syslog) using configuration**, either select an existing configuration or click **New**. For details, see "Define a Syslog configuration" on page 1068.
3. Click **Save**.

If Deep Security Manager is multi-node, system events are only sent from one node to avoid duplicates.

## Forward security events

Deep Security Agent protection features generate security events (such as detecting malware or triggering an IPS rule). You can forward events either:

- Directly
- Indirectly, via Deep Security Manager

Some event forwarding options require forwarding agent events indirectly, via Deep Security Manager.

Similarly to other policy settings, you can override event forwarding settings for specific policies or computers. See "Policies, inheritance, and overrides" on page 634.

1. Go to **Policies**.
2. Double-click the policy used by the computers.
3. Select **Settings**.
4. Select the **Event Forwarding** tab.
5. From **Period between sending of events**, select the frequency of the event forwarding.
6. From **Anti-Malware Syslog Configuration** and other protection modules' context menus, either select which Syslog configuration to use, click **Edit** to change it, select **None** to disable it, or click **New**. For details, see "Define a Syslog configuration" on page 1068.
7. Click **Save.**

## Troubleshoot event forwarding

### Failed to Send Syslog Message alert

If there is a problem with your Syslog configuration, you might see this alert:

```
Failed to Send Syslog Message
The Deep Security Manager was unable to forward messages to a Syslog Server.
Unable to forward messages to a Syslog Server
```

The alert also contains a link to the affected Syslog configuration. Click the link to open the configuration and then click **Test Connection** to get more diagnostic information. It will either indicate that the connection was successful or display an error message with more details about the cause.

### Can't edit Syslog configurations

If you can see the Syslog configurations but can't edit them, the role associated with your account might not have the appropriate rights. An administrator who is able to configure roles can check your permissions by going to **Administration > User Management**. Then select your name and click **Properties**. On the **Other Rights** tab, the **Syslog Configurations** setting controls your ability to edit Syslog configurations. For more information on users and roles, see "Add and manage users" on page 1410.

#### Can't see the Syslog configuration sections of Deep Security Manager

If you cannot see the Syslog configurations UI in Deep Security Manager, you may be a tenant in a multi-tenant environment where the primary tenant has disabled this feature or configured it for you.

#### Syslog not transferred due to an expired certificate

Valid certificates are required to connect securely via TLS. If you set up TLS client authentication and the certificate expires, messages are not sent to the Syslog server. To fix this problem, get a new certificate, update the Syslog configuration with the new certificate values, test the connection, and then save the configuration.

#### Syslog not delivered due to an expired or changed server certificate

Valid certificates are required to connect securely via TLS. If the Syslog server's certificate has expired or changed, open the Syslog configuration and click **Test Connection**. You are prompted to accept the new certificate.

#### Compatibility

Deep Security has been tested with the enterprise version of the following:

- IBM QRadar 7.2.8 Patch 3 (with the TLS protocol patch, PROTOCOL-TLSSyslog-7.2-20170104125004.noarch)
- HP ArcSight 7.2.2 (with a TLS Syslog-NG connector created using the ArcSight-7.2.2.7742.0-Connector tool)

Other standard Syslog software might work, but has not been verified.

## Syslog message formats

Common Event Format (CEF) and Log Event Extended Format (LEEF) log message formats are slightly different. For example, the **Source User** column in the UI corresponds to a field named `suser` in CEF; in LEEF, the same field is named `usrName` instead. Log message fields also vary by whether the event originated on Deep Security Agent or Deep Security Manager and which feature created the log message.

> **Note:** If your syslog messages are being truncated, it may be because you are using User Datagram Protocol (UDP). To prevent truncation, transfer your syslog messages over Transport

Layer Security (TLS) instead. For instructions on switching to TLS, see "Define a Syslog configuration" on page 1068.

Basic syslog format is not supported by the Anti-Malware, Web Reputation, Integrity Monitoring, and Application Control protection modules.

If the syslog messages are sent from the manager, there are several differences. In order to preserve the original Deep Security Agent hostname (the source of the event), a new extension (`dvc` or `dvchost`) is present. `dvc` is used if the hostname is an IPv4 address; `dvchost` is used for hostnames and IPv6 addresses. Additionally, the extension `TrendMicroDsTags` is used if the events are tagged. This applies only to auto-tagging with run on future, since events are forwarded via syslog only as they are collected by the manager. The product for logs relayed through the manager still reads "Deep Security Agent"; however, the product version is the version of the manager.

## CEF syslog message format

All CEF events include `dvc=IPv4 Address` or `dvchost=Hostname` (or the IPv6 address) for the purposes of determining the original Deep Security Agent source of the event. This extension is important for events sent from a Deep Security Virtual Appliance or Manager, since in this case the syslog sender of the message is not the originator of the event.

**Base CEF format:** CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

To determine whether the log entry comes from Deep Security Manager or Deep Security Agent, look at the Device Product field:

**Sample CEF Log Entry:** Jan 18 11:07:53 dsmhost CEF:0|Trend Micro|**Deep Security Manager**|<DSM version>|600|Administrator Signed In|4|suser=Master...

**Note:** Events that occur on a VM that is protected by a virtual appliance, but do not have an in-guest agent are still identified as coming from an agent.

To further determine what kind of rule triggered the event, look at the Signature ID and Name fields:

**Sample Log Entry:** Mar 19 15:19:15 root CEF:0|Trend Micro|Deep Security Agent|<DSA version>|**123**|**Out Of Allowed Policy**|5|cn1=1...

The Signature ID value indicates what kind of event has been triggered:

| Signature IDs | Description |
|---|---|
| 10 | Custom Intrusion Prevention (IPS) rule |
| 20 | Log-only Firewall rule |
| 21 | Deny Firewall rule |
| 30 | Custom Integrity Monitoring rule |
| 40 | Custom Log Inspection rule |
| 100-7499 | System events |
| 100-199 | Policy Firewall rule and Firewall stateful configuration |
| 200-299 | IPS internal errors |
| 300-399 | SSL/TLS events |
| 500-899 | IPS normalization |
| 1,000,000-1,999,999 | Trend Micro IPS rule. The signature ID is the same as the IPS rule ID. |
| 2,000,000-2,999,999 | Integrity Monitoring rule. The signature ID is the Integrity Monitoring rule ID + 1,000,000. |
| 3,000,000-3,999,999 | Log Inspection rule. The signature ID is the Log Inspection rule ID + 2,000,000. |
| 4,000,000-4,999,999 | Anti-Malware events. Currently, only these signature IDs are used:<br>• 4,000,000 - Anti-Malware - Real-Time Scan<br>• 4,000,001 - Anti-Malware - Manual Scan<br>• 4,000,002 - Anti-Malware - Scheduled Scan<br>• 4,000,003 - Anti-Malware - Quick Scan<br>• 4,000,010 - Anti-Spyware - Real-Time Scan<br>• 4,000,011 - Anti-Spyware - Manual Scan<br>• 4,000,012 - Anti-Spyware - Scheduled Scan<br>• 4,000,013 - Anti-Spyware - Quick Scan<br>• 4,000,020 - Suspicious Activity - Real-Time Scan<br>• 4,000,030 - Unauthorized Change - Real-Time Scan |
| 5,000,000-5,999,999 | Web Reputation events. Currently, only these signature IDs are used:<br>• 5,000,000 - Web Reputation - Blocked<br>• 5,000,001 - Web Reputation - Detect Only |
| 6,000,000-6,999,999 | Application Control events. Currently, only these signature IDs are used:<br>• 6,001,100 - Application Control - Detect Only, in block list<br>• 6,001,200 - Application Control - Detect Only, not in allow list<br>• 6,002,100 - Application Control - Blocked, in block list |

| Signature IDs | Description |
|---|---|
| | - 6,002,200 - Application Control – Blocked, not in allow list |
| 7,000,000-7,999,999 | Device Control events. Currently, only these signature IDs are used:<br>- 7,000,000 - Device Control - access unknown device was blocked<br>- 7,000,200 - Device Control - write unknown device was blocked<br>- 7,001,000 - Device Control - access USB device was blocked<br>- 7,001,200 - Device Control - write USB device was blocked<br>- 7,002,000 - Device Control - access mobile device was blocked<br>- 7,002,200 - Device Control - write mobile device was blocked |

Log entries do not always have all CEF extensions described in the event log format tables. CEF extensions also may not be always in the same order. If you are using regular expressions (regex) to parse the entries, make sure your expressions do not depend on each key-value pair to exist, or to be in a specific order.

Syslog messages are limited to 64 KB by the syslog protocol specification. If the message is longer, data may be truncated. The basic syslog format is limited to 1 KB.

## LEEF 2.0 syslog message format

**Base LEEF 2.0 format:** LEEF:2.0|Vendor|Product|Version|EventID|(Delimiter Character, optional if the Delimiter Character is tab)|Extension

**Sample LEEF 2.0 Log Entry (DSM System Event Log Sample):** LEEF:2.0|Trend Micro|Deep Security Manager|<DSA version>|192|cat=System name=Alert Ended desc=Alert: CPU Warning Threshold Exceeded\nSubject: 10.201.114.164\nSeverity: Warning sev=3 src=10.201.114.164 usrName=System msg=Alert: CPUWarning Threshold Exceeded\nSubject: 10.201.114.164\nSeverity:Warning TrendMicroDsTenant=Primary

## Events originating in the manager

### System event log format

**Base CEF Format:** CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

**Sample CEF Log Entry:** CEF:0|Trend Micro|Deep Security Manager|<DSM version>|600|User Signed In|3|src=10.52.116.160 suser=admin target=admin msg=User signed in from 2001:db8::5

**Base LEEF 2.0 format:** LEEF:2.0|Vendor|Product|Version|EventID|(Delimiter Character, optional if the Delimiter Character is tab)|Extension

**Sample LEEF 2.0 Log Entry:** LEEF:2.0|Trend Micro|Deep Security Manager|<DSA version>|192|cat=System name=Alert Ended desc=Alert: CPU Warning Threshold Exceeded\nSubject: 10.201.114.164\nSeverity: Warning sev=3 src=10.201.114.164 usrName=System msg=Alert: CPU Warning Threshold Exceeded\nSubject: 10.201.114.164\nSeverity: Warning TrendMicroDsTenant=Primary

LEEF format uses a reserved `sev` key to show severity and `name` for the Name value.

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| src | src | Source IP Address | Deep Security Manager IP address. | src=10.52.116.23 |
| suser | usrName | Source User | Deep Security Manager administrator's account. | suser=MasterAdmin |
| target | target | Target Entity | The subject of the event. It can be the administrator account logged into Deep Security Manager, or a computer. | target=MasterAdmin<br>target=server01 |
| targetID | targetID | Target Entity ID | The identifier added in the manager. | targetID=1 |
| targetType | targetType | Target Entity Type | The event target entity type. | targetType=Host |
| msg | msg | Details | Details of the system event. May | msg=User password incorrect for username MasterAdmin on an attempt |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | contain a verbose description of the event. | to sign in from 127.0.0.1 msg=A Scan for Recommendations on computer (localhost) has completed... |
| TrendMicroDsTags | TrendMicroDsTags | Event Tags | Deep Security event tags assigned to the event | TrendMicroDsTags=suspicious |
| TrendMicroDsTenant | TrendMicroDsTenant | Tenant Name | Deep Security tenant | TrendMicroDsTenant=Primary |
| TrendMicroDsTenantId | TrendMicroDsTenantId | Tenant ID | Deep Security tenant ID | TrendMicroDsTenantId=0 |
| TrendMicroDsReasonId | TrendMicroDsReasonId | Event reason ID | Indicates the reason ID for event descriptions. Each event has its own reason ID definition. | TrendMicroDsReasonId=1 |
| None | sev | Severity | The severity of the event. 1 is the least severe; 10 is the most severe. | sev=3 |
| None | cat | Category | Event category | cat=System |
| None | name | Name | Event name | name=Alert Ended |
| None | desc | Description | Event description | desc:Alert: CPU Warning Threshold Exceeded |

## Events originating in the agent

### Anti-Malware event format

**Base CEF format:** CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

**Sample CEF Log Entry:** CEF:0|Trend Micro|Deep Security Agent|<DSA version>|4000000|Eicar_test_file|6|cn1=1 cn1Label=Host ID dvchost=hostname cn2=205 cn2Label=Quarantine File Size cs6=ContainerImageName | ContainerName | ContainerID cs6Label=Container filePath=C:\\Users\\trend\\Desktop\\eicar.exe act=Delete result=Delete msg=Realtime TrendMicroDsMalwareTarget=N/A TrendMicroDsMalwareTargetType=N/TrendMicroDsFileMD5=44D88612FEA8A8F36DE82E1278ABB02F TrendMicroDsFileSHA1=3395856CE81F2B7382DEE72602F798B642F14140 TrendMicroDsFileSHA256=275A021BBFB6489E54D471899F7DB9D1663FC695EC2FE2A2C4538AABF651FD0F TrendMicroDsDetectionConfidence=95 TrendMicroDsRelevantDetectionNames=Ransom_CERBER.BZC;Ransom_CERBER.C;Ransom_CRYPNISCA.SM

**Base LEEF 2.0 format:** LEEF:2.0|Vendor|Product|Version|EventID|(Delimiter Character, optional if the Delimiter Character is tab)|Extension

**Sample LEEF Log Entry:** LEEF: 2.0|Trend Micro|Deep Security Agent|<DSA version>|4000030|cat=Anti-Malware name=HEU_AEGIS_CRYPT desc=HEU_AEGIS_CRYPT sev=6 cn1=241 cn1Label=Host ID dvc=10.0.0.1 TrendMicroDsTags=FS TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 filePath=C:\\Windows\\System32\\virus.exe act=Terminate msg=Realtime TrendMicroDsMalwareTarget=Multiple TrendMicroDsMalwareTargetType=File System TrendMicroDsFileMD5=1947A1BC0982C5871FA3768CD025453E#011 TrendMicroDsFileSHA1=5AD084DDCD8F80FBF2EE3F0E4F812E812DEE60C1#011 TrendMicroDsFileSHA256=25F231556700749F8F0394CAABDED83C2882317669DA2C01299B45173482FA6E TrendMicroDsDetectionConfidence=95 TrendMicroDsRelevantDetectionNames=Ransom_CERBER.BZC;Ransom_CERBER.C;Ransom_CRYPNISCA.SM

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| cn1 | cn1 | Host Identifier | The agent computer's internal unique identifier. | cn1=1 |
| cn1Label | cn1Label | Host ID | The name label for the field cn1. | cn1Label=Host ID |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| cn2 | cn2 | File Size | The size of the quarantine file. | cn2=100 |
| cn2Label | cn2Label | File Size | The name label for the field cn2. | cn2Label=Quarantine File Size |
| cs3 | cs3 | Infected Resource | The path of the spyware item. This field is only for spyware detection events. | cs3=C:\test\atse_samples\SPYW_Test_Virus.exe |
| cs3Label | cs3Label | Infected Resource | The name label for the field cs3. This field is only for spyware detection events. | cs3Label=Infected Resource |
| cs4 | cs4 | Resource Type | Resource Type values: | cs4=10 |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | 10=Files and Directories<br>11=System Registry<br>12=Internet Cookies<br>13=Internet URL Shortcut<br>14=Programs in Memory<br>15=Program Startup Areas<br>16=Browser Helper Object<br>17=Lay | |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | ered Service Provider<br>18=Hosts File<br>19=Windows Policy Settings<br>20=Browser<br>23=Windows Shell Setting<br>24=IE Downloaded Program Files<br>25=Add/Remove Programs<br>26=Services | |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | other= Other<br>For example, if there's a spyware file named spy.exe that creates a registry run key to keep its persistence after system reboot, there will be two items in the spyware report: the item for | |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | spy.exe has cs4=10 (Files and Directories), and the item for the run key registry has cs4=11 (System Registry).<br>This field is only for spyware detection events. | |
| cs4Label | cd4Label | Resource Type | The name label for the field cs4. This field is only for spywar | cs4Label=Resource Type |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | e detection events. | |
| cs5 | cs5 | Risk Level | Risk level values:<br>0=Very Low<br>25=Low<br>50=Medium<br>75=High<br>100=Very High<br>This field is only for spyware detection events. | cs5=25 |
| cs5Label | cs5Label | Risk Level | The name label for the field cs5. | cs5Label=Risk Level |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | This field is only for spyware detection events. | |
| cs6 | cs6 | Container | The image name of the Docker container, container name, and container ID where the malware was detected. | cs6=ContainerImageName \| ContainerName \| ContainerID |
| cs6Label | cs6Label | Container | The name label for the field cs6. | cs6Label=Container |
| cs7 | cs7 | Flow | Indicates whether the packets that triggered this event | cs7=FWD |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | were travelling with (forward) or against (reverse) the direction of traffic being monitored by the intrusion prevention rule.<br>Flow values:<br>FWD= Connection Flow<br>REV= Reverse Flow | |
| cs7Label | cs7Label | Flow | The name label for the field cs7. | cs7Label=Flow |
| filePath | filePath | File Path | The location of the | filePath=C:\\Users\\Mei\\Desktop\\virus.exe |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | malware file. | |
| act | act | Action | The action performed by the Anti-Malware engine. Possible values are: Deny Access, Quarantine, Delete, Pass, Clean, Terminate, and Unspecified. | act=Clean<br>act=Pass |
| result | result | Result | The result of the failed Anti-Malware action. | result=Passed<br>result=Deleted<br>result=Quarantined<br>result=Cleaned<br>result=Access Denied<br>result=Terminated<br>result=Log<br>result=Failed<br>result=Pass Failed<br>result=Delete Failed<br>result=Quarantine Failed<br>result=Clean Failed<br>result=Terminate Failed<br>result=Log Failed<br>result=Scan Failed<br>result=Passed (Scan Failed)<br>result=Quarantined (Scan Failed) |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | | result=Quarantine Failed (Scan Failed)<br>result=Deny Access (Scan Failed) |
| msg | msg | Message | The type of scan. Possible values are: Realtime, Scheduled, and Manual. | msg=Realtime<br>msg=Scheduled |
| dvc | dvc | Device address | The IPv4 address for cn1.<br>Does not appear if the source is an IPv6 address or hostname. (Uses dvchost instead.) | dvc=10.1.144.199 |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| dvchost | dvchost | Device hostname | The hostname or IPv6 address for cn1.<br>Does not appear if the source is an IPv4 address. (Uses dvc field instead.) | dvchost=www.example.com<br>dvchost=fe80::f018:a3c6:20f9:afa6%5 |
| TrendMicroDsBehaviorRuleID | TrendMicroDsBehaviorRuleID | Behavior monitoring rule ID | The behavior monitoring rule ID for internal malware case tracking. | BehaviorRuleID=CS913 |
| TrendMicroDsBehaviorType | TrendMicroDsBehaviorType | Behavior Monitori | The type of behavior monito | BehaviorType=Threat-Detection |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | ng type | ring event detected. | |
| TrendMicroDsTags | TrendMicroDsTags | Events tags | Deep Security event tags assigned to the event | TrendMicroDsTags=suspicious |
| TrendMicroDsTenant | TrendMicroDsTenant | Tenant name | Deep Security tenant | TrendMicroDsTenant=Primary |
| TrendMicroDsTenantId | TrendMicroDsTenantId | Tenant ID | Deep Security tenant ID | TrendMicroDsTenantId=0 |
| TrendMicroDsMalwareTarget | TrendMicroDsMalwareTarget | Target(s) | The file, process, or registry key (if any) that the malware was trying to affect. If the malware was trying to | TrendMicroDsMalwareTarget=N/A<br>TrendMicroDsMalwareTarget=C:\\Windows\\System32\\cmd.exe<br>TrendMicroDsMalwareTarget=HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings<br>TrendMicroDsMalwareTarget=Multiple |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | affect more than one, this field will contain the value "Multiple." | |
| TrendMicroDsMalwareTargetCount | TrendMicroDsMalwareTargetCount | Target count | The number of target files. | TrendMicroDsMalwareTargetCount=3 |
| TrendMicroDsMalwareTargetType | TrendMicroDsMalwareTargetType | Target Type | The type of system resource that this malware was trying to affect, such as the file system, a process, or Windo | TrendMicroDsMalwareTargetType=N/A<br>TrendMicroDsMalwareTargetType=Exploit<br>TrendMicroDsMalwareTargetType=File System<br>TrendMicroDsMalwareTargetType=Process<br>TrendMicroDsMalwareTargetType=Registry |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | ws registry. | |
| TrendMicroDsProcess | TrendMicroDsProcess | Process | Process Name | TrendMicroDsProcess= abc.exe |
| TrendMicroDsFileMD5 | TrendMicroDsFileMD5 | File MD5 | The MD5 hash of the file | TrendMicroDsFileMD5=1947A1BC0982C5871FA3768CD025453E |
| TrendMicroDsFileSHA1 | TrendMicroDsFileSHA1 | File SHA1 | The SHA1 hash of the file | TrendMicroDsFileSHA1=5AD084DDCD8F80FBF2EE3F0E4F812E812DEE60C1 |
| TrendMicroDsFileSHA256 | TrendMicroDsFileSHA256 | File SHA256 | The SHA256 hash of the file | TrendMicroDsFileSHA256=25F231556700749F8F0394CAABDED83C2882317669DA2C01299B45173482FA6E |
| TrendMicroDsDetectionConfidence | TrendMicroDsDetectionConfidence | Threat Probability | Indicates how closely (in %) the file matched the malware model | TrendMicroDsDetectionConfidence=95 |
| TrendMicroDsRelevantDetectionNames | TrendMicroDsRelevantDetectionNames | Probable Threat Type | Indicates the most likely type of threat contained in the file after Predictive Machin | TrendMicroDsRelevantDetectionNames=Ransom_CERBER.BZC;Ransom_CERBER.C;Ransom_CRYPNISCA.SM |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | e Learning compared the analysis to other known threats (separate by semicolon";" ) | |
| None | sev | Severity | The severity of the event. 1 is the least severe; 10 is the most severe. | sev=6 |
| None | cat | Category | Category | cat=Anti-Malware |
| None | name | Name | Event name | name=SPYWARE_KEYL_ACTIVE |
| None | desc | Description | Event description. Anti-Malware uses the event name as the description. | desc=SPYWARE_KEYL_ACTIVE |
| TrendMicroDsCommandLine | TrendMicroDsCommandLine | Comm | The comma | TrendMicroDsCommandLine=/tmp/orca-testkit-sample/testsys_m64 -u 1000 -g 1000 -U 1000 - |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | and Line | nds that the subject process executes | G 1000 -e cve_2017_16995 1 -d 4000000 |
| TrendMicroDsCve | TrendMicroDsCve | CVE | The CVE information, if the process behavior is identified in one of Common Vulnerabilities and Exposures. | TrendMicroDsCve=CVE-2016-5195,CVE-2016-5195,CVE-2016-5195 |
| TrendMicroDsMitre | TrendMicroDsMitre | MITRE | The MITRE information, if the process behavior is identified in one of MITRE attack scenarios. | TrendMicroDsMitre=T1068,T1068,T1068 |
| suser | suser | username | The user | suser=root |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | account name who triggered this event | |

### Application Control event format

**Base CEF format:** CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

**Example CEF Log Entry:** `CEF: 0|Trend Micro|Deep Security Agent|10.2.229|6001200|AppControl detectOnly|6|cn1=202 cn1Label=Host ID dvc=192.168.33.128 TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 fileHash=80D4AC182F97D2AB48EE4310AC51DA5974167C596D133D64A83107B9069745E0 suser=root suid=0 act=detectOnly filePath=/home/user1/Desktop/Directory1//heartbeatSync.sh fsize=20 aggregationType=0 repeatCount=1 cs1=notWhitelisted cs1Label=actionReason cs2=0CC9713BA896193A527213D9C94892D41797EB7C cs2Label=sha1 cs3=7EA8EF10BEB2E9876D4D7F7E5A46CF8D cs3Label=md5`

**Base LEEF 2.0 format:** LEEF:2.0|Vendor|Product|Version|EventID|(Delimiter Character, optional if the Delimiter Character is tab)|Extension

**Example LEEF Log Entry:** `LEEF:2.0|Trend Micro|Deep Security Agent|10.0.2883|60|`cat=AppControl name=blocked desc=blocked sev=6 cn1=2 cn1Label=Host ID dvc=10.203.156.39 TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 fileHash=E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855 suser=root suid=0 act=blocked filePath=/bin/my.jar fsize=123857 aggregationType=0 repeatCount=1 cs1=notWhitelisted cs1Label=actionReason

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| cn1 | cn1 | Host Identifier | The agent computer's internal | cn1=2 |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | unique identifier. | |
| cn1Label | cn1Label | Host ID | The name label for the field cn1. | cn1Label=Host ID |
| cs1 | cs1 | Reason | The reason why application control performed the specified action, such as "notWhitelisted" (the software did not have a matching rule, and application control was configured to block unrecognized software). | cs1=notWhitelisted |
| cs1Label | cs1Label | | The name label for the field cs1. | cs1Label=actionReason |
| cs2 | cs2 | | If it was calculated, the | cs2=156F4CB711FDBD668943711F853FB6DA89581AAD |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | SHA-1 hash of the file. | |
| cs2Label | cs2Label | | The name label for the field cs2. | cs2Label=sha1 |
| cs3 | cs3 | | If it was calculated, the MD5 hash of the file. | cs3=4E8701AC951BC4537F8420FDAC7EFBB5 |
| cs3Label | cs3Label | | The name label for the field cs3. | cs3Label=md5 |
| act | act | Action | The action performed by the Application Control engine. Possible values are: Blocked, Allowed. | act=blocked |
| dvc | dvc | Device address | The IPv4 address for cn1.<br>Does not appear if the source is an IPv6 address or | dvc=10.1.1.10 |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | hostname. (Uses dvchost instead.) | |
| dvchost | dvchost | Device host name | The hostname or IPv6 address for cn1.<br>Does not appear if the source is an IPv4 address. (Uses dvc field instead.) | dvchost=www.example.com<br>dvchost=2001:db8::5 |
| suid | suid | User ID | The account ID number of the user name. | suid=0 |
| suser | suser | User Name | The name of the user account that installed the software on the protected computer. | suser=root |
| TrendMicroDsTenant | TrendMicroDsTenant | Tenant name | Deep Security tenant name. | TrendMicroDsTenant=Primary |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| TrendMicroDsTenantId | TrendMicroDsTenantId | Tenant ID | Deep Security tenant ID number. | TrendMicroDsTenantId=0 |
| fileHash | fileHash | File hash | The SHA 256 hash that identifies the software file. | fileHash=E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855 |
| filePath | filePath | File Path | The location of the malware file. | filePath=/bin/my.jar |
| fsize | fsize | File Size | The file size in bytes. | fsize=16 |
| aggregationType | aggregationType | Aggregation Type | An integer that indicates how the event is aggregated:<br>• 0: The event is not aggregated | aggregationType=2 |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | - 1: The event is aggregated based on file name, path, and event type.<br>- 2: The event is aggregated based | |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | on event type.<br>For information, about event aggregation, see "View Application Control event logs" on page 1005. | |
| repeatCount | repeatCount | Repeat Count | The number of occurrences of the event. Non-aggregated events have a value of 1. Aggregated events have a value of 2 or | repeatCount=4 |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | more. | |
| None | sev | Severity | The severity of the event. 1 is the least severe; 10 is the most severe. | sev=6 |
| None | cat | Category | Category | cat=AppControl |
| None | name | Name | Event name | name=blocked |
| None | desc | Description | Event description. Application Control uses the action as the description. | desc=blocked |

**Firewall event log format**

**Base CEF format:** CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

**Sample CEF Log Entry:** CEF:0|Trend Micro|Deep Security Agent|<DSA version>|20|Log for TCP Port 80|0|cn1=1 cn1Label=Host ID dvc=hostname act=Log dmac=00:50:56:F5:7F:47 smac=00:0C:29:EB:35:DE TrendMicroDsFrameType=IP src=192.168.126.150 dst=72.14.204.147 out=1019 cs3=DF MF cs3Label=Fragmentation Bits proto=TCP spt=49617 dpt=80 cs2=0x00 ACK PSH cs2Label=TCP Flags cnt=1 TrendMicroDsPacketData=AFB...

**Sample LEEF Log Entry:** LEEF:2.0|Trend Micro|Deep Security Agent|<DSA version>|21|cat=Firewall name=Remote Domain Enforcement (Split Tunnel) desc=Remote Domain Enforcement (Split Tunnel) sev=5 cn1=37 cn1Label=Host ID dvchost=www.example.com TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 act=Deny dstMAC=67:BF:1B:2F:13:EE srcMAC=78:FD:E7:07:9F:2C TrendMicroDsFrameType=IP src=10.0.110.221 dst=105.152.185.81 out=177 cs3= cs3Label=Fragmentation Bits proto=UDP srcPort=23 dstPort=445 cnt=1 TrendMicroDsPacketData=AFB...

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| act | act | Action | | act=Log<br>act=Deny |
| cn1 | cn1 | Host Identifier | The agent computer's internal unique identifier. | cn1=113 |
| cn1Label | cn1Label | Host ID | The name label for the field cn1. | cn1Label=Host ID |
| cnt | cnt | Repeat Count | The number of times this event was sequentially repeated. | cnt=8 |
| cs2 | cs2 | TCP Flags | | cs2=0x10 ACK<br>cs2=0x14 ACK RST |
| cs2Label | cs2Label | TCP Flags | The name label for the field cs2. | cs2Label=TCP Flags |
| cs3 | cs3 | Packet Fragmentation Information | | cs3=DF<br>cs3=MF<br>cs3=DF MF |
| cs3Label | cs3Label | Fragmentation Bits | The name label for the field cs3. | cs3Label=Fragmentation Bits |
| cs4 | cs4 | ICMP Type and Code | (For the ICMP protocol only) The ICMP type and code, delimited by a space. | cs4=11 0<br>cs4=8 0 |
| cs4Label | cs4Label | ICMP | The name label for the field cs4. | cs4Label=ICMP Type and Code |
| dmac | dstMAC | Destination MAC Address | MAC address of the | dmac= 00:0C:29:2F:09:B3 |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | destination computer's network interface. | |
| dpt | dstPort | Destination Port | (For TCP and UDP protocol only) Port number of the destination computer's connection or session. | dpt=80<br>dpt=135 |
| dst | dst | Destination IP Address | IP address of the destination computer. | dst=192.168.1.102<br>dst=10.30.128.2 |
| in | in | Inbound Bytes Read | (For inbound connections only) Number of inbound bytes read. | in=137<br>in=21 |
| out | out | Outbound Bytes Read | (For outbound connections only) Number of outbound bytes read. | out=216<br>out=13 |
| proto | proto | Transport protocol | Name of the transport protocol used. | proto=tcp<br>proto=udp<br>proto=icmp |
| smac | srcMAC | Source MAC Address | MAC address of the source computer's network interface. | smac= 00:0E:04:2C:02:B3 |
| spt | srcPort | Source Port | (For TCP and UDP protocol | spt=1032<br>spt=443 |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | only) Port number of the source computer's connection or session. | |
| src | src | Source IP Address | The packet's source IP address at this event. | src=192.168.1.105<br>src=10.10.251.231 |
| TrendMicroDsFrameType | TrendMicroDsFrameType | Ethernet frame type | Connection ethernet frame type. | TrendMicroDsFrameType=IP<br>TrendMicroDsFrameType=ARP<br>TrendMicroDsFrameType=RevARP<br>TrendMicroDsFrameType=NetBEUI |
| TrendMicroDsPacketData | TrendMicroDsPacketData | Packet data | The packet data, represented in Base64. | TrendMicroDsPacketData=AFB... |
| dvc | dvc | Device address | The IPv4 address for cn1.<br>Does not appear if the source is an IPv6 address or hostname. (Uses dvchost instead.) | dvc=10.1.144.199 |
| dvchost | dvchost | Device host name | The hostname | dvchost=exch01.example.com<br>dvchost=2001:db8::5 |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | or IPv6 address for cn1.<br>Does not appear if the source is an IPv4 address. (Uses dvc field instead.) | |
| TrendMicroDsTags | TrendMicroDsTags | Event Tags | Deep Security event tags assigned to the event | TrendMicroDsTags=suspicious |
| TrendMicroDsTenant | TrendMicroDsTenant | Tenant Name | Deep Security tenant | TrendMicroDsTenant=Primary |
| TrendMicroDsTenantId | TrendMicroDsTenantId | Tenant ID | Deep Security tenant ID | TrendMicroDsTenantId=0 |
| None | sev | Severity | The severity of the event. 1 is the least severe; 10 is the most severe. | sev=5 |
| None | cat | Category | Category | cat=Firewall |
| None | name | Name | Event name | name=Remote Domain Enforcement (Split Tunnel) |
| None | desc | Description | Event description. Firewall events use the event name as the description. | desc=Remote Domain Enforcement (Split Tunnel) |

### Integrity Monitoring log event format

**Base CEF format:** CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

**Sample CEF Log Entry:** CEF:0|Trend Micro|Deep Security Agent|<DSA version>|30|New Integrity Monitoring Rule|6|cn1=1 cn1Label=Host ID dvchost=hostname act=updated filePath=c:\\windows\\message.dll suser=admin sproc=C:\\Windows\\System32\\notepad.exe msg=lastModified,sha1,size

**Base LEEF 2.0 format:** LEEF:2.0|Vendor|Product|Version|EventID|(Delimiter Character, optional if the Delimiter Character is tab)|Extension

**Sample LEEF Log Entry:** LEEF:2.0|Trend Micro|Deep Security Agent|<DSA version>|2002779|cat=Integrity Monitor name=Microsoft Windows - System file modified desc=Microsoft Windows - System file modified sev=8 cn1=37 cn1Label=Host ID dvchost=www.example.com TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 act=updated suser=admin sproc=C:\\Windows\\System32\\notepad.exe

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| act | act | Action | The action detected by the integrity rule. Can contain: created, updated, deleted or renamed. | act=created<br>act=deleted |
| cn1 | cn1 | Host Identifier | The agent computer's internal unique identifier. | cn1=113 |
| cn1Label | cn1Label | Host ID | The name label for the field cn1. | cn1Label=Host ID |
| filePath | filePath | Target Entity | The integrity rule target entity. May contain a file or directory path, registry key, etc. | filePath=C:\WINDOWS\system32\drivers\etc\hosts |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| suser | suser | Source User | Account of the user who changed the file being monitored. | suser=WIN-038M7CQDHIN\Administrator |
| sproc | sproc | Source Process | The name of the event's source process. | sproc=C:\\Windows\\System32\\notepad.exe |
| msg | msg | Attribute changes | (For "renamed" action only) A list of changed attribute names. If "Relay via Manager" is selected, all event action types include a full description. | msg=lastModified,sha1,size |
| oldfilePath | oldfilePath | Old target entity | (For "renamed" action only) The previous integrity rule target entity to capture the rename action from the previous target entity to the new, which is recorded in the filePath field. | oldFilePath=C:\WINDOWS\system32\logfiles\ds_agent.log |
| dvc | dvc | Device address | The IPv4 address for cn1.<br>Does not appear if the | dvc=10.1.144.199 |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | source is an IPv6 address or hostname. (Uses dvchost instead.) | |
| dvchost | dvchost | Device host name | The hostname or IPv6 address for cn1.<br>Does not appear if the source is an IPv4 address. (Uses dvc field instead.) | dvchost=www.example.com<br>dvchost=2001:db8::5 |
| TrendMicroDsTags | TrendMicroDsTags | Events tags | Deep Security event tags assigned to the event | TrendMicroDsTags=suspicious |
| TrendMicroDsTenant | TrendMicroDsTenant | Tenant name | Deep Security tenant | TrendMicroDsTenant=Primary |
| TrendMicroDsTenantId | TrendMicroDsTenantId | Tenant ID | Deep Security tenant ID | TrendMicroDsTenantId=0 |
| None | sev | Severity | The severity of the event. 1 is the least severe; 10 is the most severe. | sev=8 |
| None | cat | Category | Category | cat=Integrity Monitor |
| None | name | Name | Event name | name=Microsoft Windows - System file modified |
| None | desc | Description | Event description. | desc=Microsoft Windows - System file modified |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | Integrity Monitoring uses the event name as the description. | |
| entityType | entityType | EntityType | The type of entity that an Integrity Monitoring event applies to Directory, File, Group, InstalledSoftware, Port, Process, RegistryKey, RegistryValue, Service, User, or Wql | entityType=File |

**Intrusion Prevention event log format**

**Base CEF format:** CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

**Sample CEF Log Entry:** CEF:0|Trend Micro|Deep Security Agent|<DSA version>|1001111|Test Intrusion Prevention Rule|3|cn1=1 cn1Label=Host ID dvchost=hostname dmac=00:50:56:F5:7F:47 smac=00:0C:29:EB:35:DE TrendMicroDsFrameType=IP src=192.168.126.150 dst=72.14.204.105 out=1093 cs3=DF MF cs3Label=Fragmentation Bits proto=TCP spt=49786 dpt=80 cs2=0x00 ACK PSH cs2Label=TCP Flags cnt=1 act=IDS:Reset cn3=10 cn3Label=Intrusion Prevention Packet Position cs5=10 cs5Label=Intrusion Prevention Stream Position cs6=8 cs6Label=Intrusion Prevention Flags TrendMicroDsPacketData=R0VUIC9zP3...

**Base LEEF 2.0 format:** LEEF:2.0|Vendor|Product|Version|EventID|(Delimiter Character, optional if the Delimiter Character is tab)|Extension

**Sample LEEF Log Entry:** LEEF:2.0|Trend Micro|Deep Security Agent|<DSA version>|1000940|cat=Intrusion Prevention name=Sun Java RunTime Environment Multiple Buffer Overflow Vulnerabilities desc=Sun Java RunTime Environment Multiple Buffer Overflow Vulnerabilities sev=10 cn1=6 cn1Label=Host ID dvchost=exch01 TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 dstMAC=55:C0:A8:55:FF:41 srcMAC=CA:36:42:B1:78:3D

TrendMicroDsFrameType=IP src=10.0.251.84 dst=56.19.41.128 out=166 cs3= cs3Label=Fragmentation Bits proto=ICMP srcPort=0 dstPort=0 cnt=1 act=IDS:Reset cn3=0 cn3Label=DPI Packet Position cs5=0 cs5Label=DPI Stream Position cs6=0 cs6Label=DPI Flags TrendMicroDsPacketData=R0VUIC9zP3...

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| act | act | Action | (IPS rules written before Deep Security version 7.5 SP1 could additionally perform Insert, Replace, and Delete actions. These actions are no longer performed. If an older IPS Rule is triggered which still attempts to perform those actions, the event will indicate that the rule was applied in detect-only mode.) | act=Block |
| cn1 | cn1 | Host Identifier | The agent computer's internal unique identifier. | cn1=113 |
| cn1Label | cn1Label | Host ID | The name label for | cn1Label=Host ID |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | the field cn1. | |
| cn3 | cn3 | Intrusion Prevention Packet Position | Position within packet of data that triggered the event. | cn3=37 |
| cn3Label | cn3Label | Intrusion Prevention Packet Position | The name label for the field cn3. | cn3Label=Intrusion Prevention Packet Position |
| cnt | cnt | Repeat Count | The number of times this event was sequentially repeated. | cnt=8 |
| cs1 | cs1 | Intrusion Prevention Filter Note | (Optional) A note field which can contain a short binary or text note associated with the payload file. If the value of the note field is all printable ASCII characters, it will be logged as text with spaces converted to underscores. If it contains | cs1=Drop_data |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | binary data, it will be logged using Base-64 encoding. | |
| cs1Label | cs1Label | Intrusion Prevention Note | The name label for the field cs1. | cs1Label=Intrusion Prevention Note |
| cs2 | cs2 | TCP Flags | (For the TCP protocol only) The raw TCP flag byte followed by the URG, ACK, PSH, RST, SYN and FIN fields may be present if the TCP header was set. | cs2=0x10 ACK<br>cs2=0x14 ACK RST |
| cs2Label | cs2Label | TCP Flags | The name label for the field cs2. | cs2Label=TCP Flags |
| cs3 | cs3 | Packet Fragmentation Information | | cs3=DF<br>cs3=MF<br>cs3=DF MF |
| cs3Label | cs3Label | Fragmentation Bits | The name label for the field cs3. | cs3Label=Fragmentation Bits |
| cs4 | cs4 | ICMP Type and Code | (For the ICMP protocol only) The ICMP type | cs4=11 0<br>cs4=8 0 |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | and code stored in their respective order delimited by a space. | |
| cs4Label | cs4Label | ICMP | The name label for the field cs4. | cs4Label=ICMP Type and Code |
| cs5 | cs5 | Intrusion Prevention Stream Position | Position within stream of data that triggered the event. | cs5=128<br>cs5=20 |
| cs5Label | cs5Label | Intrusion Prevention Stream Position | The name label for the field cs5. | cs5Label=Intrusion Prevention Stream Position |
| cs6 | cs6 | Intrusion Prevention Filter Flags | A combined value that includes the sum of the flag values:<br>1 - Data truncated - Data could not be logged.<br>2 - Log Overflow - Log overflowed after this log.<br>4 - Suppressed - Logs threshold suppresse | The following example would be a summed combination of 1 (Data truncated) and 8 (Have Data):<br>cs6=9 |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | d after this log.<br>8 - Have Data - Contains packet data<br>16 - Reference Data - References previously logged data. | |
| cs6Label | cs6Label | Intrusion Prevention Flags | The name label for the field cs6. | cs6=Intrusion Prevention Filter Flags |
| dmac | dstMAC | Destination MAC Address | Destination computer network interface MAC address. | dmac= 00:0C:29:2F:09:B3 |
| dpt | dstPort | Destination Port | (For TCP and UDP protocol only) Destination computer connection port. | dpt=80<br>dpt=135 |
| dst | dst | Destination IP Address | Destination computer IP Address. | dst=192.168.1.102<br>dst=10.30.128.2 |
| xff | xff | X-Forwarded-For | The IP address of the last hub in the X- | xff=192.168.137.1 |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | Forwarded-For header. This is typically originating IP address, beyond the proxy that may exist. See also the src field. To include xff in events, enable the "1006540 - Enable X-Forwarded-For HTTP Header Logging" Intrusion Prevention rule. | |
| in | in | Inbound Bytes Read | (For inbound connections only) Number of inbound bytes read. | in=137<br>in=21 |
| out | out | Outbound Bytes Read | (For outbound connections only) Number of outbound bytes read. | out=216<br>out=13 |
| proto | proto | Transport protocol | Name of the connection | proto=tcp<br>proto=udp<br>proto=icmp |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | transport protocol used. | |
| smac | srcMAC | Source MAC Address | Source computer network interface MAC address. | smac= 00:0E:04:2C:02:B3 |
| spt | srcPort | Source Port | (For TCP and UDP protocol only) Source computer connection port. | spt=1032<br>spt=443 |
| src | src | Source IP Address | Source computer IP Address. This is the IP of the last proxy server, if it exists, or the client IP. See also the xff field. | src=192.168.1.105<br>src=10.10.251.231 |
| TrendMicroDsFrameType | TrendMicroDsFrameType | Ethernet frame type | Connection ethernet frame type. | TrendMicroDsFrameType=IP<br>TrendMicroDsFrameType=ARP<br>TrendMicroDsFrameType=RevARP<br>TrendMicroDsFrameType=NetBEUI |
| TrendMicroDsPacketData | TrendMicroDsPacketData | Packet data | The packet data, represented in Base64. | TrendMicroDsPacketData=R0VUIC9zP3... |
| dvc | dvc | Device | The IPv4 | dvc=10.1.144.199 |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | address | address for cn1.<br>Does not appear if the source is an IPv6 address or hostname. (Uses dvchost instead.) | |
| dvchost | dvchost | Device host name | The hostname or IPv6 address for cn1.<br>Does not appear if the source is an IPv4 address. (Uses dvc field instead.) | dvchost=www.example.com<br>dvchost=2001:db8::5 |
| TrendMicroDsTags | TrendMicroDsTags | Event tags | Deep Security event tags assigned to the event | TrendMicroDsTags=Suspicious |
| TrendMicroDsTenant | TrendMicroDsTenant | Tenant name | Deep Security tenant name | TrendMicroDsTenant=Primary |
| TrendMicroDsTenantId | TrendMicroDsTenantId | Tenant ID | Deep Security tenant ID | TrendMicroDsTenantId=0 |
| None | sev | Severity | The | sev=10 |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | severity of the event. 1 is the least severe; 10 is the most severe. | |
| None | cat | Category | Category | cat=Intrusion Prevention |
| None | name | Name | Event name | name=Sun Java RunTime Environment Multiple Buffer Overflow Vulnerabilities |
| None | desc | Description | Event description. Intrusion Prevention events use the event name as the description. | desc=Sun Java RunTime Environment Multiple Buffer Overflow Vulnerabilities |

**Log Inspection event format**

**Base CEF format:** CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

**Sample CEF Log Entry:** CEF:0|Trend Micro|Deep Security Agent|<DSA version>|3002795|Microsoft Windows Events|8|cn1=1 cn1Label=Host ID dvchost=hostname cs1Label=LI Description cs1=Multiple Windows Logon Failures fname=Security src=127.0.0.1 duser=(no user) shost=WIN-RM6HM42G65V msg=WinEvtLog Security: AUDIT_FAILURE (4625): Microsoft-Windows-Security-Auditing: (no user): no domain: WIN-RM6HM42G65V: An account failed to log on. Subject: ..

**Base LEEF 2.0 format:** LEEF:2.0|Vendor|Product|Version|EventID|(Delimiter Character, optional if the Delimiter Character is tab)|Extension

**Sample LEEF Log Entry:** LEEF:2.0|Trend Micro|Deep Security Agent|<DSA version>|3003486|cat=Log Inspection name=Mail Server - MDaemon desc=Server Shutdown. sev=3 cn1=37 cn1Label=Host ID dvchost=exch01.example.com TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 cs1=Server Shutdown. cs1Label=LI Description fname= shost= msg=

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| cn1 | cn1 | Host Identifier | The agent computer's internal unique identifier. | cn1=113 |
| cn1Label | cn1Label | Host ID | The name label for the field cn1. | cn1Label=Host ID |
| cs1 | cs1 | Specific Sub-Rule | The Log Inspection sub-rule which triggered this event. | cs1=Multiple Windows audit failure events |
| cs1Label | cs1Label | LI Description | The name label for the field cs1. | cs1Label=LI Description |
| duser | duser | User Information | (If parse-able username exists) The name of the target user initiated the log entry. | duser=(no user)<br>duser=NETWORK SERVICE |
| fname | fname | Target entity | The Log Inspection rule target entity. May contain a file or directory path, registry key, etc. | fname=Application<br>fname=C:\Program Files\CMS\logs\server0.log |
| msg | msg | Details | Details of the Log Inspection event. May contain a verbose description of the detected log event. | msg=WinEvtLog: Application: AUDIT_ FAILURE(20187): pgEvent: (no user): no domain: SERVER01: Remote login failure for user 'xyz' |
| shost | shost | Source Hostname | Source computer hostname. | shost=webserver01.corp.com |
| src | src | Source IP | Source | src=192.168.1.105 |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | Address | computer IP address. | src=10.10.251.231 |
| dvc | dvc | Device address | The IPv4 address for cn1.<br>Does not appear if the source is an IPv6 address or hostname. (Uses dvchost instead.) | dvc=10.1.144.199 |
| dvchost | dvchost | Device host name | The hostname or IPv6 address for cn1.<br>Does not appear if the source is an IPv4 address. (Uses dvc field instead.) | dvchost=www.example.com<br>dvchost=2001:db8::5 |
| TrendMicroDsTags | TrendMicroDsTags | Events tags | Deep Security event tags assigned to the event | TrendMicroDsTags=suspicious |
| TrendMicroDsTenant | TrendMicroDsTenant | Tenant name | Deep Security tenant | TrendMicroDsTenant=Primary |
| TrendMicroDsTenantId | TrendMicroDsTenantId | Tenant ID | Deep Security tenant ID | TrendMicroDsTenantId=0 |
| None | sev | Severity | The severity of the event. 1 is the least | sev=3 |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | severe; 10 is the most severe. | |
| None | cat | Category | Category | cat=Log Inspection |
| None | name | Name | Event name | name=Mail Server - MDaemon |
| None | desc | Description | Event description. | desc=Server Shutdown |

**Web Reputation event format**

**Base CEF format:** CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

**Sample CEF Log Entry:** CEF:0|Trend Micro|Deep Security Agent|<DSA version>|5000000|WebReputation|5|cn1=1 cn1Label=Host ID dvchost=hostname request=example.com msg=Blocked By Admin

**Base LEEF 2.0 format:** LEEF:2.0|Vendor|Product|Version|EventID|(Delimiter Character, optional if the Delimiter Character is tab)|Extension

**Sample LEEF Log Entry:** LEEF:2.0|Trend Micro|Deep Security Agent|<DSA version>|5000000|cat=Web Reputation name=WebReputation desc=WebReputation sev=6 cn1=3 cn1Label=Host ID dvchost=exch01.example.com TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 request=http://yw.olx5x9ny.org.it/HvuauRH/eighgSS.htm msg=Suspicious

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| cn1 | cn1 | Host Identifier | The agent computer's internal unique identifier. | cn1=1 |
| cn1Label | cn1Label | Host ID | The name label for the field cn1. | cn1Label=Host ID |
| request | request | Request | The URL of the request. | request=http://www.example.com/index.php |
| msg | msg | Message | The type of action. Possible values are: | msg=Realtime<br>msg=Scheduled |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | Realtime, Scheduled, and Manual. | |
| dvc | dvc | Device address | The IPv4 address for cn1.<br>Does not appear if the source is an IPv6 address or hostname. (Uses dvchost instead.) | dvc=10.1.144.199 |
| dvchost | dvchost | Device host name | The hostname or IPv6 address for cn1.<br>Does not appear if the source is an IPv4 address. (Uses dvc field instead.) | dvchost=www.example.com<br>dvchost=2001:db8::5 |
| TrendMicroDsTags | TrendMicroDsTags | Events tags | Deep Security event tags assigned to the event | TrendMicroDsTags=suspicious |
| TrendMicroDsTenant | TrendMicroDsTenant | Tenant name | Deep Security tenant | TrendMicroDsTenant=Primary |
| TrendMicroDsTen | TrendMicroDsTen | Tenant | Deep | TrendMicroDsTenantId=0 |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| antId | antId | ID | Security tenant ID | |
| None | sev | Severity | The severity of the event. 1 is the least severe; 10 is the most severe. | sev=6 |
| None | cat | Category | Category | cat=Web Reputation |
| None | name | Name | Event name | name=WebReputation |
| None | desc | Description | Event description. Web Reputation uses the event name as the description. | desc=WebReputation |

**Device Control event format**

**Base CEF format:** CEF:Version|Device Vendor|Device Product|Device Version|Signature ID|Name|Severity|Extension

**Sample CEF Log Entry:** CEF:0|Trend Micro|Deep Security Agent|50.0.1063|7000000|Device Control DeviceControl|6|cn1=1 cn1Label=Host ID dvchost=test-hostname TrendMicroDsTenant=tenantName TrendMicroDsTenantId=1 device=deviceName processName=processName1 fileName=/tmp/some_path2 vendor=vendorName serial=aaaa-bbbb-cccc model=modelName computerName=computerName domainName=computerDomain deviceType=0 permission=0

**Base LEEF 2.0 format:** LEEF:2.0|Vendor|Product|Version|EventID|(Delimiter Character, optional if the Delimiter Character is tab)|Extension

**Sample LEEF Log Entry:** LEEF:2.0|Trend Micro|Deep Security Agent|50.0.1063|7000000|cat=Device Control name=DeviceControl desc=DeviceControl sev=6 cn1=1 cn1Label=Host ID dvchost=test-hostname TrendMicroDsTenant=tenantName TrendMicroDsTenantId=1 device=deviceName processName=processName1 fileName=/tmp/some_path2 vendor=vendorName serial=aaaa-bbbb-cccc model=modelName computerName=computerName domainName=computerDomain deviceType=0 permission=0

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| cn1 | cn1 | Host Identifier | The agent computer's internal unique identifier. | cn1=1 |
| cn1Label | cn1Label | Host ID | The name label for the field cn1. | cn1Label=Host ID |
| dvchost | dvchost | Device host name | The hostname or IPv6 address for cn1.<br>Does not appear if the source is an IPv4 address. (Uses dvc field instead.) | dvchost=www.example.com dvchost=2001:db8::5 |
| TrendMicroDsTenant | TrendMicroDsTenant | Tenant name | Deep Security tenant | TrendMicroDsTenant=Primary |
| TrendMicroDsTenantId | TrendMicroDsTenantId | Tenant ID | Deep Security tenant ID | TrendMicroDsTenantId=0 |
| device | device | Device Name | The device that was accessed. | device=Sandisk_USB |
| processName | processName | Process Name | The process name. | processName=someProcess.exe |
| fileName | fileName | File Name | The file name that was accessed. | fileName=E:\somepath\a.exe |
| vendor | vendor | Vendor Name | The vendor name of the device. | vendor=sandisk |
| serial | serial | Serial Number | The serial number of | serial=aaa-bbb-ccc |

| CEF Extension Field | LEEF Extension Field | Name | Description | Examples |
|---|---|---|---|---|
| | | | the device. | |
| model | model | Model | The product name of the device. | model=A270_USB |
| computerName | computerName | Computer Name | The computer name. | computerName=Jonh_ Computer |
| domainName | domainName | Domain Name | The domain name. | domainName=CompanyDomain |
| deviceType | deviceType | Device Type | The device type of the device<br>USB_ STORAGE_ DEVICE(1)<br>MOBILE_ DEVICE(2) | deviceType=1 |
| permission | permission | Permission | The block reason of the access<br>BLOCK(0)<br>READ_ ONLY(2) | permission=0 |

## Configure Red Hat Enterprise Linux to receive event logs

### Set up a Syslog on Red Hat Enterprise Linux 8 or later

The following steps describe how to configure rsyslog on Red Hat Enterprise Linux 8 and later versions to receive logs from Deep Security:

1. Log in as root.
2. Execute the following command:

   ```
   vi /etc/rsyslog.conf
   ```
3. Uncomment the following lines near the top of the `rsyslog.conf` to change them from

   ```
    #module(load="imudp")
   #input(type="imudp" port="514")

   #module(load="imtcp")
   #input(type="imtcp" port="514")
   ```

to

```
 module(load="imudp")
 input(type="imudp" port="514")

 module(load="imtcp")
 input(type="imtcp" port="514")
```

4. Add the following two lines of text to the end of the `rsyslog.conf`:
   - `#Save Deep Security Manager logs to DSM.log`
   - `Local4.* /var/log/DSM.log`

     You may need to replace `Local4` with another value, depending on your manager settings.
5. Save the file and exit.
6. Create the `/var/log/DSM.log` file by typing `touch /var/log/DSM.log`
7. Set the permissions on the DSM log so that syslog can write to it.
8. Save the file and exit.
9. Restart syslog by executing the following command:

   ```
   systemctl restart rsyslog
   ```

When Syslog is functioning, the logs are populated in `/var/log/DSM.log`

## Set up a Syslog on Red Hat Enterprise Linux 6 or 7

The following steps describe how to configure rsyslog on Red Hat Enterprise Linux 6 or 7 to receive logs from Deep Security:

1. Log in as root.
2. Execute the following command:
   `vi /etc/rsyslog.conf`
3. Uncomment the following lines near the top of the `rsyslog.conf` to change them from

   ```
    #$ModLoad imudp
    #$UDPServerRun 514

    #$ModLoad imtcp
    #$InputTCPServerRun 514
   ```

to

```
 $ModLoad imudp
 $UDPServerRun 514

 $ModLoad imtcp
 $InputTCPServerRun 514

```

4. Add the following two lines of text to the end of the `rsyslog.conf`:
   - `#Save Deep Security Manager logs to DSM.log`
   - `Local4.* /var/log/DSM.log`

   > **Note:** You may need to replace `Local4` with another value, depending on your manager settings.

5. Save the file and exit.
6. Create the `/var/log/DSM.log` file by typing `touch /var/log/DSM.log`
7. Set the permissions on the DSM log so that syslog can write to it.
8. Save the file and exit.
9. Restart syslog by executing the following command:

   ```
   service rsyslog restart
   ```

When Syslog is functioning, the logs are populated in `/var/log/DSM.log`

## Set up a Syslog on Red Hat Enterprise Linux 5

The following steps describe how to configure Syslog on Red Hat Enterprise Linux 5 to receive logs from Deep Security:

1. Log in as root.
2. Execute the following command:
   `vi /etc/syslog.conf`
3. Add the following two lines of text to the end of the `syslog.conf` :
   - `#Save Deep Security Manager logs to DSM.log`
   - `Local4.* /var/log/DSM.log`

   > **Note:** You may need to replace `Local4` with another value, depending on your manager settings.

4. Save the file and exit.

5. Create the `/var/log/DSM.log` file by typing `touch /var/log/DSM.log`
6. Set the permissions on the DSM log so that syslog can write to it.
7. Execute the following command:

   :

   ```
   vi /etc/sysconfig/syslog
   ```
8. Modify the line `SYSLOGD_OPTIONS` and add a `-r` to the options.
9. Save the file and exit.
10. Restart syslog by executing the following command:

    ```
    /etc/init.d/syslog restart
    ```

When Syslog is functioning, the logs are populated in `/var/log/DSM.log`

# Set up Amazon Simple Notification Service

## Set up Amazon Simple Notification Service

If you have an AWS account, you can take advantage of Amazon Simple Notification Service (SNS) to publish notifications about Deep Security events and deliver them to subscribers.

To set up Amazon SNS, do the following:

1. "Configure AWS authentication" below.
2. "Create an Amazon SNS topic" on page 1132.
3. "Enable SNS" on page 1132.
4. "Create subscriptions" on page 1133.

### Configure AWS authentication

To access Amazon SNS, Deep Security needs to be authenticated through either an AWS Identity and Access Management (IAM) role or AWS access keys.

#### Use an IAM role

If your Deep Security Manager is running on an AWS EC2 instance, you can use an IAM role for authentication. This method provides automatic credential rotation and improved security.

1. In the AWS IAM console, create an IAM role with SNS publish permissions.
2. Attach the following policy to the role:

   ```
   {
           "Version": "2012-10-17",
           "Statement": [
                   {
                   "Action": [
                           "sns:Publish"
                   ],
                   "Effect": "Allow",
                   "Resource": "*"
                   }
           ]
   }
   ```

   If you want to limit publishing rights to a single topic, you can replace `"Resource":"*"` with `"Resource":"TOPIC ARN"`.

3. Attach the IAM role to your Deep Security Manager EC2 instance.

When you configure event forwarding, Deep Security will automatically detect and use this IAM role for authentication.

#### Use AWS access keys

If your Deep Security Manager is not running on AWS EC2, or if you prefer to use access keys, create an AWS user with the appropriate permissions for SNS. Save the access key and secret key for the user, as you will need them to "Enable SNS" on the next page.

The AWS user needs the `sns:Publish` permission on all SNS topics to which Deep Security will publish. The following is an example of a policy with this permission:

```
{
        "Version": "2012-10-17",
        "Statement": [
                {
                "Action": [
                        "sns:Publish"
                ],
                "Effect": "Allow",
```

```
                    "Resource": "*"
                    }
            ]
    }
```

If you want to limit publishing rights to a single topic, you can replace `"Resource":"*"` with `"Resource":"TOPIC ARN"`.

For more information, see Controlling user access to your AWS account and Amazon SNS API permissions: Actions and resources reference.

## Create an Amazon SNS topic

In AWS, create an SNS topic where the events will be published. For instructions, see Creating an Amazon SNS topic. Save the SNS Topic ARN, as you will need it to "Enable SNS" below.

## Enable SNS

1. In Deep Security Manager, go to **Administration** > **System Settings** > **Event Forwarding**.
2. In the **Amazon SNS** section, select **Publish Events to Amazon Simple Notification Service**.
3. Configure authentication based on the authentication method you selected:
   - If an IAM role was used, Deep Security will automatically detect the IAM role attached to your EC2 instance. The **Access key** and **Secret key** fields can be left empty.
   - If access keys were used, enter the **Access key** and **Secret key** of the AWS user.
4. Enter the **SNS Topic ARN** to which events will be sent. This is the ARN that you previously saved.
5. Select the types of events you want to forward to SNS. This automatically generates a JSON SNS configuration.

   Note that IAM roles are recommended for EC2 deployments, as this provides automatic credential rotation, eliminates the need to manage static access keys, and improves security.

6. Optionally, you can also click **Edit JSON SNS configuration** to edit the JSON SNS configuration directly if you want to filter the events in greater detail and configure the forwarding instructions for each filter. For details on the configuration language, see "SNS configuration in JSON format" on the next page.

If you edit the JSON, the event selection becomes unavailable. If you want to select or deselect any of the events, you can click **Revert to basic SNS configuration**, but any configurations you have made to the JSON SNS configuration will be discarded.

7. Click **Save**.

### Create subscriptions

Now that SNS is enabled and events are being published to the topic, go to the Amazon SNS console and subscribe to the topic to access the events. There are several ways that you can subscribe to events, including email, SMS, and Lambda endpoints.

Note that Lambda is not available in all AWS regions.

## SNS configuration in JSON format

You can edit the JSON configuration that is used when you have enabled event forwarding to Amazon SNS topics. It defines which conditions an event must meet in order to be published to a topic. The configuration language is modeled after Amazon's Policy language for SNS.

Each field is specified below. Basic SNS configuration looks like:

```
{
  "Version": "2014-09-24",
  "Statement": [statement1, statement2, ...]
}
```

For examples, see "Example SNS configurations" on page 1147.

### Version

The **Version** element specifies the version of the configuration language.

**Note:** The only currently valid value of "Version" is the string "2014-09-24".

```
"Version": "2014-09-24",
```

## Statement

The **Statement** element is an array of individual statements. Each individual statement is a distinct JSON object giving the SNS topic to send to if an event meets given conditions.

```
"Statement": [{...}, {...}, ...]
```

An individual statement has the form:

```
{
  "Topic": "destination topic",
  "Condition": {conditions event must meet to be published to the
destination topic}
}
```

### Topic

The **Topic** element must be the Amazon Resource Name of the SNS Topic to publish to.

```
"Topic": "arn:aws:sns:us-east-1:012345678901:myTopic"
```

### Condition

The **Condition** element is the most complex part of the configuration. It contains one or more conditions an event must match in order to be published to the topic.

Each condition can have one or more key-value pairs that the event must match (or not match, depending on the type of condition) to be included in the topic. Keys are any valid event property. (For event properties, see "Events in JSON format" on page 1149). Valid values vary by key. Some keys support multiple values.

```
"Condition": {
  "ConditionName": {
    "key1": [value1, value2],
    "key2": value3
  },
  "ConditionName2": {
    "key3": [value4]
  },
  ...
}
```

Valid condition names and their syntax are described below.

## Bool

The **Bool** condition performs Boolean matching. To match, an event must have a property with the desired Boolean value. If the property in the event exists but is not itself a Boolean value, the property is tested as follows:

- Numbers equal to 0 evaluate to false. Numbers not equal to 0 evaluate to true.
- Empty strings and the special strings "false" and "0" evaluate to false. Other strings evaluate to true.
- Any other property value in an event cannot be converted to a Boolean and will not match.

Allows for multiple values? No

The following example shows a configuration that publishes events that have a "DetectOnly" property with a value false:

```
  {
    "Version": "2014-09-24",
    "Statement": [
      {
        "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
        "Condition": {
          "Bool": {
            "DetectOnly": false
          }
        }
      }
    ]
```

```
}
```

## Exists

The **Exists** condition tests for the existence or non-existence of a property in an event. The value of the property is not considered.

Allows for multiple values? No

The following example shows a configuration that publishes events when the event has the property "Severity" but does not have the property "Title":

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "Exists": {
          "Severity": true,
          "Title": false
        }
      }
    }
  ]
}
```

## IpAddress

The **IpAddress** condition tests the value of an event's property is an IP address in a range given in CIDR format, or exactly equals a single IP address.

Allows for multiple values? Yes

The following example shows a configuration that publishes events when the event has the property "DestinationIP" with an IP address in the range 10.0.1.0/24, or to 10.0.0.5:

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "IpAddress": {
          "DestinationIP": ["10.0.1.0/24", "10.0.0.5"]
        }
      }
    }
  ]
}
```

## NotIpAddress

The **NotIpAddress** condition tests the value of an event's property is not an IP address in any of the specified IP address ranges.

Allows for multiple values? Yes

The following example shows a configuration that publishes events when the event has the property "DestinationIP" with an IP address not in the range 10.0.0.0/8:

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "NotIpAddress": {
          "DestinationIP": "10.0.0.0/8"
        }
      }
    }
  ]
}
```

## NumericEquals

The **NumericEquals** condition tests the numeric value of an event's property equals one or more desired values. If the property in the event exists but is not itself a numeric value, the property is tested as follows:

- Strings are converted to numbers. Strings that cannot be converted to numbers will not match.
- Any other property value in an event cannot be converted to a number and will not match.

Allows for multiple values? Yes

The following example shows a configuration that publishes events when the event has the property "Protocol" with the value 6 or 17:

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "NumericEquals": {
          "Protocol": [6, 17]
        }
      }
    }
  ]
}
```

## NumericNotEquals

The **NumericNotEquals** condition tests the numeric value of an event's property is not equal to any one of an undesired set of values.

Allows for multiple values? Yes

The following example shows a configuration that publishes events when the event has the property "Protocol" not equal to 6, and the property "Risk" not equal to 2 or 3:

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "NumericNotEquals": {
          "Protocol": 6,
          "Risk" : [2, 3]
        }
      }
    }
  ]
}
```

## NumericGreaterThan

The **NumericGreaterThan** condition tests the numeric value of an event's property is strictly greater than a desired value. If the property in the event exists but is not itself a numeric value it is converted to a number as described for NumericEquals.

Allows for multiple values? No

The following example shows a configuration that publishes events when the event has the property "Protocol" with the value greater than 6:

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "NumericGreaterThan": {
          "Protocol": 6
        }
      }
    }
  ]
}
```

## NumericGreaterThanEquals

The **NumericGreaterThanEquals** condition tests the numeric value of an event's property is greater than or equal to a desired value. If the property in the event exists but is not itself a numeric value it is converted to a number as described for NumericEquals.

Allows for multiple values? No

The following example shows a configuration that publishes events when the event has the property "Number" with a value greater than or equal to 600:

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "NumericGreaterThanEquals": {
          "Number": 600
        }
      }
      }
    ]
  }
```

## NumericLessThan

The **NumericLessThan** condition tests the numeric value of an event's property is strictly less than a desired value. If the property in the event exists but is not itself a numeric value it is converted to a number as described for NumericEquals.

Allows for multiple values? No

The following example shows a configuration that publishes events when the event has the property "Number" with a value greater than 1000:

```
  {
    "Version": "2014-09-24",
    "Statement": [
      {
        "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
        "Condition": {
          "NumericLessThan": {
            "Number": 1000
          }
        }
      }
    ]
  }
```

## NumericLessThanEquals

The **NumericLessThanEquals** condition tests the numeric value of an event's property is less than or equal to a desired value. If the property in the event exists but is not itself a numeric value it is converted to a number as described for NumericEquals.

Allows for multiple values? No

The following example shows a configuration that publishes events when the event has the property "Number" with a value less than or equal to 500:

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "NumericLessThanEquals": {
          "Number": 500
        }
      }
    }
  ]
}
```

## StringEquals

The **StringEquals** condition tests the string value of an event's property is strictly equal to or more desired values.

Allows for multiple values? Yes

The following example shows a configuration that publishes events when the event has the property "EventType" equal to "SystemEvent" and property "TargetType" equal to "User" or "Role":

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "StringEquals": {
          "EventType": ["SystemEvent"],
          "TargetType" : ["User", "Role"]
        }
      }
    }
  ]
}
```

## StringNotEquals

The **StringNotEquals** condition tests the string value of an event's property does not equal any of an undesired set of values.

Allows for multiple values? Yes

The following example shows a configuration that publishes events when the event has the property "EventType" not equal to "PacketLog" or "IntegrityEvent":

```
  {
    "Version": "2014-09-24",
    "Statement": [
      {
        "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
        "Condition": {
          "StringNotEquals": {
            "EventType": ["PacketLog", "IntegrityEvent"]
          }
        }
      }
    ]
  }
```

## StringEqualsIgnoreCase

The **StringEqualsIgnoreCase** condition is the same as the StringEquals condition, except string matching is performed in a case-insensitive manner.

## StringNotEqualsIgnoreCase

The **StringNotEqualsIgnoreCase** condition is the same as the StringNotEquals condition, except string matching is performed in a case-insensitive manner.

## StringLike

The **StringLike** condition tests the string value of an event's property is equal to or more desired values, where the desired values may include the wildcard '*' to match any number of characters or '?' to match a single character. String comparisons are case-sensitive.

Allows for multiple values? Yes

The following example shows a configuration that publishes events when the event has the property "Title" which contains the string "User" or "Role":

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "StringLike": {
          "Title": ["*User*", "*Role*"]
        }
      }
    }
  ]
}
```

## StringNotLike

The **StringNotLike** condition tests that the string value of an event's property is not equal to any of an undesired set of values, where the values may include the wildcard '*' to match any number of characters or '?' to match a single character. String comparisons are case-sensitive.

Allows for multiple values? Yes

The following example shows a configuration that publishes all events except the "System Settings Saved" event:

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "StringNotLike": {
          "Title":"System Settings Saved"
        }
      }
    }
  ]
}
```

The next example shows a configuration that publishes events when the event has the property "Title" that does not start with "User" and does not end with "Created":

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "StringNotLike": {
          "Title": ["User*", "*Created"]
        }
      }
    }
  ]
}
```

## Multiple statements vs. multiple conditions

If you create multiple statements for the same SNS topic, those statements are evaluated as if they are joined by "or". If a statement contains multiple conditions, those conditions are evaluated as if they are joined by "and".

### Multiple statements

This is an example of what not to do. The first statement says to forward all events other than "System Settings Saved". The second statement says to forward all "System Settings Saved" events. The result is that all events will be forwarded because any event will match either the condition in the first statement **or** the one in the second statement:

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "StringNotLike" : {
          "Title" : "System Settings Saved"
        }
      }
    },
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "StringLike" : {
          "Title" : "System Settings Saved"
        }
      }
    }
  ]
}
```

### Multiple conditions

This is another example of what not to do. The first condition says to forward all events other than "System Settings Saved". The second condition says to forward all "System Settings Saved" events. The result is that no events will be forwarded because no events will match both the condition in the first statement **and** the one in the second statement:

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "StringNotLike" : {
          "Title" : "System Settings Saved"
        },
        "StringLike" : {
          "Title" : "System Settings Saved"
        }
      }
    }
  ]
}
```

## Example SNS configurations

These configurations send matching events for some specific scenarios. For more event property names and values that you can use to filter SNS topics, see "Events in JSON format" on page 1149.

### Send all critical intrusion prevention events to an SNS topic

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:myTopic",
      "Condition": {
        "NumericEquals": {
          "Severity": 4
        },
        "StringEquals" : {
          "EventType" : "PayloadLog"
        }
      }
    }
  ]
}
```

### Send different events to different SNS topics

This example shows sending all system events to one topic and all integrity monitoring events to a different topic.

```
{
  "Version": "2014-09-24",
  "Statement": [
    {
      "Topic": "arn:aws:sns:us-east-
1:012345678901:systemEventsTopic",
      "Condition": {
        "StringEquals" : {
          "EventType" : "SystemEvent"
        }
      }
    },
    {
      "Topic": "arn:aws:sns:us-east-1:012345678901:integrityTopic",
      "Condition": {
        "StringEquals" : {
          "EventType" : "IntegrityEvent"
        }
      }
    }
  ]
}
```

## Events in JSON format

When published to Amazon SNS, events are sent in the SNS `Message` as an array of JSON objects that are encoded as strings. Each object in the array is one event.

Valid properties vary by the type of event. For example, `MajorVirusType` is a valid property only for Deep Security Anti-Malware events, not system events etc. Valid property values vary for each property. For examples, see "Example events in JSON format" on page 1176.

Event property values can be used to filter which events are published to the SNS topic. For details, see "SNS configuration in JSON format" on page 1133.

### Valid event properties

**Note:** Some events don't have all of the properties that usually apply to their event type.

| Property Name | Data Type | Description | Applies To Event Type(s) |
|---|---|---|---|
| ACRulesetID | Integer | The unique identifier of the Application Control Ruleset applied to the computer where the event was detected. | Application Control events |
| Action | String (enum) | Action taken for the application control event, such as "Execution of Software Blocked by Rule", "Execution of Unrecognized Software Allowed" (due to detect-only mode) or "Execution of Unrecognized Software Blocked". | Application Control events |
| Action | Integer (enum) | Action taken for the firewall event. "Detect Only" values | Firewall events |

| Property Name | Data Type | Description | Applies To Event Type(s) |
|---|---|---|---|
| | | show what would have happened if the rule had been enabled. 0=Unknown, 1=Deny, 6=Log Only, 0x81=Detect Only: Deny. | |
| Action | Integer (enum) | Action taken for the Intrusion Prevention event. 0=Unknown, 1=Deny, 2=Reset, 3=Insert, 4=Delete, 5=Replace, 6=Log Only, 0x81=Detect Only: Deny, 0x82=Detect Only: Reset, 0x83=Detect Only: Insert, 0x84=Detect Only: Delete, 0x85=Detect Only: Replace. | Intrusion Prevention events |
| ActionBy | String | Name of the Deep Security Manager user who performed the event, or "System" if the event was not generated by a user. | System events |
| ActionReasonDesc | String | The reason the Action was blocked. | Application Control events |
| ActionString | String | Conversion of Action to a readable string. | Firewall events, Intrusion Prevention events |
| AdministratorID | Integer | Unique identifier of the Deep Security user who performed an action. Events generated by the system and not by a user will not have an identifier. | System events |
| AggregationType | Integer (enum) | Whether or not the Application Control event occurred repeatedly. If "AggregationType" is not "0", | Application Control events |

| Property Name | Data Type | Description | Applies To Event Type(s) |
|---|---|---|---|
| | | then the number of occurrences is in "RepeatCount." 0=Not aggregated, 1=Aggregated based on file name, path and event type, 2=Aggregated based on event type | |
| AMTarget | String | The file, process, or registry key (if any) that the malware was trying to affect. If the malware was trying to affect more than one, this field will contain the value "Multiple." | Anti-Malware events |
| AMTargetCount | Integer | The number of target files. | Anti-Malware events |
| AMTargetType | Integer | The numeric code for the type of system resources that this malware was trying to affect. For the descriptive version, see AMTargetTypeString. 0=Unknown, 1=Process, 2=Registry, 3=File System, 4=Invoke, 5=Exploit, 6=API, 7=Memory, 8=Network Connection, 9=Uncategorized | Anti-Malware events |
| AMTargetTypeString | String | The type of system resource that this malware was trying to affect, such as the file system, a process, or Windows registry. | Anti-Malware events |
| ATSEDDetectionLevel | Integer | The detection level of document exploit protection. | Anti-Malware events |
| ApplicationType | String | Name of the network application type associated with the Intrusion Prevention rule, if available. | Intrusion Prevention events |

| Property Name | Data Type | Description | Applies To Event Type(s) |
|---|---|---|---|
| BehaviorRuleId | String | The behavior monitoring rule ID for internal malware case tracking. | Anti-Malware events |
| BehaviorType | String | The type of behavior monitoring event detected. | Anti-Malware events |
| BlockReason | Integer (enum) | A reason that corresponds to the Action. 0=Unknown, 1=Blocked due to rule, 2=Blocked due to unrecognized | Application Control events |
| Change | Integer (enum) | What type of change was made to a file, process, registry key, etc. for an Integrity Monitoring event. 1=Created, 2=Updated, 3=Deleted, 4=Renamed. | Integrity Monitoring events |
| ChangeString | String | What type of change was made to a file, process, registry key, etc. for an Integrity Monitoring event: Created, Updated, Deleted, or Renamed. | Integrity Monitoring events |
| CommandLine | String | The commands that the subject process executed. | Anti-Malware events |
| ContainerID | String | ID of the container where the event occurred. | Anti-Malware events, Intrusion Prevention events, Firewall events |
| ContainerImageName | String | Image name of the Docker container where the malware was found. | Anti-Malware events |
| ContainerName | String | Name of the container where | Anti-Malware |

| Property Name | Data Type | Description | Applies To Event Type(s) |
|---|---|---|---|
| | | the event occurred. | events, Intrusion Prevention events, Firewall events |
| CreationTime | String (Date) | The creation time of the infected file. | Anti-Malware events |
| Cve | String | The CVE information, if the process behavior is identified in one of Common Vulnerabilities and Exposures. | Anti-Malware events |
| DataIndex | Integer | A unique ID for packet data. | Intrusion Prevention events |
| Description | String | Description of the change made to the entity (created, deleted, updated) along with details about the attributes changed. | Integrity Monitoring events |
| Description | String | Brief description of what happened during an event. | System events |
| DestinationIP | String (IP) | The IP address of the destination of a packet. | Firewall events, Intrusion Prevention events |
| DestinationMAC | String (MAC) | The MAC address of the destination of a packet. | Firewall events, Intrusion Prevention events |
| DestinationPort | Integer | The network port number a packet was sent to. | Firewall events, |

| Property Name | Data Type | Description | Applies To Event Type(s) |
|---|---|---|---|
| | | | Intrusion Prevention events |
| DetectionCategory | Integer (enum) | The detection category for a web reputation event. 12=User Defined, 13=Custom, 91=Global. | Web Reputation events |
| DetectOnly | Boolean | Whether or not the event was returned with the Detect Only flag turned on. If true, this indicates that the URL was not blocked, but access was detected. | Web Reputation events |
| Direction | Integer (enum) | Network packet direction. 0=Incoming, 1=Outgoing. | Firewall events, Intrusion Prevention events |
| DirectionString | String | Conversion Direction to a readable string. | Firewall events, Intrusion Prevention events |
| DriverTime | Integer | The time the log was generated as recorded by the driver. | Firewall events, Intrusion Prevention events |
| EndLogDate | String (Date) | The last log date recorded for repeated events. Will not be present for events that did not repeat. | Firewall events, Intrusion Prevention events |
| EngineType | Integer | The Anti-Malware engine type. | Anti-Malware events |

| Property Name | Data Type | Description | Applies To Event Type(s) |
|---|---|---|---|
| EngineVersion | String | The Anti-Malware engine version. | Anti-Malware events |
| EntityType | String (enum) | The type of entity an integrity monitoring event applies to: Directory, File, Group, InstalledSoftware, Port, Process, RegistryKey, RegistryValue, Service, User, or Wql | Integrity Monitoring events |
| ErrorCode | Integer | Error code for malware scanning events. If non-zero the scan failed, and the scan action and scan result fields contain more details. | Anti-Malware events |
| EventID | Integer | The identifier of the event. Identifiers are unique per event type, but events of different types may share the same identifier. For example, it is possible for events with both EventType firewall and ips to have EventID equal to 1. **The combination of EventID, EventType and TenantID are required to completely, uniquely identify an event in Deep Security.** Note that this property is not related to the "Event ID" property of a System Event in the Deep Security Manager. | All event types |
| EventType | String (enum) | The type of the event. One of: "SystemEvent", "PacketLog", "PayloadLog", "AntiMalwareEvent", "WebReputationEvent", "IntegrityEvent", "LogInspectionEvent", "AppControlEvent". | All event types |

| Property Name | Data Type | Description | Applies To Event Type(s) |
|---|---|---|---|
| FileName | String | File name of the software that was allowed or blocked, such as "script.sh". (The full path is separate, in "Path".) | Application Control events |
| FileSHA1 | String | The filesha1 (Secure Hash Algorithm 1 result) of the infected file. | Anti-Malware events |
| FileSHA256 | String | The filesha256 of the infected file. | Anti-Malware events |
| FileSize | Integer | File size of the software that was allowed or blocked | Application Control events |
| Flags | String | Flags recorded from a network packet; a space-separated list of strings. | Firewall events, Intrusion Prevention events |
| Flow | Integer (enum) | Network connection flow. Possible values: -1=Not Applicable, 0=Connection Flow, 1=Reverse Flow | Firewall events, Intrusion Prevention events |
| FlowString | String | Conversion of Flow to a readable string. | Firewall events, Intrusion Prevention events |
| ForwardedSrc | Array (Byte) | The source information of a forwarded packet | Intrusion Prevention events |
| Frame | Integer (enum) | Frame type. -1=Unknown, 2048=IP, 2054=ARP, 32821=REVARP, 33169=NETBEUI, 0x86DD=IPv6 | Firewall events, Intrusion Prevention events |

| Property Name | Data Type | Description | Applies To Event Type(s) |
|---|---|---|---|
| FrameString | String | Conversion of Frame to a readable string. | Firewall events, Intrusion Prevention events |
| GroupID | String | The group ID, if any, of the user account that tried to start the software, such as "0". | Application Control events |
| GroupName | String | The group name, if any, of the user account that tried to start the software, such as "root". | Application Control events |
| HostAgentVersion | String | The version of the Deep Security Agent that was protecting the computer where the event was detected. | Application Control events, Anti-Malware events, Web Reputation events, Integrity Monitoring events, Log Inspection events, Firewall events, Intrusion Prevention events |
| HostAgentGUID | String | The global unique identifier (GUID) of the Deep Security Agent when activated with the Deep Security Manager. | Anti-Malware events, Application Control events, Firewall events, Integrity Monitoring events, |

| Property Name | Data Type | Description | Applies To Event Type(s) |
|---|---|---|---|
| | | | Intrusion Prevention events, Log Inspection events, Web Reputation events |
| HostAssetValue | Integer | The asset value assigned to the computer at the time the event was generated. | Anti-Malware events, Web Reputation events, Integrity Monitoring events, Log Inspection events, Firewall events, Intrusion Prevention events, Application Control events |
| HostCloudType | String | The cloud service provider where the Deep Security Agent is hosted. | Anti-Malware events, Application Control events, Firewall events, Integrity Monitoring events, Intrusion Prevention events, Log Inspection events, Web Reputation events |
| HostGUID | String | The global unique identifier (GUID) of the Deep Security | Anti-Malware |

| Property Name | Data Type | Description | Applies To Event Type(s) |
|---|---|---|---|
| | | Agent. | events, Application Control events, Firewall events, Integrity Monitoring events, Intrusion Prevention events, Log Inspection events, Web Reputation events |
| HostGroupID | Integer | The unique identifier of the Computer Group of the computer where the event was detected. | Application Control events, Anti-Malware events, Web Reputation events, Integrity Monitoring events, Log Inspection events, Firewall events, Intrusion Prevention events |
| HostGroupName | String | The name of the Computer Group of the computer where the event was detected. Note that Computer Group names may not be unique. | Application Control events, Anti-Malware events, Web Reputation events, Integrity Monitoring events, Log |

| Property Name | Data Type | Description | Applies To Event Type(s) |
|---|---|---|---|
| | | | Inspection events, Firewall events, Intrusion Prevention events |
| HostID | Integer | Unique identifier of the computer where the event occurred. | Anti-Malware events, Web Reputation events, Integrity Monitoring events, Log Inspection events, Firewall events, Intrusion Prevention events, Application Control events |
| HostInstanceID | String | The cloud instance ID of the computer where the event was detected. This property will only be set for computers synchronized with a Cloud Connector. | Application Control events, Anti-Malware events, Web Reputation events, Integrity Monitoring events, Log Inspection events, Firewall events, Intrusion Prevention events |

| Property Name | Data Type | Description | Applies To Event Type(s) |
|---|---|---|---|
| HostLastIPUsed | String (IP) | The latest IP address updated from the agent when communicated to Deep Security Manager. | Anti-Malware events, Application Control events, Firewall events, Integrity Monitoring events, Intrusion Prevention events, Log Inspection events, Web Reputation events |
| Hostname | String | Hostname of the computer on which the event was generated. | Anti-Malware events, Web Reputation events, Integrity Monitoring events, Log Inspection events, Firewall events, Intrusion Prevention events, Application Control events |
| HostOS | String | The operating system of the computer where the event was detected. | Anti-Malware events, Web Reputation events, Integrity Monitoring events, Log Inspection events, |

| Property Name | Data Type | Description | Applies To Event Type(s) |
|---|---|---|---|
| | | | Firewall events, Intrusion Prevention events, Application Control events |
| HostOwnerID | String | The cloud account ID of the computer where the event was detected. This property will only be set for computers synchronized with a Cloud Connector. | Application Control events, Anti-Malware events, Web Reputation events, Integrity Monitoring events, Log Inspection events, Firewall events, Intrusion Prevention events |
| HostSecurityPolicyID | Integer | The unique identifier of the Deep Security policy applied to the computer where the event was detected. | Anti-Malware events, Web Reputation events, Integrity Monitoring events, Log Inspection events, Firewall events, Intrusion Prevention events, Application Control events |

| Property Name | Data Type | Description | Applies To Event Type(s) |
|---|---|---|---|
| HostSecurityPolicyName | String | The name of the Deep Security policy applied to the computer where the event was detected. Note that security policy names may not be unique. | Anti-Malware events, Web Reputation events, Integrity Monitoring events, Log Inspection events, Firewall events, Intrusion Prevention events, Application Control events |
| HostVCUUID | String | The vCenter UUID of the computer the event applies to, if known. | Application Control events, Anti-Malware events, Web Reputation events, Integrity Monitoring events, Log Inspection events, Firewall events, Intrusion Prevention events |
| ImageDigest | String | A unique summary of data used to identify the container image. | Intrusion Prevention events, Firewall events |
| ImageID | String | Image ID of the Docker container where the event occurred | Intrusion Prevention events |

| Property Name | Data Type | Description | Applies To Event Type(s) |
|---|---|---|---|
| ImageName | String | Image name that was used to create the container where the event occurred. | Intrusion Prevention events, Firewall events |
| InfectedFilePath | String | Path of the infected file in the case of malware detection. | Anti-Malware events |
| InfectionSource | String | The name of the computer that's the source of a malware infection, if known. | Anti-Malware events |
| Interface | String (MAC) | MAC address of the network interface sending or receiving a packet. | Firewall events, Intrusion Prevention events |
| InterfaceType | String | Container interface type. 0=physical interfaces belong to host that can be controlled separately in Deep Security Manager, 1=all virtual interfaces, 7=unknown type (typically the host interface). | Intrusion Prevention events, Firewall events |
| IPDatagramLength | Integer | The length of the IP datagram. | Intrusion Prevention events |
| IsHash | String | The SHA-1 content hash (hexadecimal encoded) of the file after it was modified. | Integrity Monitoring events |
| Key | String | The file or registry key an integrity event refers to. | Integrity Monitoring events |
| LogDate | String (Date) | The date and time when the event was recorded. For Deep Security Agent-generated events (Firewall, | All event types |

| Property Name | Data Type | Description | Applies To Event Type(s) |
|---|---|---|---|
| | | IPS, etc.), the time is when the event was recorded by the agent, not when the event was received by Deep Security Manager. | |
| MajorVirusType | Integer (enum) | The classification of malware detected. 0=Joke, 1=Trojan, 2=Virus, 3=Test, 4=Spyware, 5=Packer, 6=Generic, 7=Other | Anti-Malware events |
| MajorVirusTypeString | String | Conversion of MajorVirusType to a readable string. | Anti-Malware events |
| MalwareName | String | The name of the malware detected. | Anti-Malware events |
| MalwareType | Integer (enum) | The type of malware detected. 1=General malware, 2=Spyware. General malware events will have an InfectedFilePath, spyware events will not. | Anti-Malware events |
| ManagerNodeID | Integer | Unique identifier of the Deep Security Manager Node where the event was generated. | System events |
| ManagerNodeName | String | Name of the Deep Security Manager Node where the event was generated. | System events |
| MD5 | String | The MD5 checksum (hash) of the software, if any. | Application Control events |
| Mitre | String | The MITRE information, if the process behavior is identified in one of MITRE attack scenarios. | Anti-Malware events |

| Property Name | Data Type | Description | Applies To Event Type(s) |
|---|---|---|---|
| ModificationTime | String (Date) | The modification time of the infected file. | Anti-Malware events |
| Note | Array (Byte) | Encoded note about the packet where the event occurred. | Intrusion Prevention events |
| Number | Integer | System events have an additional ID that identifies the event. Note that in the Deep Security Manager, this property appears as "Event ID". | System events |
| Operation | Integer (enum) | 0=Unknown, 1=Allowed due to detect-only mode, 2=Blocked | Application control |
| OperationDesc | String | Describes the Operation value | Application Control events |
| Origin | Integer (enum) | The origin of the event. -1=Unknown, 0=Deep Security Agent, 1=In-VM guest agent, 2=Deep Security Appliance, 3=Deep Security Manager | All event types |
| OriginString | String | Conversion of Origin to a human-readable string. | All event types |
| OSSEC_Action | String | OSSEC action | Log Inspection events |
| OSSEC_Command | String | OSSEC command | Log Inspection events |
| OSSEC_Data | String | OSSEC data | Log Inspection events |
| OSSEC_Description | String | OSSEC description | Log Inspection events |

| Property Name | Data Type | Description | Applies To Event Type(s) |
|---|---|---|---|
| OSSEC_DestinationIP | String | OSSEC dstip | Log Inspection events |
| OSSEC_DestinationPort | String | OSSEC dstport | Log Inspection events |
| OSSEC_DestinationUser | String | OSSEC dstuser | Log Inspection events |
| OSSEC_FullLog | String | OSSEC full log | Log Inspection events |
| OSSEC_Groups | String | OSSEC groups result (e.g. syslog,authentication_ failure) | Log Inspection events |
| OSSEC_Hostname | String | OSSEC hostname. This is the name of the host as read from a log entry, which is not necessarily the same as the name of the host on which the event was generated. | Log Inspection events |
| OSSEC_ID | String | OSSEC id | Log Inspection events |
| OSSEC_Level | Integer (enum) | OSSEC level. An integer in the range 0 to 15 inclusive. 0-3=Low severity, 4-7=Medium severity, 8-11=High severity, 12-15=Critical severity. | Log Inspection events |
| OSSEC_Location | String | OSSEC location | Log Inspection events |
| OSSEC_Log | String | OSSEC log | Log Inspection events |
| OSSEC_ProgramName | String | OSSEC program_name | Log Inspection events |

| Property Name | Data Type | Description | Applies To Event Type(s) |
|---|---|---|---|
| OSSEC_Protocol | String | OSSEC protocol | Log Inspection events |
| OSSEC_RuleID | Integer | OSSEC rule id | Log Inspection events |
| OSSEC_SourceIP | Integer | OSSEC srcip | Log Inspection events |
| OSSEC_SourcePort | Integer | OSSEC srcport | Log Inspection events |
| OSSEC_SourceUser | Integer | OSSEC srcuser | Log Inspection events |
| OSSEC_Status | Integer | OSSEC status | Log Inspection events |
| OSSEC_SystemName | Integer | OSSEC systemname | Log Inspection events |
| OSSEC_URL | Integer | OSSEC url | Log Inspection events |
| PacketData | Integer | Hexadecimal encoding of captured packet data, if the rule was configured to capture packet data. | Intrusion Prevention events |
| PacketSize | Integer | The size of the network packet. | Firewall events |
| Path | String | Directory path of the software file that was allowed or blocked, such as "/usr/bin/". (The file name is separate, in "FileName".) | Application Control events |
| PatternVersion | Integer (enum) | The malware detection pattern version. | Anti-Malware events |

| Property Name | Data Type | Description | Applies To Event Type(s) |
|---|---|---|---|
| PayloadFlags | Integer | Intrusion Prevention Filter Flags. A bitmask value that can include the following flag values: 1 - Data truncated - Data could not be logged. 2 - Log Overflow - Log overflowed after this log. 4 - Suppressed - Logs threshold suppressed after this log. 8 - Have Data - Contains packet data. 16 - Reference Data - References previously logged data. | Intrusion Prevention events |
| PodID | String | Pod unique ID (UID) | Intrusion Prevention events, Firewall events |
| PosInBuffer | Integer | Position within packet of data that triggered the event. | Intrusion Prevention events |
| PosInStream | Integer | Position within stream of data that triggered the event. | Intrusion Prevention events |
| Process | String | The name of the process that generated the event, if available. | Integrity Monitoring events |
| ProcessID | Integer | The identifier (PID) of the process that generated the event, if available. | Application Control events, Intrusion Prevention events, Firewall events |
| Process | String | The process name of behavior monitoring event detected. | Anti-Malware events |

| Property Name | Data Type | Description | Applies To Event Type(s) |
|---|---|---|---|
| ProcessName | String | The name of the process that generated the event, if available, such as "/usr/bin/bash". | Application Control events, Intrusion Prevention events, Firewall events |
| Protocol | Integer (enum) | The numerical network protocol identifier. -1=Unknown, 1=ICMP, 2=IGMP, 3=GGP, 6=TCP, 12=PUP, 17=UDP, 22=IDP, 58=ICMPv6, 77=ND, 255=RAW | Firewall events, Intrusion Prevention events |
| Protocol | Integer | The numerical value for the file scan protocol. 0=Local file | Anti-Malware events |
| ProtocolString | String | Conversion of Protocol to a readable string. | Firewall events, Intrusion Prevention events |
| Rank | Integer | The numerical rank of the event; the product of the computer's assigned asset value and the severity value setting for an event of this severity. | Integrity Monitoring events, Log Inspection events, Firewall events, Intrusion Prevention events |
| Reason | String | Name of the Deep Security rule or configuration object that triggered the event, or (for Firewall and Intrusion Prevention) a mapping of Status to String if the event | Firewall, Intrusion Prevention, Integrity Monitoring, Log |

| Property Name | Data Type | Description | Applies To Event Type(s) |
|---|---|---|---|
| | | was not triggered by a rule. For Application Control, "Reason" may be "None"; see "BlockReason" instead. | Inspection, Anti-Malware, and Application Control events |
| RepeatCount | Integer | The number of times this event occurred repeatedly. A repeat count of 1 indicates the event was only observed once and did not repeat. | Firewall events, Intrusion Prevention events, Application Control events |
| Risk | Integer (enum) | Translated risk level of the URL accessed. 2=Suspicious, 3=Highly Suspicious, 4=Dangerous, 5=Untested, 6=Blocked by Administrator | Web Reputation events |
| RiskLevel | Integer | The raw risk level of the URL from 0 to 100. Will not be present if the URL was blocked by a block rule. | Web Reputation events |
| RiskString | String | Conversion of Risk to a readable string. | Web Reputation events |
| ScanAction1 | Integer | Scan action 1. Scan action 1 & 2 and scan result actions 1 & 2 and ErrorCode are combined to form the single "summaryScanResult". | Anti-Malware events |
| ScanAction2 | Integer | Scan action 2. | Anti-Malware events |
| ScanResultAction1 | Integer | Scan result action 1. | Anti-Malware events |

| Property Name | Data Type | Description | Applies To Event Type(s) |
|---|---|---|---|
| ScanResultAction2 | Integer | Scan result action 2. | Anti-Malware events |
| ScanResultString | String | Malware scan result, as a string. A combination of ScanAction 1 and 2, ScanActionResult 1 and 2, and ErrorCode. | Anti-Malware events |
| ScanType | Integer (enum) | Malware scan type that created the event. 0=Real-Time, 1=Manual, 2=Scheduled, 3=Quick Scan | Anti-Malware events |
| ScanTypeString | String | Conversion of ScanType to a readable string. | Anti-Malware events |
| Severity | Integer | 1=Info, 2=Warning, 3=Error | System events |
| Severity | Integer (enum) | 1=Low, 2=Medium, 3=High, 4=Critical | Integrity Monitoring events, Intrusion Prevention events |
| SeverityString | String | Conversion of Severity to a human-readable string. | System events, Integrity Monitoring events, Intrusion Prevention events |
| SeverityString | String | Conversion of OSSEC_Level to a human-readable string. | Log Inspection events |
| SHA1 | String | The SHA-1 checksum (hash) of the software, if any. | Application Control events |

| Property Name | Data Type | Description | Applies To Event Type(s) |
|---|---|---|---|
| SHA256 | String | The SHA-256 checksum (hash) of the software, if any. | Application Control events |
| SourceIP | String (IP) | The source IP address of a packet. | Firewall events, Intrusion Prevention events |
| SourceMAC | String (MAC) | The source MAC Address of the packet. | Firewall events, Intrusion Prevention events |
| SourcePort | Integer | The network source port number of the packet. | Firewall events, Intrusion Prevention events |
| Status | Integer | If this event was not generated by a specific Firewall rule, then this status is one of approximately 50 hard-coded rules, such as 123=Out Of Allowed Policy | Firewall events |
| Status | Integer | If this event was not generated by a specific IPS rule, then this status is one of approximately 50 hard-coded reasons, such as -504=Invalid UTF8 encoding | Intrusion Prevention events |
| Tags | String | Comma-separated list of tags that have been applied to the event. This list will only include tags that are automatically applied when the event is generated. | All event types |

| Property Name | Data Type | Description | Applies To Event Type(s) |
|---|---|---|---|
| TagSetID | Integer | Identifier of the group of tags that was applied to the event. | All event types |
| TargetID | Integer | Unique identifier of the target of the event. This identifier is unique for the targets of the same type within a tenant. It is possible for target IDs to be reused across different types, for example, both a Computer and a Policy may have target ID 10. | System events |
| TargetIP | String (IP) | IP Address that was being contacted when a Web Reputation Event was generated. | Web Reputation events |
| TargetName | String | The name of the target of the event. The target of a system event can be many things, including computers, policies, users, roles, and tasks. | System events |
| TargetType | String | The type of the target of the event. | System events |
| TenantGUID | String | The global unique identifier (GUID) of the tenant associated with the event. | All event types |
| TenantID | Integer | Unique identifier of the tenant associated with the event. | All event types |
| TenantName | String | Name of the tenant associated with the event. | All event types |
| ThreadID | String | ID of the thread (from the container) that caused the event. | Intrusion Prevention events, |

| Property Name | Data Type | Description | Applies To Event Type(s) |
|---|---|---|---|
| | | | Firewall events |
| Title | String | Title of the event. | System events |
| URL | String (URL) | The URL being accessed that generated the event. | Web Reputation events |
| User | String | The user account that was the target of an integrity monitoring event, if known. | Integrity Monitoring events |
| UserID | String | The user identifier (UID), if any, of the user account that tried to start the software, such as "0". | Application Control events |
| UserName | String | For Anti-Malware events, this is the user account name who triggered the event.<br>For Application Control events, this is the user name, if any, of the user account that tried to start the software, such as "root". | Anti-Malware events, Application Control events |

### Data types of event properties

Events forwarded as JSON usually use strings to encode other data types.

| Data Type | Description |
|---|---|
| Array (Byte) | JSON `array`, composed of byte values. |
| Boolean | JSON `true` or `false`. |
| Integer | JSON `int`. Deep Security does not output floating point numbers in events. |

| Data Type | Description |
|---|---|
| | **Note:** Integers in events may be more than 32 bits. Verify the code that processes events can handle this. For example, [JavaScript's `Number` data type cannot safely handle larger than 32-bit integers]. |
| Integer (enum) | JSON `int`, restricted to a set of enumerated values. |
| String | JSON `string`. |
| String (Date) | JSON `string`, formatted as a date and time in the pattern YYYY-MM-DDThh:mm:ss.sssZ (ISO 8601). 'Z' is the time zone. 'sss' are the three digits for sub-seconds. See also the W3C note on date and time formats. |
| String (IP) | JSON `string`, formatted as an IPv4 or IPv6 address. |
| String (MAC) | JSON `string`, formatted as a network MAC address. |
| String (URL) | JSON `string`, formatted as a URL. |
| String (enum) | JSON `string`, restricted to a set of enumerated values. |

## Example events in JSON format

### System event

```
{
  "Type" :              "Notification",
  "MessageId" :         "123abc-123-123-123-123abc",
  "TopicArn" :          "arn:aws:sns:us-west-2:123456789:DS_Events",
  "Message" :           "[
                          {
                            "ActionBy":"System",
                            "Description":"Alert: New Pattern Update
is Downloaded and Available\\nSeverity: Warning\",
                            "EventID":6813,
                            "EventType":"SystemEvent",
                            "LogDate":"2018-12-04T15:54:24.086Z",
                            "ManagerNodeID":123,
                            "ManagerNodeName":"job7-123",
                            "Number":192,
                            "Origin":3,
                            "OriginString":"Manager",
                            "Severity":1,
                            "SeverityString":"Info",
                            "Tags":"\",
                            "TargetID":1,
                            "TargetName":"ec2-12-123-123-123.us-west-
2.compute.amazonaws.com",
                            "TargetType":"Host",
                            "TenantID":123,
                            "TenantName":"Umbrella Corp.",
                            "Title":"Alert Ended"
                          }
                        ]",
  "Timestamp" :       "2018-12-04T15:54:25.130Z",
  "SignatureVersion" : "1",
  "Signature" :       "500PER10NG5!gnaTURE==",
  "SigningCertURL" :  "https://sns.us-west-
2.amazonaws.com/SimpleNotificationService-abc123.pem",
  "UnsubscribeURL" :  "https://sns.us-west-
2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:123456:DS_Events:123abc-123-123-123-123abc"
}
```

### Anti-Malware events

Multiple virus detection events can be in each SNS `Message`. (For brevity, repeated event properties are omitted below, indicated by "...".)

```
{
  "Type" :              "Notification",
  "MessageId" :         "123abc-123-123-123-123abc",
  "TopicArn" :          "arn:aws:sns:us-west-2:123456789:DS_Events",
  "Message" :           "[
                          {
                            "AMTarget": "VDSO memory",
                            "AMTargetCount": 1,
                            "AMTargetType": 7,
                            "AMTargetTypeString": "Memory",
                            "ATSEDetectionLevel": 0,
                            "BehaviorRuleId": "DIRTYCOW_MADVISE_EXPL",
                            "BehaviorType": "Exploit_Detection",
                            "CommandLine": "/tmp/demo -f esiv [xxxx]",
                            "Cve": "CVE-2016-5195",
                            "ErrorCode": 0,
                            "EventID": 1179519,
                             "EventType": "AntiMalwareEvent",
                            "FileSHA1":
"CEF4644713633C0864D4283FEFA0CE174D48F115",
                            "HostAgentGUID": "FF8162DF-4CB5-B158-DE42-
EBD52967FCF7",
                            "HostAgentVersion": "20.0.0.1685",
                            "HostGUID": "9089E800-41D3-2CA9-FF0B-
3A30A42ED650",
                            "HostID": 38,
                            "HostLastIPUsed": "172.31.21.47",
                            "HostOS": "Red Hat Enterprise 7 (64 bit)
(3.10.0-957.12.2.el7.x86_64)",
                            "HostSecurityPolicyID": 11,
                            "HostSecurityPolicyName": "Linux_AM_
Sensor",
                            "Hostname": "ec2-3-131-151-239.us-east-
2.compute.amazonaws.com",
                            "InfectedFilePath": "/tmp/demo",
                            "LogDate": "2021-01-07T10:32:11.000Z",
                            "MajorVirusType": 14,
                            "MajorVirusTypeString": "Suspicious
Activity",
                            "MalwareName": "TM_MALWARE_BEHAVIOR",
                            "MalwareType": 4,
                            "Mitre": "T1068",
                            "Origin": 0,
                            "OriginString": "Agent",
                            "PatternVersion": "1.2.1189",
                            "Process": "testsys_m64",
                            "Protocol": 0,
                            "Reason": "Default Real-Time Scan
Configuration",
                            "ScanAction1": 1,
                            "ScanAction2": 0,
                            "ScanResultAction1": 0,
                            "ScanResultAction2": 0,
                            "ScanResultString": "Passed",
                            "ScanType": 0,
                            "ScanTypeString": "Real Time",
                            "Tags": "",
                            "TenantGUID": "",
                            "TenantID": 0,
                            "TenantName": "Primary",
                            "UserName": "root"
                          }
                        ]",
  "Timestamp" :      "2018-12-04T15:57:50.833Z",
  "SignatureVersion" : "1",
  "Signature" :      "500PER10NG5!gnaTURE==",
  "SigningCertURL" :  "https://sns.us-west-
2.amazonaws.com/SimpleNotificationService-abc123.pem",
  "UnsubscribeURL" :  "https://sns.us-west-
2.amazonaws.com/?Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:123456:DS_Events:123abc-123-123-123-123abc"
}
```

# Forward system events to a remote computer via SNMP

Deep Security supports SNMP for forwarding system events to a computer from Deep Security Manager. On Windows, the MIB file ("DeepSecurity.mib") is located in \Trend Micro\Deep Security Manager\util. On Linux, the default location is /opt/dsm/util.

# Configure alerts

Alerts are generated when Deep Security requires your attention, such as an administrator-issued command failing, or a hard disk running out of space. Deep Security includes a pre-defined set of alerts (for a list, see "Predefined alerts" on page 1196). Additionally, when you create protection module rules, you can configure them to generate alerts if they are triggered.

There are several ways to see which alerts have been triggered:

- They're displayed in the "Alert Status" dashboard widget in Deep Security Manager.
- They're displayed on the Alerts page in Deep Security Manager (see "View alerts in Deep Security Manager" on the next page).
- You can get an email notification when an alert is triggered (see "Set up email notification for alerts" on page 1182.)
- You can generate alert reports (see "Generate reports about alerts and other activity" on page 1192).

Unlike security events and system events, alerts are not purged from the database after a period of time. Alerts remain until they are dismissed, either manually or automatically.

## View alerts in Deep Security Manager

The **Alerts** page in Deep Security Manager displays all alerts that have been triggered, but not yet responded to. You can display alerts in a summary view that groups similar alerts together, or in list view, which lists all alerts individually. To switch between the two views, use the menu next to "Alerts" in the page's title. You can also sort the alerts by time or by severity.

In summary view, expanding an Alert panel (by clicking **Show Details**) displays all the computers (or users) that have generated that particular alert. Clicking the computer will display the computer's **Details** window. If an alert applies to more than five computers, an ellipsis ("...") appears after the fifth computer. Clicking the ellipsis displays the full list. Once you have taken the appropriate action to deal with an alert, you can dismiss the alert by selecting the check box next to the target of the alert and clicking **Dismiss**. (In list view, right-click the alert to see the list of options in the context menu.)

Alerts that can't be dismissed (like "Relay Update Service Not Available") will be dismissed automatically when the condition no longer exists.

**Note:** In cases where an alert condition occurs more than once on the same computer, the alert will show the timestamp of the first occurrence of the condition. If the alert is dismissed and the condition reoccurs, the timestamp of the first re-occurrence will be displayed.

**Tip:** Use the Computers filtering bar to view only alerts for computers in a particular computer group, with a particular policy, etc.

Unlike security events and system events, alerts are not purged from the database after a period of time. Alerts remain until they are dismissed, either manually or automatically.

## Configure alert settings

To configure the settings for individual alerts, go to the **Alerts** page in Deep Security Manager and click **Configure Alerts**. This displays a list of all alerts. A green check mark next to an alert indicates that it is enabled. An alert will be triggered if the corresponding situation occurs, and it will appear in the Deep Security Manager.

You can select an alert and click **Properties** to change other settings for the alert, such as the severity level and email notification settings.

## Set up email notification for alerts

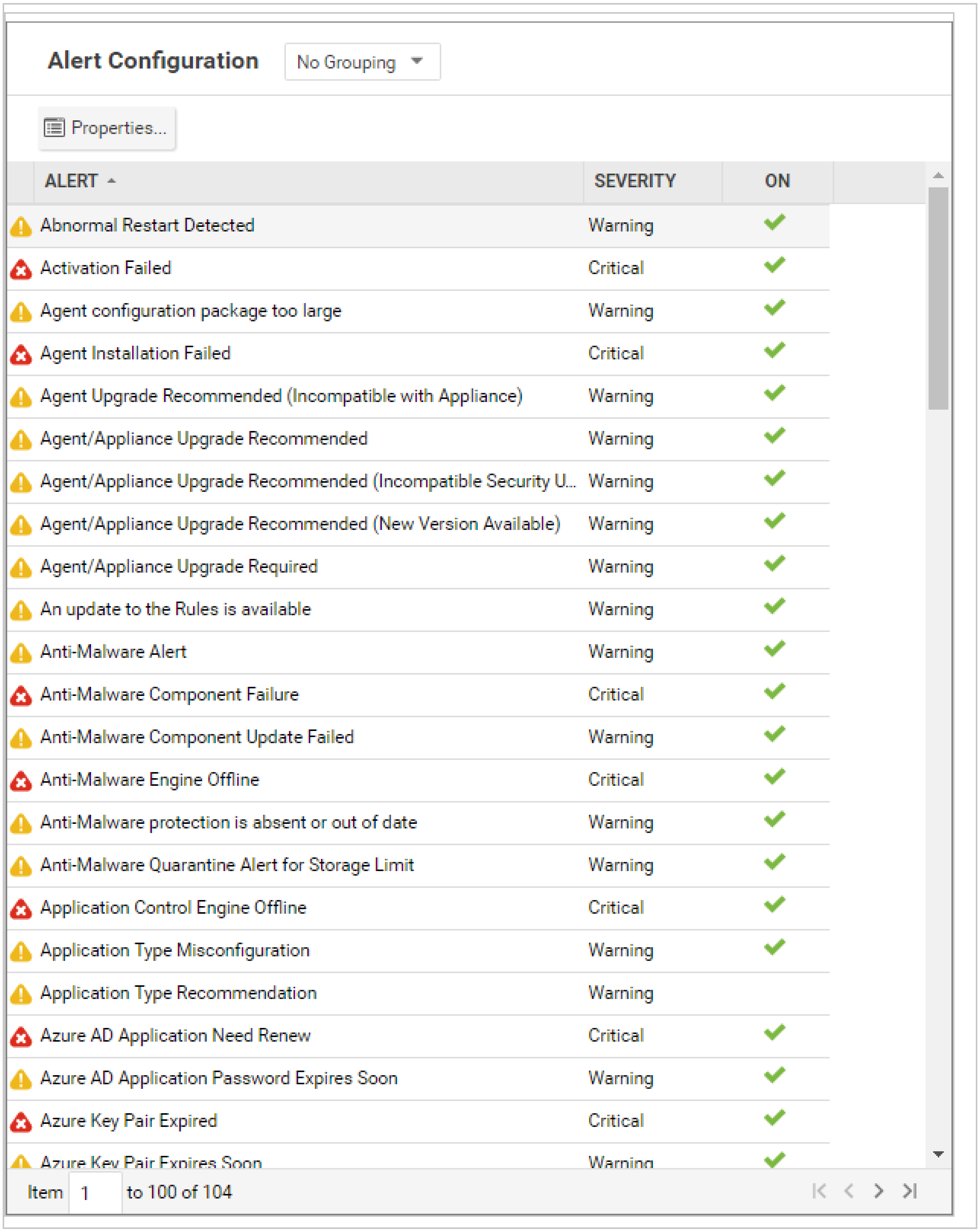
Deep Security Manager can send emails to specific users when selected alerts are triggered.

To enable email notifications:

1. Give Deep Security Manager access to an SMTP mail server (see "Configure SMTP settings for email notifications" on page 1186).
2. Specify which alerts cause email notifications to be sent. For example, you can send email only for the most critical alerts. Most alerts send email notifications by default. (see "Turn alert emails on or off" on the next page).
3. Specify who will receive email notifications. You can configure user accounts so that they receive alert emails (see "Configure an individual user to receive alert emails" on page 1185). You can also configure alerts to specify the email account of a user or a distribution list. With this option, email is sent regardless of the configuration of the user accounts (see "Configure recipients for all alert emails" on page 1186).

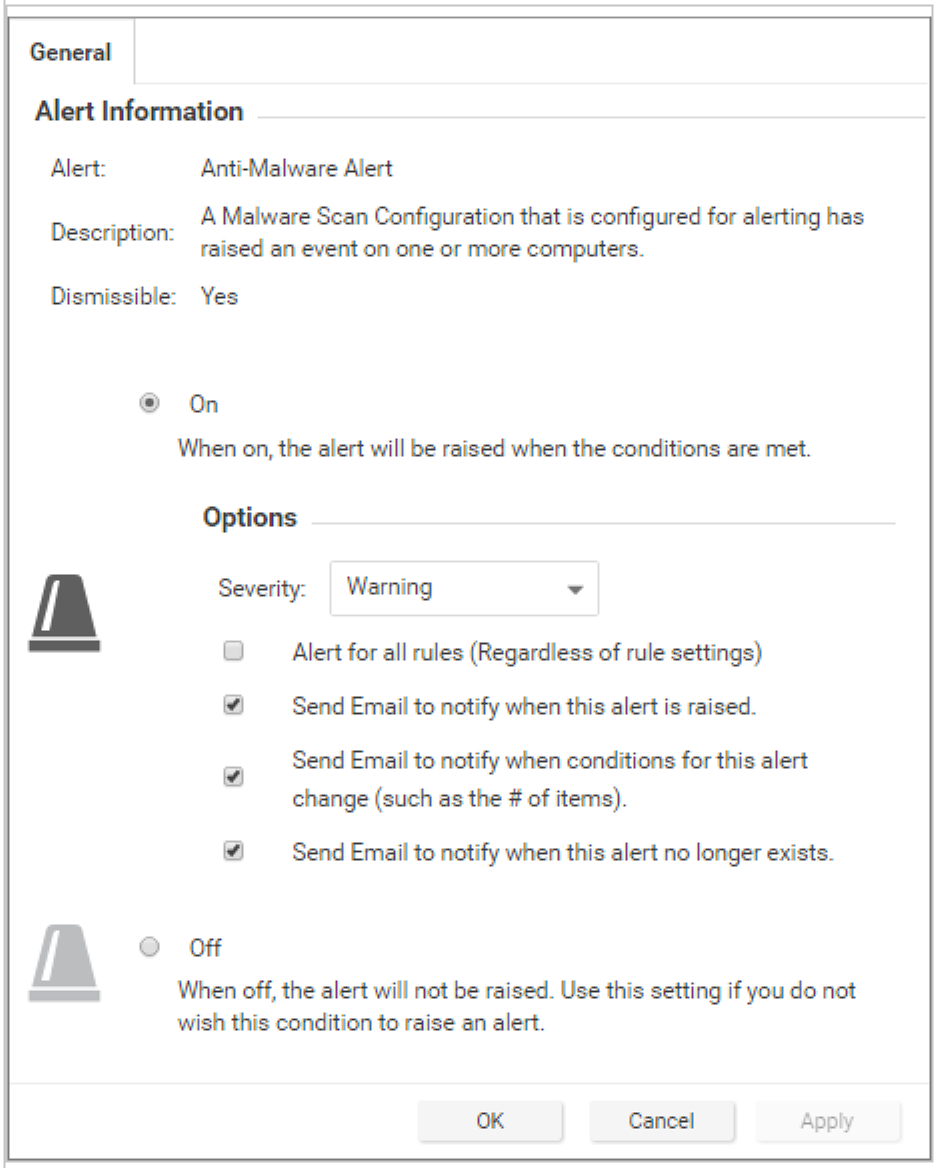
## Turn alert emails on or off

1. Go to the **Alerts** page and click **Configure Alerts** to display the list of alerts.



| ALERT | SEVERITY | ON |
|---|---|---|
| Abnormal Restart Detected | Warning | ✓ |
| Activation Failed | Critical | ✓ |
| Agent configuration package too large | Warning | ✓ |
| Agent Installation Failed | Critical | ✓ |
| Agent Upgrade Recommended (Incompatible with Appliance) | Warning | ✓ |
| Agent/Appliance Upgrade Recommended | Warning | ✓ |
| Agent/Appliance Upgrade Recommended (Incompatible Security U... | Warning | ✓ |
| Agent/Appliance Upgrade Recommended (New Version Available) | Warning | ✓ |
| Agent/Appliance Upgrade Required | Warning | ✓ |
| An update to the Rules is available | Warning | ✓ |
| Anti-Malware Alert | Warning | ✓ |
| Anti-Malware Component Failure | Critical | ✓ |
| Anti-Malware Component Update Failed | Warning | ✓ |
| Anti-Malware Engine Offline | Critical | ✓ |
| Anti-Malware protection is absent or out of date | Warning | ✓ |
| Anti-Malware Quarantine Alert for Storage Limit | Warning | ✓ |
| Application Control Engine Offline | Critical | ✓ |
| Application Type Misconfiguration | Warning | ✓ |
| Application Type Recommendation | Warning | |
| Azure AD Application Need Renew | Critical | ✓ |
| Azure AD Application Password Expires Soon | Warning | ✓ |
| Azure Key Pair Expired | Critical | ✓ |
| Azure Key Pair Expires Soon | Warning | ✓ |

2. A green check mark next to an alert indicates that it is enabled. An alert will be triggered if the corresponding situation occurs, and appear in the Deep Security Manager GUI. If you also want to receive email about the alert, double-click on an alert to display its Properties window, then select at least one of the "Send Email" check boxes.



General

Alert Information

Alert: Anti-Malware Alert

Description: A Malware Scan Configuration that is configured for alerting has raised an event on one or more computers.

Dismissible: Yes

● On

When on, the alert will be raised when the conditions are met.

Options

Severity: Warning

□ Alert for all rules (Regardless of rule settings)

☑ Send Email to notify when this alert is raised.

☑ Send Email to notify when conditions for this alert change (such as the # of items).

☑ Send Email to notify when this alert no longer exists.

○ Off

When off, the alert will not be raised. Use this setting if you do not wish this condition to raise an alert.

## Configure an individual user to receive alert emails

1. Go to **Administration** > **User Management** > **Users** and double-click a user account to display its Properties window.
2. On the **Contact Information** tab, enter an email address and select **Receive Alert Emails**.

### Configure recipients for all alert emails

> **Note:** All alert emails will be sent to this address or email distribution list, even if the recipients have not been set up in their user account properties to receive email notifications.

1. Go to **Administration** > **System Settings** > **Alerts**.
2. For **Alert Email Address - The email address to which all alert emails should be sent**, provide an email address or a distribution list email address.

## Configure SMTP settings for email notifications

Deep Security Manager can send emails to users when selected alerts are triggered (see "Configure alerts" on page 1180). Before setting up the email notifications, you need to allow Deep Security Manager access to a simple mail transfer protocol (SMTP) mail server:

Starting with Deep Security 20.0, you can use OAuth 2.0 authentication for Microsoft Exchange Online SMTP. This provides secure email delivery without requiring basic authentication or application-specific passwords. See Configure OAuth 2.0 for Microsoft Exchange Online.

1. Go to **Administration > System Settings > SMTP**.
2. Type the IP address or hostname of your SMTP email server. Include the port number if different from the default port number.
   AWS throttles (rate limits) email on the Internet Assigned Numbers Authority (IANA) standard port number for SMTP: Port 25. If you use AWS Marketplace, you may have faster alerts if you instead use SMTP over StartTLS (Start Transport Layer Security, a secure type of SMTP). For more information, see Connecting to an Amazon SES SMTP endpoint.
3. Use the From field to enter the email address from which the emails should be sent.
   If you are using Amazon Simple Email Service (SES), the sender email address must be verified. To learn how to verify your email address in Amazon SES and view a list of addresses you have already verified, see Verifying an email address identity.
4. Optionally, type a bounce address to which delivery status notifications (DSN) should be sent if the alert emails cannot be delivered to one or more users.
5. Configure authentication based on your SMTP server:
   - For Microsoft Exchange Online with OAuth 2.0, select **Mail server requires OAuth 2.0 authentication for Microsoft Exchange Online** and enter your OAuth 2.0 credentials. See Configure OAuth 2.0 for Microsoft Exchange Online.
   - For standard SMTP authentication, select **Mail server requires authentication** and enter your SMTP user name and password.

6. Select **STARTTLS** if your SMTP server supports the protocol. Deep Security Manager FIPS mode supports StarTTLS in Deep Security Manager 20 LTS Update 2022-03-22 and later. See "FIPS 140 support" on page 1639.
   If OAuth 2.0 authentication is enabled for Microsoft Exchange Online, STARTTLS is automatically enabled and cannot be disabled, as this is a requirement for OAuth 2.0.
7. After entering the necessary information, click **Test SMTP Settings** to test the connection.

## Configure OAuth 2.0 for Microsoft Exchange Online

Starting with Deep Security 20.0, Deep Security Manager supports OAuth 2.0 authentication for SMTP, allowing secure email delivery through Microsoft Exchange Online without requiring basic authentication or application-specific passwords.

### Prerequisites

Ensure that you have the following:

- Microsoft 365 subscription with Exchange Online (Business or Enterprise license). Basic Office 365 plans without Exchange Online are not supported.
- Administrator role:
  - Global Administrator or Application Administrator - for Azure AD configuration
  - Exchange Administrator or Global Administrator - for Exchange Online configuration

  If you do not have the required administrator permissions, you need to work with your IT department or Microsoft 365 administrator to complete the Azure AD and Exchange Online configuration. The final DSM configuration can be performed by any DSM user with the Settings Update permission.

### Configure Microsoft Entra ID

Configuring Microsoft Entra ID is a multi-step process.

**Step 1: Register an application in Microsoft Entra ID**

1. Sign in to the Azure portal.
2. Navigate to **Microsoft Entra ID** (formerly Azure Active Directory).
3. Select **App registrations** from the menu on the left.
4. Click **New registration**.

5. Configure the application by defining the following:
   - **Name**: Provide the Deep Security Manager SMTP or your preferred name.
   - **Supported account types**: Select **Accounts in this organizational directory only**.
   - **Redirect URI**: Leave this field blank.
6. Click **Register**.
7. After registration, note the values of the **Application (client) ID** and **Directory (tenant) ID** fields on the **Overview** page, as you will need them later.

#### Step 2: Create a client secret

1. In your application registration, select **Certificates & secrets** from the menu on the left.
2. Under **Client secrets**, click **New client secret**.
3. Configure the secret by defining the following:
   - **Description**: Enter the DSM SMTP secret or your preferred description.
   - **Expires**: Set the appropriate expiration period (for example, 24 months).
4. Click **Add**.
5. Copy the **Value** immediately and store it in a secure location - this is your client secret and it is only visible once. You will need it to configure DSM.

#### Step 3: Configure API permissions

1. In your application registration, select **API permissions** from the menu on the left.
2. Click **Add a permission**.
3. Select **APIs my organization uses**.
4. Search for and select **Office 365 Exchange Online**.
5. Select **Application permissions** (not Delegated permissions).
6. Add s permission by expanding the **SMTP** section and selecting **SMTP.SendAsApp**.
7. Click **Add permissions**.
8. If you are a Global Administrator, click **Grant admin consent for [Your Organization]**, then click **Yes**.
9. Verify that the status is **Granted for [Your Organization]** with a green checkmark.

It is important that you select **Office 365 Exchange Online** API, as opposed to Microsoft Graph. The permission should be `SMTP.SendAsApp` in the API permissions list.

### Configure Exchange Online

#### Step 4: Enable SMTP AUTH for your tenant

SMTP AUTH may be disabled by default in your tenant. You need to verify this and if it turns out to be disabled, enable it as follows:

1. Sign in to the Exchange admin center.
2. Navigate to **Settings > Mail flow > Accepted domains**.
3. Select your domain and verify SMTP is enabled.

   If you encounter an error about SMTP AUTH being disabled:

   - In Exchange admin center, go to **Settings > Mail flow**.
   - Click on **SMTP AUTH settings**.
   - Enable **Authenticated SMTP (SMTP AUTH)** for your organization.

### Step 5: Enable SMTP AUTH for the mailbox

SMTP AUTH needs to be enabled for the specific mailbox used by DSM.

**Option A: Enable using Exchange Online PowerShell** (recommended for bulk operations)

1. Connect to Exchange Online PowerShell by executing the following command:

   ```
   Connect-ExchangeOnline -UserPrincipalName admin@yourcompany.com
   ```

2. Enable SMTP AUTH for the mailbox by executing the following command:

   ```
   Set-CASMailbox -Identity "dsm-notifications@yourcompany.com" -
   SmtpClientAuthenticationDisabled $false
   ```

3. Verify the setting by executing the following command:

   ```
   Get-CASMailbox -Identity "dsm-notifications@yourcompany.com" |
   Select-Object SmtpClientAuthenticationDisabled
   ```

   The value should be `False`.

**Option B: Enable using Exchange Admin Center**

1. Go to **Recipients > Mailboxes**.
2. Select the mailbox and click **Manage email apps settings**.
3. Ensure that **Authenticated SMTP** is enabled.
4. Click **Save**.

### Step 6: Register service principal in Exchange Online

The application must be registered as a service principal in Exchange Online.

To register, perform the following procedure using PowerShell (there is no UI option available):

1. Connect to Exchange Online PowerShell (if not already connected) by executing the following command:

   ```
   Connect-ExchangeOnline -UserPrincipalName admin@yourcompany.com
   ```

2. Register the service principal by executing the following command:

   ```
   New-ServicePrincipal -AppId <Application (client) ID> -ServiceId
   <Object ID> -DisplayName "Deep Security Manager SMTP"
   ```

   Replace the following values:
   - `<Application (client) ID>`: The Application (client) ID from Step 1.
   - `<Object ID>`: The Object ID in Azure Portal > App registrations > Your app > Overview > Object ID

3. Grant the service principal permission to send email as the mailbox by executing the following command:

   ```
   Add-MailboxPermission -Identity "dsm-
   notifications@yourcompany.com" -User <Application (client) ID> -
   AccessRights FullAccess
   ```

## Configure Deep Security Manager

### Step 7: Configure SMTP settings in DSM

1. Log in to the Deep Security Manager console.
2. Navigate to **Administration > System Settings > SMTP** tab.
3. Configure the following:
   - **SMTP mail server address**: Set it to `smtp://smtp.office365.com:587`
   - **From email address**: Set it to dsm-notifications@yourcompany.com. This is the mailbox you configured in Step 5.
   - **Bounce email address**: Set it to dsm-notifications@yourcompany.com
4. Select **Mail server requires OAuth 2.0 authentication for Microsoft Exchange Online**.
5. Enter OAuth 2.0 credentials:
   - **Directory (tenant) ID**: Enter the value from Step 1.
   - **Application (client) ID**: Enter the value from Step 1.
   - **Client secret**: Enter the value from Step 2.
6. Click **Test SMTP settings** to verify the configuration.
7. If the test is successful, click **Save**.

When **Mail server requires OAuth 2.0 authentication for Microsoft Exchange Online** is selected, the following applies:

- Standard SMTP authentication fields SMTP username and SMTP password are not available.
- STARTTLS is automatically enabled and cannot be disabled, as this is required for OAuth 2.0.

## Troubleshooting

The following are common errors and solutions when using OAuth 2.0 with Microsoft Exchange Online:

#### Error: "535 5.7.139 Authentication unsuccessful, SmtpClientAuthentication is disabled"

**Cause:** SMTP AUTH is disabled at the tenant or mailbox level.

**Solution:**

1. Enable SMTP AUTH for the tenant (see Step 4).
2. Enable SMTP AUTH for the mailbox (see Step 5).
3. Wait 5-10 minutes for changes to propagate.

#### Error: "535 5.7.3 Authentication unsuccessful"

**Cause:** One or more of the following:

- Incorrect Application (client) ID, Directory (tenant) ID, or Client secret.
- Service principal not registered in Exchange Online.
- Missing API permissions or admin consent not granted.
- Client secret has expired.

**Solution:**

1. Verify all credentials are entered correctly in DSM.
2. Ensure service principal is registered (see Step 6).
3. Verify SMTP.SendAsApp permission is granted with admin consent (see Step 3).
4. Verify that Client secret has not expired in Azure Portal.

#### Error: "430 4.2.0 STOREDRV; mailbox logon failure"

**Cause:** The service principal does not have permission to access the mailbox.

**Solution:**

1. Grant the service principal FullAccess permission to the mailbox (see Step 6).
2. Wait 15-30 minutes for permission changes to propagate.

For more information, see the following:

- How to authenticate an IMAP, POP or SMTP connection using OAuth
- Enable or disable authenticated client SMTP submission (SMTP AUTH) in Exchange Online

## Generate reports about alerts and other activity

Deep Security Manager produces reports in PDF or RTF formats. Most of the reports have configurable parameters such as date range or reporting by computer group. Parameter options are disabled for reports to which they do not apply. You can set up a one-time report (see "Set up a single report" below) or set up a schedule to run a report on a regular basis (see "Set up a scheduled report " on page 1195).

### Set up a single report

1. In the Deep Security Manager, go to the **Events & Reports** tab and then in the left pane, click **Generate Reports > Single Report**.
2. In the **Report** list, select the type of report that you want to generate. Depending on which protection modules you are using, the following reports may be available:
   - **Alert Report:** List of the most common alerts.
   - **Anti-Malware Report:** List of the top 25 infected computers.
   - **Attack Report:** Summary table with analysis activity, divided by mode. See About attack reports.
   - **AWS Metered Billing Report:** Summary table of AWS Metered Billing consumption in hours per day by instance size.
   - **Azure Metered Billing Report:** Summary table of Azure Metered Billing consumption in hours per day by instance size.
   - **Computer Report:** Summary of each computer listed on the **Computer** tab.
   - **DPI Rule Recommendation Report:** Intrusion prevention rule recommendations. This report can be run for only one security policy or computer at a time.
   - **Firewall Report:** Record of firewall rule and stateful configuration activity.

   - **Forensic Computer Audit Report:** Configuration of an agent on a computer
   - **Integrity Monitoring Baseline Report** [1]**:** Baseline of the computers at a particular time, showing Type, Key, and Fingerprinted Date.
   - **Integrity Monitoring Detailed Change Report:** Details about the changes detected
   - **Integrity Monitoring Report:** Summary of the changes detected.
   - **Intrusion Prevention Report:** Record of intrusion prevention rule activity.
   - **Log Inspection Detailed Report:** Details of log data that has been collected.
   - **Log Inspection Report:** Summary of log data that has been collected.
   - **Recommendation Report:** Record of recommendation scan activity.
   - **Security Module Usage Cumulative Report:** Current computer usage of protection modules, including a cumulative total and the total in blocks of 100.
   - **Security Module Usage Report:** Current computer usage of protection modules.
   - **Summary Report:** Consolidated summary of Deep Security activity.
   - **Suspicious Application Activity Report:** Information about suspected malicious activity.
   - **System Event Report:** Record of system (non-security) activity.
   - **System Report:** Overview of computers, contacts, and users.
   - **Tenant Report:** Overview of tenants.
   - **User and Contact Report:** Content and activity detail for users and contacts.
   - **Web Reputation Report:** List of computers with the most web reputation events.

3. Select the **Format** for the report, either PDF or RTF. Note that the Security Module Usage Report and Security Module Usage Cumulative Report are exceptions and are always output as CSV files.
4. You can also add an optional **Classification** to PDF or RTF reports: BLANK, TOP SECRET, SECRET, CONFIDENTIAL, FOR OFFICIAL USE ONLY, LAW ENFORCEMENT SENSITIVE (LES), LIMITED DISTRIBUTION, UNCLASSIFIED, INTERNAL USE ONLY, CUSTOM.

   If you specify CUSTOM, the **Name** field is displayed, allowing you to enter a custom string. For example, "Alert report classification".
5. You can use the **Tag Filter** area to filter the report data using event tags (if you have selected a report that contains event data). Select **All** for all events, **Untagged** for only untagged events, or select **Tag(s)** and specify one or more tags to include only those events with your selected tags.

   If you apply multiple contradicting tags, the tags will counteract each other, rather than combine. For example, if you select User Signed In and User Signed Out, there will be no system events.

6. You can use the **Time Filter** area to set a time filter for any period for which records exist. This is useful for security audits. The following are time filter options:
   - **Last 24 Hours:** Includes events from the past 24 hours, starting and ending at the top of the hour. For example, if you generate a report on December 5th at 10:14am, you will get a report for events that occurred between December 4th at 10:00am and December 5th at 10:00am.
   - **Last 7 Days:** Includes events from the past week. Weeks start and end at midnight (00:00). For example, if you generate a report on December 5th at 10:14am, you will get a report for events that occurred between November 28th at 0:00am and December 5th at 0:00am.
   - **Previous Month:** Includes events from the last full calendar month, starting and ending at midnight (00:00). For example, if you select this option on November 15, you will receive a report for events that occurred between midnight October 1 to midnight November 1.
   - **Custom Range:** Enables you to specify your own date and time range for the report. In the report, the start time may be changed to midnight if the start date is more than two days ago.

     Note that reports use data stored in counters. Counters are data aggregated periodically from Events. Counter data is aggregated on an hourly basis for the most recent three days. Data from the current hour is not included in reports. Data older than three days is stored in counters that are aggregated on a daily basis. For this reason, the time period covered by reports for the last three days can be specified at an hourly level of granularity, but beyond three days, the time period can only be specified on a daily level of granularity.
7. In the **Computer Filter** area, select the computers whose data will be included in the report:
   - **All Computers:** Every computer in Deep Security Manager.
   - **My Computers:** If the signed in user has restricted access to computers based on their user role's rights settings, these are the computers to which the signed-in user has view access.
   - **In Group:** The computers in a Deep Security group.
   - **Using Policy:** The computers using a specific protection Policy.
   - **Computer:** A single computer.

     To generate a report on specific computers from multiple computer groups, create a user who has viewing rights only to the computers in question and then either create a scheduled task to regularly generate an All Computers report for that user or sign in as that user and run an All Computers report. The report includes only the computers to which that user has viewing rights.

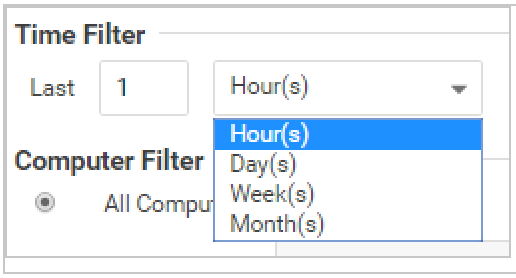
8. In the **Encryption** area, you can protect the report with the password of the currently signed in user or with a new password for this report only:
   - **Disable Report Password:** Report is not password protected.
   - **Use Current User's Report Password:** Use the current user's PDF report password. To view or modify the user's PDF report password, go to **Administration > User Management > Users > Properties > Settings > Reports**.
   - **Use Custom Report Password:** Create a one-time-only password for this report. The password does not have any complexity requirements.

## Set up a scheduled report

Scheduled reports are scheduled tasks that periodically generate and distribute reports to any number of users and contacts.

To set up a scheduled report, follow these steps:

1. On the **Events & Reports** tab, in the left pane, click **Generate Reports > Scheduled Reports**.
2. Click **New**. The **New Scheduled Task** wizard opens. Most of the options are identical to those for single reports, with the exception of **Time Filter**:



Time Filter

Last 1 Hour(s)

- **Last [N] Hour(s):** When [N] is less than 60, the start and end times will be at the top of the specified hour. When [N] is more than 60, hourly data is not available for the beginning of the time range, so the start time in the report will be changed to midnight (00:00) of the start day.
- **Last [N] Day(s):** Includes data from midnight [N] days ago to midnight of the current day.
- **Last [N] Week(s):** Includes events from the last [N] weeks, starting and ending at midnight (00:00).

- **Last [N] Month(s):** Includes events from the last [N] full calendar month, starting and ending at midnight (00:00). For example, if you select "Last 1 Month(s)" on November 15, you will receive a report for events that occurred between midnight October 1 to midnight November 1.

Reports use data stored in counters. Counters are data aggregated periodically from events. Counter data is aggregated on an hourly basis for the most recent three days. Data from the current hour is not included in reports. Data older than three days is stored in counters that are aggregated on a daily basis. For this reason, the time period covered by reports for the last three days can be specified at an hourly level of granularity, but beyond three days, the time period can only be specified on a daily level of granularity.

For more information on scheduled tasks, see the "Schedule Deep Security to perform tasks" on page 1600.

**Footnotes:**

[1] Due to performance issues related to large amounts of baseline data, in the latest version of Deep Security Manager, it is not possible to access baseline data from the UI. For details, see Database performance issue due to lots of Integrity Monitoring baseline data.

# Lists of events and alerts

## Predefined alerts

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| A computer reboot is required to enable Deep Security Agent protection | Critical | Yes | The agent software upgrade was successful, but a computer reboot is required to disable Windows Defender and enable Deep Security Agent protection. |
| A Deep Security Relay cannot download security components | Critical | No | A Deep Security Relay can't successfully download security components. This might be due to network connectivity issues or misconfigurations in Deep Security Manager under **Administration > System Settings > Updates**. Check your network configurations (for example, the proxy settings of the relay group) and **System Settings**, and then manually initiate an update on the relay using the **Download** |

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| | | | **Security Update** option on the **Administration > Updates > Software** page. |
| Abnormal Restart Detected | Warning | Yes | An abnormal restart has been detected on the computer. This condition may be caused by a variety of conditions. If the agent/appliance is suspected as the root cause then the diagnostics package (located in the Support section of the Computer Details dialog) should be invoked.<br>This alert indicates that the Deep Security Agent service was restarted abnormally. You can safely dismiss this alert, or, if the alert reoccurs, create a diagnostics package and open a case with Technical Support. |
| Activation Failed | Critical | No | This may indicate a problem with the agent/appliance, but it also can occur if agent self-protection is enabled. On the Deep Security Manager, go to **Computer editor**[1] **> Settings > General**. In **Agent Self Protection**, and then either deselect **Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent** or enter a password for local override. |
| Agent configuration package too large | Warning | Yes | This is usually caused by too many firewall and intrusion prevention rules being assigned. Run a recommendation scan on the computer to determine if any rules can be safely unassigned. |
| Agent Heartbeat Public Server Certificate Expired | Critical | No | The public server certificate used for TLS on the agent heartbeat port has expired. New agents may not be able to activate until the certificate is updated. |
| Agent Heartbeat Public | Warning | No | The public server certificate used for TLS |

[1] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| Server Certificate Expires Soon | | | on the agent heartbeat port will expire soon. Renew soon to prevent any disruption to agent communication. |
| Agent Installation Failed | Critical | Yes | The agent failed to install successfully on one or more computers. Those computers are currently unprotected. You must reboot the computers which will automatically restart the agent install program.<br>This may indicate a problem with the agent/appliance, but it also can occur if agent self-protection is enabled. On the Deep Security Manager, go to **Computer editor**[1] **> Settings > General**. In **Agent Self Protection**, and then either deselect **Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent** or enter a password for local override. |
| Agent Upgrade Recommended (Incompatible with Appliance) | Warning | No | Deep Security Manager has detected a computer with a version of the agent that is not compatible with the appliance. The appliance will always filter network traffic in this configuration resulting in redundant protection. (Deprecated in 9.5) |
| Agent/Appliance Upgrade Recommended | Warning | No | The Deep Security Manager has detected an older agent/appliance version on the computer that does not support all available features. An upgrade of the agent/appliance software is recommended. (Deprecated in 9.5) |
| Agent/ApplianceUpgrade Recommended (Incompatible Security Update(s)) | Warning | No | Deep Security Manager has detected a computer with a version of the agent/appliance that is not compatible with one or more security updates assigned to it. An upgrade of the agent/appliance software is recommended. |

[1] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| Agent/ApplianceUpgrade Recommended (New Version Available) | Warning | No | Deep Security Manager has detected one or more computers with a version of the agent/appliance that is older than the latest version imported into the manager. An upgrade of the agent/appliance software is recommended. |
| Agent/Appliance Upgrade Required | Warning | No | Deep Security Manager has detected a computer with a version of the agent/appliance that is not compatible with this version of the manager. An upgrade of the agent/appliance software is required. |
| An update to the Rules is available | Warning | No | Updated rules have been downloaded but not applied to your policies. To apply the rules, go to **Administration** > **Updates** > **Security** and in the **Rule Updates** column, click **Apply Rules to Policies**. |
| Anti-Malware Alert | Warning | Yes | A malware scan configuration that is configured for alerting has raised an event on one or more computers. |
| Anti-Malware Component Failure | Critical | Yes | An anti-malware component failed on one or more computers. See the event descriptions on the individual computers for specific details. |
| Anti-Malware Component Update Failed | Warning | No | One or more agent or relay failed to update anti-malware components. See the affected computers for more information. |
| Anti-Malware Engine Offline | Critical | No | The agent or appliance has reported that the anti-malware engine is not responding. Please check the system events for the computer to determine the cause of the failure. |
| Anti-malware module maximum disk space used to store identified files exceeded | Warning | Yes | The Anti-Malware module was unable to analyze or quarantine a file because the maximum disk space used to store identified files was reached. To change the maximum disk space for identified files setting, open the computer or policy editor and go to the Anti-malware > Advanced tab. |
| Anti-Malware protection is absent or out of date | Warning | No | The agent on this computer has not received its initial anti-malware protection package, or its anti-malware protection is out of date. Make sure a relay is available and that the agent has been properly configured to communicate with it. To configure relays and other update options, |

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| | | | go to Administration > System Settings > Updates. |
| API Key Locked Out | Warning | No | API Keys can be locked out manually, or by repeated failed validation attempts. |
| Application Control Engine Offline | Critical | No | The agent has reported that the Application Control engine failed to initialize. Please check the system events for the computer to determine the cause of the failure. |
| Application Control Ruleset is incompatible with agent version | Critical | No | An application control ruleset could not be assigned to one or more computers because the ruleset is not supported by the installed version of the agent. Typically, the problem is that a hash-based ruleset (which is compatible only with Deep Security Agent 11.0 or newer) has been assigned to an older Deep Security Agent. Deep Security Agent 10.x supports only file-based rulesets. (For details, see "Differences in how Deep Security Agent 10 and 11 compare files" on page 996.) To fix this issue, upgrade the Deep Security Agent to version 11.0 or newer. Alternatively, if you are using local rulesets, reset application control for the agent. Or if you are using a shared ruleset, use a shared ruleset that was created with Deep Security 10.x until all agents using the shared ruleset are upgraded to Deep Security Agent 11.0 or newer. |
| Application Type Misconfiguration | Warning | No | Misconfiguration of application types may prevent proper security coverage. |
| Application Type Recommendation | Warning | Yes | Deep Security Manager has determined that a computer should be assigned an application type. This could be because an agent was installed on a new computer and vulnerable applications were detected, or because a new vulnerability has been discovered in an installed application that was previously thought to be safe. To assign the application type to the computer, open the 'Computer Details' dialog box, click on 'Intrusion Prevention Rules', and assign the application type. |
| Azure Account Not Authorized to Read | Critical | No | Azure Cloud Account can't retrieve resources information from Azure API |

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| Resources Information | | | because the Azure Application is not authorized to read resources. Please verify that the Reader role has been assigned to the application. |
| Azure Account Password Invalid | Critical | No | Azure Cloud Account can't retrieve resources information from Azure API because the Azure Application password is invalid. |
| Azure Account Secret Expired | Critical | No | Azure Cloud Account can't retrieve resources information from Azure API because the Azure Application secret key has expired. |
| Microsoft Entra ID Application Not Found | Critical | No | Azure Cloud Account can't retrieve resources information from Azure API because the Azure Application is not found. The application possibly has been removed from Microsoft Entra ID. |
| Microsoft Entra ID Application Certificate expired | Critical | No | The Microsoft Entra ID application cannot sync the cloud data because the application certificate has expired. Renew the Azure Application certificate. |
| Microsoft Entra ID Application Certificate expires soon | Warning | No | The Microsoft Entra ID application certificate will expire soon. Renew the Azure Application certificate. |
| Microsoft Entra ID Application Need Renew | Critical | No | The Microsoft Entra ID application can not sync the cloud data now. Maybe the application password is expired or the application is deleted. Please renew the application via **Computers > Properties (right click on the target group) > Renew Application Now**. |
| Azure Key Pair Expired | Critical | No | The key pair for Azure service(s) has expired. You can remove this alert by updating your key pair on the Azure service's property page. |
| Azure Key Pair Expires Soon | Warning | No | The key pair for Azure service(s) will expire soon. You can remove this alert by updating your key pair on the Azure service's property page. |
| Azure Subscription Not Found | Critical | No | Azure Cloud Account can't retrieve resources information from Azure API because the Azure Subscription cannot be found. |
| Cisco ISE pxGrid certificate expires soon | Warning | Yes | The root and/or client certificates are approaching their expiration date. This alert will trigger 30 days prior to expiration. |

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| | | | Deep Security Manager users should regenerate these certificates in Cisco ISE and upload or replace the pxGrid connection certificates in the manager. |
| Cisco ISE pxGrid certificate has expired | Critical | Yes | Root or/and client certificate has already expired. Deep Security Manager users should regenerate these certificates in Cisco ISE and upload or replace the pxGrid connection certificates in the manager. |
| Census, Good File Reputation, and Predictive Machine Learning Service Disconnected | Warning | Yes | Disconnected from Census, Good File Reputation, and Predictive Machine Learning Service. Please see the event details below for possible solutions.<br>Refer to "Warning: Census, Good File Reputation, and Predictive Machine Learning Service Disconnected" on page 1331 for troubleshooting tips. |
| Certified Safe Software Service Offline | Warning | No | A Deep Security Manager node cannot connect to the Trend Micro Certified Safe Software Service to perform file signature comparisons for the integrity monitoring module. A locally cached database will be used until connectivity is restored. Make sure the manager node has internet connectivity and that proxy settings (if any) are correct. |
| Clock Change Detected | Warning | Yes | A clock change has been detected on the computer. Unexpected clock changes may indicate a problem on the computer and should be investigated before the alert is dismissed. |
| Cloud Computer Not Managed as Part of Cloud Account | Warning | Yes | An agent was activated on one or more computers belonging to a cloud account that is not synchronized with Deep Security. Click the link in the 'Action' field above to add the cloud account to Deep Security. The computer(s) will be moved into the account, and may be billed at a lower hourly rate. |

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| Communications Problem Detected | Warning | Yes | A communications problem has been detected on the computer. Communications problems indicate that the computer cannot initiate communication with the Deep Security Manager(s) because of network configuration or load reasons. Please check the system events in addition to verifying communications can be established to the Deep Security Manager (s) from the computer. The cause of the issue should be investigated before the alert is dismissed. |
| Computer Not Receiving Updates | Warning | No | These computer(s) have stopped receiving updates. Manual intervention may be required. |
| Computer Reboot Required | Critical | Yes | The agent software upgrade was successful, but the computer must be rebooted for the install to be completed. The computer(s) should be manually updated before the alert is dismissed. |
| Computer Reboot Required for Anti-Malware Protection | Critical | No | The anti-malware protection on the agent has reported that the computer needs to be rebooted. Please check the system events for the computer to determine the reason for the reboot. |
| Computer Reboot Required for Application Control Protection | Critical | No | The Application Control protection on Agent has reported that the computer needs to be rebooted. Please check the system events for the computer to determine the reason for the reboot. |
| Computer Reboot Required for Integrity Monitoring Protection | Critical | No | The Integrity Monitoring protection on Agent has reported that the computer needs to be rebooted. Please check the system events for the computer to determine the reason for the reboot. |
| Configuration Required | Warning | No | One or more computers are using a policy that defines multiple interface types where not all interfaces have been mapped. |
| Connection to Filter Driver Failure | Critical | No | An appliance has reported a failure connecting to the filter driver. This may indicate a configuration issue with the filter driver running on the ESXi or with the appliance. The appliance must be able to connect to the filter driver in order to protect guests. The cause of the issue |

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| | | | should be investigated and resolved. |
| CPU Critical Threshold Exceeded | Critical | No | The CPU critical threshold has been exceeded. |
| CPU Warning Threshold Exceeded | Warning | No | The CPU warning threshold has been exceeded. |
| Critical database error while creating new table partitions during maintenance job | Critical | No | A critical error occurred during routine database maintenance. During maintenance, new partitions are added to partitioned tables to accommodate new data. During the most recent maintenance job, errors occurred, meaning that some tables are missing future partitions. New data that would ordinarily be written to those partitions may be lost.<br>Please contact your support provider immediately for assistance in resolving this issue. (To facilitate the process, try to have server logs ready, which can be found at the root directory of Deep Security Manager) |
| Duplicate Computer Detected | Warning | Yes | A duplicate computer has been activated or imported. Please remove the duplicate computer and reactivate the original computer if necessary. |
| Duplicate Unique Identifiers Detected | Warning | No | Duplicate UUIDs have been detected. Please remove the duplicate UUID. |
| Empty Relay Group Assigned | Critical | No | These computers have been assigned an empty relay group. Assign a different relay group to the computers or add relays to the empty relay group(s). |
| Events Suppressed | Warning | Yes | The agent/appliance encountered an unexpectedly high volume of events. As a result, one or more events were not recorded (suppressed) to prevent a potential denial of service. Check the firewall events to determine the cause of the suppression. |
| Events Truncated | Warning | Yes | Some events were lost because the data file grew too large for the agent/appliance to store. This may have been caused by an unexpected increase in the number of |

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| | | | events being generated, or the inability of the agent/appliance to send the data to the Deep Security Manager. For more information, see the properties of the "Events Truncated" system event on the computer. |
| Execution of Software Blocked | Warning | Yes | Execution of software was blocked on one or more computers. See the Application Control Events on the following computers for more information. |
| Failed to Send SNS Message | Critical | No | The Deep Security Manager was unable to forward messages to Amazon SNS |
| Failed to Send Syslog Message | Warning | No | The Deep Security Manager was unable to forward messages to one or more Syslog Servers. |
| Files could not be scanned for malware | Warning | No | Files could not be scanned for malware because the file path exceeded the maximum file path length limit or the directory depth exceeded the maximum directory depth limit. Please check the system events for the computer to determine the reason. |
| Firewall Engine Offline | Critical | No | The agent/appliance has reported that the firewall engine is offline. Please check the status of the engine on the agent/appliance. |
| Firewall Rule Alert | Warning | Yes | A firewall rule that is selected for alerting has been encountered on one or more computers. |
| Firewall Rule Recommendation | Warning | Yes | Deep Security Manager has determined that a computer on your network should be assigned a firewall rule. This could be because an agent was installed on a new computer and vulnerable applications were detected, or because a new vulnerability has been discovered in an installed application that was previously thought to be safe. To assign the firewall rule to the computer, open the 'Computer Details' dialog box, click on the 'Firewall Rules' node, and assign the firewall rule. |
| Heartbeat Server Failed | Warning | No | The heartbeat server failed to start properly. This may be due to a port number conflict. Agents/appliances will not be able to contact the manager until this problem is resolved. To resolve this |

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| | | | problem ensure that another service is not using the port number reserved for use by the heartbeat server and "Restart the Deep Security Manager" on page 1560 service. If you do not wish to use the heartbeat you can turn this alert off in the Alert Configuration section. |
| Incompatible Agent/Appliance Version | Error | No | Deep Security Manager has detected a more recent agent/appliance version on the computer that is not compatible with this version of the manager. An upgrade of the manager software is recommended. |
| Insufficient Disk Space | Warning | Yes | The agent/appliance has reported that it was forced to delete an old log file to free up disk space for a new log file. Please immediately free up disk space to prevent loss of intrusion prevention, firewall and agent/appliance events. See "Warning: Insufficient disk space" on page 1333. |
| Integrity Monitoring Engine Offline | Critical | No | The agent/appliance has reported that the integrity monitoring engine is not responding. Please check the system events for the computer to determine the cause of the failure. |
| Integrity Monitoring information collection has been delayed | Warning | No | The rate at which integrity monitoring information is collected has been temporarily delayed due to an increased amount of integrity monitoring data. During this time the baseline and integrity event views may not be current for some computers. This alert will be dismissed automatically once integrity monitoring data is no longer being delayed. |
| Integrity Monitoring Rule Alert | Warning | Yes | An integrity monitoring rule that is selected for alerting has been encountered on one or more computers. |
| Integrity Monitoring Rule Compilation Error | Critical | No | An error was encountered compiling an integrity monitoring rule on a computer. This may result in the integrity monitoring rule not operating as expected. |
| Integrity Monitoring Rule Recommendation | Warning | Yes | Deep Security Manager has determined that a computer on your network should be assigned an integrity monitoring rule. To assign the integrity monitoring rule to the computer, open the 'Computer Details' dialog box, click on the 'Integrity |

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| | | | Monitoring > Integrity Monitoring Rules' node, and assign the integrity monitoring rule. |
| Integrity Monitoring Rule Requires Configuration | Warning | No | An integrity monitoring rule that requires configuration before use has been assigned to one or more computers. This rule will not be sent to the computer(s). Open the integrity monitoring rule properties and select the Configuration tab for more information. |
| Integrity Monitoring Trusted Platform Module Not Enabled | Warning | Yes | Trusted platform module not enabled. Please ensure the hardware is installed and the BIOS setting is correct. |
| Integrity Monitoring Trusted Platform Module Register Value Changed | Warning | Yes | Trusted platform module register value changed. If you have not modified the ESXi hypervisor configuration this may represent an attack. |
| Intrusion Prevention Engine Offline | Critical | No | The agent/appliance has reported that the intrusion prevention engine is offline. Please check the status of the engine on the agent/appliance. |
| Intrusion Prevention Rule Alert | Warning | Yes | An intrusion prevention rule that is selected for alerting has been encountered on one or more computers. |
| Intrusion Prevention Rule Compilation Failed | Critical | Yes | This is usually caused by a misconfigured IPS Rule. The Rule name can be found in the Event's Properties window. To resolve this issue, identify the Rule and unassign it or contact Trend Micro Support for assistance. |
| Intrusion Prevention Rule Requires Configuration | Warning | No | An intrusion prevention rule that requires configuration before use has been assigned to one or more computers. This rule will not be sent to the computer(s). Open the intrusion prevention rule properties and select the Configuration tab for more information. |
| Invalid System Settings Detected | Critical | No | The Deep Security Manager detected invalid values for one or more system settings. |
| IoT event overloaded | Warning | No | The IoT events are unable to be processed in time. There might be some computers that produce a lot of events, or some rules are misconfigured. |
| Legacy Agent Software Detected | Warning | Yes | We have detected software whose version |

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| | | | is less than 9.5, and is no longer supported. Please import the latest software to replace it.<br>For details, see "Get Deep Security Agent software" on page 520. |
| Log Inspection Engine Offline | Critical | No | The agent/appliance has reported that the log inspection engine has failed to initialize. Please check the system events for the computer to determine the cause of the failure. |
| Log Inspection Rule Alert | Warning | Yes | A log inspection rule that is selected for alerting has been encountered on one or more computers. |
| Log Inspection Rule Recommendation | Warning | Yes | Deep Security Manager has determined that a computer on your network should be assigned a log inspection rule. To assign the log inspection rule to the computer, open the 'Computer Details' dialog box, click on the 'Log Inspection > Log Inspection Rules' node, and assign the log inspection rule. |
| Log Inspection Rule Requires Configuration | Warning | No | A log inspection rule that requires configuration before use has been assigned to one or more computers. This rule will not be sent to the computer(s). Open the Log Inspection Rule properties and select the Configuration tab for more information. |
| Low Disk Space | Warning | No | A Deep Security Manager Node has less than 10% remaining disk space. Please free space by deleting old or unnecessary files, or add more storage capacity. |
| Maintenance Mode On | Warning | No | Maintenance mode is currently active for application control on one or more computers. While this mode is active, application control continues to enforce block rules (if you selected **Block unrecognized software until it is explicitly allowed**), but will allow software updates, and automatically add them to the inventory part of the ruleset. When the software update is finished for each computer, disable maintenance mode so that unauthorized software is not |

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| | | | accidentally added to the ruleset. |
| Manager Offline | Warning | No | A Deep Security Manager node is offline. It is possible the computer has a hardware or software problem, or has simply lost network connectivity. Please check the status of the manager's computer. |
| Manager Time Out of Sync | Critical | No | The clock on each manager node must be synchronized with the clock on the database. If the clocks are too far out of sync (more than 30 seconds) the manager node will not perform its tasks correctly. Synchronize the clock on your manager node with the clock on the database. |
| Memory Critical Threshold Exceeded | Critical | No | The memory critical threshold has been exceeded. |
| Memory Warning Threshold Exceeded | Warning | No | The memory warning threshold has been exceeded. |
| Move Failed | Warning | Yes | Computer was not moved to Trend Cloud One - Endpoint & Workload Security due to a connectivity issue.<br>Before trying the move again:<br>- Check that all parameters specified for the move are correct, including the tenant information, activation token, public CA certificate, and proxy settings.<br>- Check that there are no networking/firewall settings preventing the agent from reaching Trend Cloud One - Endpoint & Workload Security.<br>- Use the CLI to create an agent diagnostic package, which will include a ds_agent.log file containing information about the failed move. For instructions on creating diagnostic packages, see Create a diagnostic package and |

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| | | | logs. |
| Move Failed: No response | Warning | Yes | Computer was not moved to Trend Cloud One - Endpoint & Workload Security because the move request timed out.<br>If using manager-initiated activation, there was no response from the agent after the manager initiated the command.<br>If using agent-initiated activation, there was no heartbeat from the agent.<br>Check the agent status and try the move again. |
| Move Failed: Failed to activate | Warning | Yes | The move to Trend Cloud One - Endpoint & Workload Security failed due to an activation issue and was rolled back.<br>Before trying the move again:<br>• Check that all parameters specified for the move are correct, including the tenant information, activation token, public CA certificate, and proxy settings.<br>• Use the CLI to create an agent diagnostic package, which will include dsa_move.log and dsa_control.log files containing information about the failed move. For instructions on creating diagnostic packages, see Create a diagnostic package and logs. |
| Move Failed: Unmanaged | Critical | Yes | The move to Trend Cloud One - Endpoint & Workload Security failed due to an activation issue and the move could not be rolled back. The computer is in an |

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| | | | unmanaged state.<br>To troubleshoot this issue:<br>• Look into the dsa_move.log file, which contains information about the failed move.<br>• Manually restore the agent or reactivate the agent. See the troubleshooting section for more details.<br>Before trying the move again:<br>• Check that the Workload Security Link is up-to-date.<br>• Check that all parameters specified for the move are correct, including the tenant information, activation token, public CA certificate, and proxy settings. |
| Network Engine Mode Incompatibility | Warning | No | Setting Network Engine Mode to Tap is only available on agent versions 5.2 or later. Review and update the agent's configuration or upgrade the agent to resolve the incompatibility. |
| New Pattern Update is Downloaded and Available | Warning | No | New patterns are available as part of a security update. The patterns have been downloaded to Deep Security but have not yet been applied to your computers. To apply the update to your computers, go to the Administration > Updates > Security page. |
| New Rule Update is Downloaded and Available | Warning | No | New rules are available as part of a security update. The rules have been downloaded to Deep Security but have not yet been applied to policies and sent to your computers. To apply the update and send the updated policies to your computers, go to the Administration > Updates > Security page. |

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| Newer Version of Deep Security Manager is Available | Warning | No | A new version of the Deep Security Manager is available. Download the latest version from the Trend Micro Download Center at http://downloadcenter.trendmicro.com/ |
| Newer Versions of Software Available | Warning | No | New software is available. Software can be downloaded from the Download Center. |
| Number of Computers exceeds database limit | Warning | No | The number of activated computers has exceeded the recommended limit for an embedded database. Performance will degrade rapidly if more computers are added and it is strongly suggested that another database option (Oracle or SQL Server) be considered at this point. Please contact Trend Micro for more information on upgrading your database. |
| Protection Module Licensing Expired | Warning | Yes | The protection module license has expired. |
| Protection Module Licensing Expires Soon | Warning | No | The protection module licensing will expire soon. You can remove this alert by changing your license on the Administration > Licenses page. |
| Recommendation | Warning | Yes | Deep Security Manager has determined that the security configuration of one of your computers should be updated. To see what changes are recommended, open the **Computer editor**[1] and look through the module pages for warnings of unresolved recommendations. In the Assigned Rules area, click **Assign/Unassign** to display the list of available rules and then filter them using the "Show Recommended for Assignment" viewing filter option. (Select "Show Recommended for Unassignment" to display rules that can safely be unassigned.) |
| Reconnaissance Detected: Computer OS Fingerprint Probe | Warning | Yes | The agent or appliance detected an attempt to identify the computer operating system via a "fingerprint" probe. Such activity is often a precursor to an attack that targets specific vulnerabilities. Check |

[1] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| | | | the computer's events to see the details of the probe and see "Warning: Reconnaissance Detected" on page 1333. |
| Reconnaissance Detected: Network or Port Scan | Warning | Yes | The agent or appliance detected network activity typical of a network or port scan. Such activity is often a precursor to an attack that targets specific vulnerabilities. Check the computer's events to see the details of the probe and see "Warning: Reconnaissance Detected" on page 1333. |
| Reconnaissance Detected: TCP Null Scan | Warning | Yes | The agent or appliance detected a TCP "Null" scan. Such activity is often a precursor to an attack that targets specific vulnerabilities. Check the computer's events to see the details of the probe and see "Warning: Reconnaissance Detected" on page 1333. |
| Reconnaissance Detected: TCP SYNFIN Scan | Warning | Yes | The agent or appliance detected a TCP "SYNFIN" scan. Such activity is often a precursor to an attack that targets specific vulnerabilities. Check the computer's events to see the details of the probe and see "Warning: Reconnaissance Detected" on page 1333. |
| Reconnaissance Detected: TCP Xmas Scan | Warning | Yes | The agent or appliance detected a TCP "Xmas" scan. Such activity is often a precursor to an attack that targets specific vulnerabilities. Check the computer's events to see the details of the probe and see "Warning: Reconnaissance Detected" on page 1333. |
| Relay Upgrade Required For Agent Integrity Check | Warning | No | To enable Agent Integrity Check, please upgrade relay. |
| SAML Identity Provider Certificate expired | Critical | No | One or more SAML Identity Provider Certificate(s) expired. |
| SAML Identity Provider Certificate expires soon | Warning | No | One or more SAML Identity Provider Certificate(s) will expire soon. |
| SAML Service Certificate expired | Critical | No | SAML Service Provider Certifcate expired. |
| SAML Service Certificate expires soon | Warning | No | SAML Service Provider Certificate expires soon. |
| Scheduled Malware Scan Missed | Warning | No | Scheduled malware scan tasks were initiated on computers that already had pending scan tasks. This may indicate a scanning frequency that is too high. Consider lowering the scanning |

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| | | | frequency, or selecting fewer computers to scan during each scheduled scan job. |
| Send Policy Failed | Critical | No | Inability to send policy may indicate a problem with the agent/appliance. Please check the affected computers. |
| Smart Protection Server Connection Failed | Warning | Yes | Failed to connect to a Smart Protection Server. This could be due to a configuration issue, or due to network connectivity. |
| Software Changes Detected | Warning | No | During ongoing file system monitoring, application control detected that new software had been installed, and it did not match any configured allow or block rule. If your system administrators did not install the software, and no other users have permissions to install software, this could indicate a security compromise. If the software tries to launch, depending on your lockdown configuration at that time, it may or may not be allowed to execute. |
| Software Package Not Found | Critical | No | An agent software package is required for the proper operation of one or more virtual appliance(s). Please import a Red Hat Enterprise Linux 6 (64 bit) agent software package with the correct version for each appliance. If the required version is not available then please import the latest package and upgrade the appliance to match. |
| Software Updates Available for Import | Warning | No | New software is available. To import new software to Deep Security, go to Administration > Updates > Software > Download Center. |
| Unable to communicate | Critical | No | Deep Security Manager has been unable to query the agent/appliance for its status within the configured period. Please check your network configuration and the affected computer's connectivity. |
| Unable to Upgrade the Agent Software | Warning | Yes | Deep Security Manager was unable to upgrade the agent software on the computer. |

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| | | | This may indicate a problem with the agent/appliance, but it also can occur if agent self-protection is enabled. On the Deep Security Manager, go to **Computer editor**[1] **> Settings > General**. In **Agent Self Protection**, and then either deselect **Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent** or enter a password for local override. |
| Unresolved software change limit reached | Critical | No | Software changes detected on the file system exceeded the maximum amount. Application control will continue to enforce existing rules, but will not record any more changes, and it will stop displaying any of that computer's software changes. You must resolve and prevent excessive software change. |
| Upgrade of the Deep Security Manager Software Recommended (Incompatible Security Update(s)) | Warning | No | Deep Security Manager has detected a computer that is using security updates that are not compatible with the current version of Deep Security Manager. An upgrade of Deep Security Manager software is recommended. |
| User Locked Out | Warning | No | Users can be locked out manually, by repeated incorrect sign-in attempts, if their password expires, or if they have been imported but not yet unlocked. |
| User Password Expires Soon | Warning | No | The password expiry setting is enabled and one or more users have passwords that will expire within the next 7 days. |
| Virtual Appliance is Incompatible With Filter Driver | Warning | No | The appliance is incompatible with the filter driver. Please ensure both are upgraded to their latest versions. |
| Virtual Machine Interfaces Out of Sync | Warning | No | One or more of the virtual machines monitored by a Deep Security Virtual Appliance has reported that its interfaces are out of sync with the filter driver. This means that the appliance may not be |

[1] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

| Alert | Default Severity | Dismissible | Description |
|---|---|---|---|
| | | | properly monitoring the virtual machine's interfaces. The virtual machine may require manual intervention such as a configuration change, or a restart, to correct the issue. |
| Virtual Machine Moved to Unprotected ESXi Server | Warning | Yes | A virtual machine was moved to an ESXi Server that does not have an activated Deep Security Virtual Appliance. |
| Virtual Machine Unprotected after move to another ESXi | Warning | Yes | A virtual machine that was appliance-protected has been unprotected during or after it was moved to another ESXi. This may be due to an appliance reboot or power off during the move, or it may indicate a configuration issue. The cause of the issue should be investigated before the alert is dismissed. |
| VMware Tools Not Installed | Critical | Yes | A protected virtual machine in an NSX environment does not have VMware Tools installed. VMware Tools is required to protect virtual machines in an NSX environment. |
| Web Reputation Event Alert | Warning | Yes | A web reputation event has been encountered on one or more computers that are selected for alerting. |
| WorkSpaces Disabled for AWS Account | Warning | Yes | An agent was activated on one or more Amazon WorkSpaces but WorkSpaces are not enabled for your AWS account. To enable WorkSpaces, click 'Edit AWS Account' above, and select the 'Include Amazon WorkSpaces' check box. Your WorkSpace(s) will be moved into the WorkSpaces folder of the AWS account. |

The following table lists alerts and their corresponding alert email subjects.

| Alert | Alert Email Subject |
|---|---|
| CPU Critical Threshold Exceeded | The CPU critical threshold of Manager Node ({1}) was exceeded |
| CPU Warning Threshold Exceeded | The CPU warning threshold of Manager Node ({1}) was exceeded |
| DSRU Recommended | DSRU recommended |

| Alert | Alert Email Subject |
|---|---|
| Legacy Agent Software Detected | Legacy Agent software detected |
| User Locked Out | {0} User(s) locked out |
| User Password Expires Soon | {0} User(s) have passwords due to expire |
| Abnormal Restart Detected | Abnormal restart detected on {0} computer(s) |
| Clock Change Detected | Clock change detected on {0} computer(s) |
| Communications Problem Detected | Communications problem detected on {0} computer(s) |
| Events Truncated | Events truncated on {0} computer(s) |
| Agent Heartbeat Public Server Certificate Expired | Agent heartbeat public server certificate expired |
| Agent Heartbeat Public Server Certificate Expires Soon | Agent heartbeat public server certificate expires soon |
| Agent Installation Failed | Agent installation failed on {0} computer(s) |
| Insufficient Disk Space | Insufficient disk space detected on {0} computer(s) |
| Events Suppressed | Events suppressed on {0} computer(s) |
| Unable to communicate | Unable to communicate with {0} computer(s) |
| A Deep Security Relay cannot download security components | Unable to update security components on {0} relay(s) |
| Unable to Upgrade the Agent Software | Unable to upgrade the Agent software on {0} computer(s) |
| Incompatible Agent/Appliance Version | Incompatible agent/appliance version detected on {0} computer(s) |
| Agent/Appliance Upgrade | Upgrade of the agent/appliance software is recommended |

| Alert | Alert Email Subject |
|---|---|
| Recommended (New Version Available) | on one or more computers |
| Agent Upgrade Recommended (Incompatible with Appliance) | Upgrade of the agent software is recommended on {0} computer(s) in order to coordinate protection with the appliance |
| Agent/Appliance Upgrade Recommended (Incompatible Security Update(s)) | Upgrade of the agent/appliance software is recommended on {0} computer(s) in order to support the assigned security updates |
| Agent/Appliance Upgrade Required | Upgrade of the agent/appliance software is required on {0} computer(s) |
| Agent/Appliance Upgrade Recommended | Upgrade of the agent/appliance is recommended on {0} computer(s) |
| New Pattern Update is Downloaded and Available | New pattern update available for {0} agent/appliance(s) |
| AWS Account Migration Failed | AWS account migration failed |
| WorkSpaces Disabled for AWS Account | WorkSpaces disabled for AWS account |
| API Key Locked Out | {0} API key(s) locked out |
| Connection to Filter Driver Failure | Connection to filter driver failure |
| Software Package Not Found | Software package not found |
| Microsoft Entra ID Application Certificate Expired | Microsoft Entra ID application for {0} Azure service(s) has expired |
| Microsoft Entra ID Application Certificate Expires Soon | Microsoft Entra ID application certificate for {0} Azure service(s) expires soon |
| Microsoft Entra ID Application Need Renew | Microsoft Entra ID application for {0} Azure service(s) need renew |
| Azure Account Not | Microsoft Entra ID application for {0} Azure cloud account(s) |

| Alert | Alert Email Subject |
|---|---|
| Authorized to Read Resource Information | does not have read permission |
| Microsoft Entra ID Application Not Found | Microsoft Entra ID application for {0} Azure cloud account(s) not found |
| Microsoft Entra ID Application Password Expires Soon | Microsoft Entra ID application password for {0} Azure service(s) expires soon |
| Azure Account Secret Expired | Microsoft Entra ID application secret key for {0} Azure cloud account(s) has expired |
| Azure Account Password Invalid | Invalid Microsoft Entra ID application secret for {0} Azure cloud account(s) |
| Azure Subscription Not Found | Azure subscription cannot be found for {0} Azure cloud account(s) |
| Azure Key Pair Expired | Key pair for {0} Azure service(s) has expired |
| Azure Key Pair Expires Soon | Key Pair for {0} Azure service(s) will expire soon |
| Census, Good File Reputation, and Predictive Machine Learning Service Disconnected | Disconnected from Census, Good File Reputation, and Predictive Machine Learning Service |
| Cloud Computer Not Managed as Part of Cloud Account | {0} computer(s) are in cloud environment but not managed as part of cloud account |
| Duplicate Computer Detected | {0} duplicate computer(s) detected |
| Duplicate Unique Identifiers Detected | {0} duplicate unique identifiers detected |
| Upgrade of the Filter Driver Recommended (New Version Available) | Upgrade of the filter driver is recommended on {0} ESXi Server(s) in order to take advantage of the latest features |
| Heartbeat Server Failed | Heartbeat server failed to start on Manager Node ({1}) |

| Alert | Alert Email Subject |
|---|---|
| Configuration Required | Configuration required on {0} computer(s) |
| Computer Not Receiving Updates | {0} Computers(s) are not receiving updates |
| A computer reboot is required to enable Deep Security Agent protection | A computer reboot is required to enable Deep Security Agent protection |
| Invalid System Settings Detected | Invalid system settings detected |
| MQTT Connection Offline | MQTT connection offline for {0} computer(s) |
| MQTT Connection Configuration Failed | MQTT connection configuration failed for {0} computer(s) |
| Protection Module Licensing Expired | Licensing for {1} has expired |
| Protection Module Licensing Expires Soon | Licensing for {1} expires ({2}) |
| Low Disk Space | Manager node ({1}) has low disk space |
| Manager Offline | Manager node ({1}) is offline |
| Manager Time Out of Sync | The clock on Manager Node ({1}) is not synchronized with the clock on the database |
| Upgrade of the Workload Security Manager Software Recommended (Incompatible Security Update(s)) | Upgrade of the Workload Security Manager software is recommended because {0} computer(s) have assigned security updates that are incompatible with the current Workload Security Manager version |
| Memory Critical Threshold Exceeded | The memory critical threshold of Manager Node ({1}) was exceeded |
| Memory Warning Threshold Exceeded | The memory warning threshold of Manager Node ({1}) was exceeded |
| Virtual Machine Moved to Unprotected ESXi Server | Virtual Machine moved to unprotected ESXi server from a protected ESXi server |

| Alert | Alert Email Subject |
|---|---|
| Multiple Activated Appliances Detected | Multiple activated appliances detected |
| Newer Versions of Software Available | Newer versions of software available |
| Newer Version of Workload Security Manager is Available | Newer version of Workload Security Manager is available |
| Number of Computers exceeds database limit | Number of computers exceeds the recommended limit for an embedded database |
| Number of Computers exceeds License | Number of computers exceeds the licensed computers allowed |
| Number of Manager Nodes Exceeds License | Number of Manager Nodes exceeds the {3} licensed Managers allowed |
| Critical database error while creating new table partitions during maintenance job | Critical database error while creating new table partitions during maintenance job |
| Recommendation | Recommendations have been made for {0} computer(s) |
| Relay Upgrade Required For Agent Integrity Check | To enable Agent Integrity Check, please upgrade relay |
| SAML Identity Provider Certificate expired | {0} SAML Identity Provider certificate(s) expired |
| SAML Identity Provider Certificate expires soon | {0} SAML Identity Provider certificate(s) expire soon |
| SAML Service Provider Certificate expired | SAML Service Provider certificate expired |
| SAML Service Provider Certificate expires soon | SAML Service Provider certificate expires soon |
| Failed to Send SNS Message | Unable to forward messages to Amazon SNS |

| Alert | Alert Email Subject |
|---|---|
| Software Updates Available for Import | Software updates are available for download |
| Failed to Send Syslog Message | Unable to forward messages to {0} Syslog Server(s) |
| Activation Failed | Failed to activate {0} computer(s) |
| Send Policy Failed | Failed to send policy(ies) to {0} computer(s) |
| Virtual Machine Unprotected after move to another ESXi | Virtual Machine unprotected after move to another ESXi |
| VMware Tools Not Installed | VMware tools not installed |
| An update to the Rules is available | An update to the Rules is available |
| New Rule Update is Downloaded and Available | New Rule update not applied |
| Anti-Malware Alert | Malware Scan Configuration ({1}) alert on {0} Computer(s) |
| Intrusion Prevention Rule Alert | Intrusion Prevention Rule ({1}) alert on {0} Computer(s) |
| Computer Reboot Required for Activity Monitoring | Computer Reboot Required for Activity Monitoring |
| Agent requires Permission for Anti-Malware | Agent on {0} computer(s) requires permission for Anti-Malware |
| Anti-Malware Engine Offline | {0} Anti-Malware Engine(s) Offline |
| Scheduled Malware Scan Missed | Scheduled Malware Scan(s) missed on {0} computers |
| Anti-Malware protection is absent or out of date | Apply the latest Anti-Malware updates to the Agent on {0} computer(s) |
| Anti-malware module maximum disk space used to | Anti-malware module exceeded maximum disk space used to store identified files |

| Alert | Alert Email Subject |
|---|---|
| store identified files exceeded | |
| Computer Reboot Required for Anti-Malware Protection | Computer Reboot is Required for Anti-Malware Protection |
| Files could not be scanned for malware | Files(s) on {0} Agent(s)/Appliance(s) could not be scanned for malware |
| Smart Protection Server Connection Failed | Failure to connect to a Smart Protection Server |
| Anti-Malware Component Failure | An Anti-Malware component failure occurred on {0} computer(s) |
| Anti-Malware Component Update Failed | Anti-Malware Component Update Failed on {0} computers |
| Web Reputation Event Alert | Web Reputation event alert on {0} Computer(s) |
| Intrusion Defense Firewall Server Plug-in License has Expired or Will Expire Soon | Intrusion Defense Firewall Server Plug-in license expires ({2}) |
| Agent/Appliance Upgrade Recommended (Incompatible Component Update(s)) | Upgrade of the Agent/Appliance software is recommended on {0} Computer(s) in order to support the assigned Component Updates |
| Container Control authorization plugin parse request failed | The Container Control authorization plugin was unable to parse a request. This may be caused by a Docker version incompatibility. Please check that you are using a supported Docker version. |
| Container Control authorization plugin connection to Docker failed | The Container Control authorization plugin cannot connect to Docker. Please try turning the Container Control module off and then on again. |
| Container Control authorization plugin installation failed | The Container Control authorization plugin is not installed. Please try turning the Container Control module off and then on again. |
| Container Control authorization plugin failed to | The Container Control authorization plugin failed to send a configuration. Please try turning the Container Control |

| Alert | Alert Email Subject |
|---|---|
| send configuration | module off and then on again. |
| Log Inspection Engine Offline | {0} Log Inspection engine(s) offline |
| Log Inspection Rule Alert | Log Inspection Rule ({1}) alert on {0} Computer(s) |
| Log Inspection Rule Requires Configuration | Log Inspection Rule ({1}) requires configuration on {0} Computer(s) |
| Log Inspection Rule Recommendation | Log Inspection Rule ({1}) is recommended on {0} Computer (s) |
| SAP Virus Scan service is not working correctly | {0} SAP Virus Scan services are not working correctly |
| SAP Virus Scan Adapter is not installed | {0} SAP Virus Scan Adapters are not installed |
| SAP Virus Scan Adapter is not up to date | {0} SAP Virus Scan Adapters are not up to date |
| Execution of Software Blocked | Execution of Software Blocked on {0} {0,choice,1#computer\|2#computers} |
| Unresolved software change limit reached | Unresolved software change limit reached on {0} {0,choice,1#computer\|2#computers} |
| Application Control Engine Offline | {0} Application Control {0,choice,1#Engine\|2#Engines} Offline |
| Application Control Ruleset is incompatible with agent version | Application Control Ruleset is incompatible with agent version on {0} {0,choice,1#computer\|2#computers} |
| Maintenance Mode On | Maintenance Mode active on {0} {0,choice,1#computer\|2#computers} |
| Computer Reboot Required for Application Control Protection | Computer Reboot is Required for Application Control Protection |

| Alert | Alert Email Subject |
|---|---|
| Software Changes Detected | Software Changes detected on {0} {0,choice,1#computer |
| AWS Contract License Exceeded | AWS Contract License Exceeded |
| AWS SaaS Billing is not configured correctly | AWS SaaS Billing is not configured correctly |
| License Expired | License Expired |
| License Expiring Soon | License Expiring Soon |
| License Seat Limit Exceeded | License Seat Limit Exceeded |
| License Seat Limit Almost Reached | License Seat Limit Almost Reached |
| Account Balance Depleted | Account Balance Depleted |
| Account Balance Low | Account Balance Low |
| Integrity Monitoring information collection has been delayed | Integrity Monitoring information collection has been delayed |
| Integrity Monitoring Engine Offline | {0} Integrity Monitoring Engine(s) Offline |
| Certified Safe Software Service Offline | Manager node ({1}) cannot connect to Certified Safe Software Service |
| Computer Reboot Required for Integrity Monitoring Protection | Computer Reboot Required for Integrity Monitoring Protection |
| Integrity Monitoring Rule Alert | Integrity Monitoring Rule ({1}) alert on {0} Computer(s) |
| Integrity Monitoring Rule Compilation Error | Integrity Monitoring Rule Compilation Error on {0} Computer (s) |
| Integrity Monitoring Rule | Integrity Monitoring Rule ({1}) requires configuration on {0} |

| Alert | Alert Email Subject |
|---|---|
| Requires Configuration | Computer(s) |
| Integrity Monitoring Trusted Platform Module Not Enabled | Integrity Monitoring Trusted Platform Module Not Enabled |
| Integrity Monitoring Trusted Platform Module Register Value Changed | Integrity Monitoring Trusted Platform Module Register Value Changed |
| Integrity Monitoring Rule Recommendation | Integrity Monitoring Rule ({1}) is recommended on {0} Computer(s) |
| Agent configuration package too large | Agent configuration package too large on {0} computer(s) |
| Intrusion Prevention Rule Compilation Failed | Intrusion Prevention Rule Compilation Failed on {0} computer(s) |
| Reconnaissance Detected: Computer OS Fingerprint Probe | Reconnaissance Detected: Computer OS fingerprint probe on {0} Computer(s) |
| Reconnaissance Detected: TCP Null Scan | Reconnaissance Detected: TCP "Null" scan on {0} Computer(s) |
| Reconnaissance Detected: Network or Port Scan | Reconnaissance Detected: Network or port scan on {0} Computer(s) |
| Reconnaissance Detected: TCP SYNFIN Scan | Reconnaissance Detected: TCP "SYNFIN" scan on {0} Computer(s) |
| Reconnaissance Detected: TCP Xmas Scan | Reconnaissance Detected: TCP "Xmas" scan on {0} Computer(s) |
| Application Type Misconfiguration | {0} Computer(s) have Application Type Misconfiguration |
| Network Engine Mode Incompatibility | {0} Agent(s) unable to implement Network Engine Mode |
| Firewall Engine Offline | {0} firewall engine(s) offline |

| Alert | Alert Email Subject |
|---|---|
| Firewall Rule Alert | Firewall Rule ({1}) alert on {0} Computer(s) |
| Intrusion Prevention Engine Offline | {0} Intrusion Prevention engine(s) offline |
| Intrusion Prevention Rule Alert | Intrusion Prevention Rule ({1}) alert on {0} Computer(s) |
| Intrusion Prevention Rule Requires Configuration | Intrusion Prevention Rule ({1}) requires configuration on {0} Computer(s) |
| Application Type Recommendation | Application Type ({1}) is recommended on {0} Computer(s) |
| Firewall Rule Recommendation | Firewall Rule ({1}) is recommended on {0} Computer(s) |
| Intrusion Prevention Rule Recommendation | Intrusion Prevention Rule ({1}) is recommended on {0} Computer(s) |
| Intrusion Prevention Rule Removal Recommendation | Intrusion Prevention Rule ({1}) is recommended for removal on {0} Computer(s) |
| Virtual Machine Interfaces Out of Sync | Virtual Machine Interfaces Out of Sync |
| Wrong AWS credential | Wrong AWS credential for {0} Account(s) |
| Virtual Appliance is Incompatible With Filter Driver | Incompatibility with Filter Driver was detected for {0} Virtual Appliance(s) |
| Empty Relay Group Assigned | {0} Computers(s) are assigned an empty Relay Group |
| Computer Reboot Required | Computer reboot required on {0} Computer(s) |

## Agent events

| ID | Severity | Event | Notes |
|---|---|---|---|
| **Special Events** | | | |

| ID | Severity | Event | Notes |
|---|---|---|---|
| 0 | Error | Unknown Agent/Appliance Event | |
| **Driver-Related Events** | | | |
| 1000 | Error | Unable To Open Engine | |
| 1001 | Error | Engine Command Failed | |
| 1002 | Warning | Engine List Objects Error | |
| 1003 | Warning | Remove Object Failed | |
| 1004 | Error | Driver Upgrade Stalled | |
| 1005 | Info | Upgrading Driver | |
| 1006 | Error | Driver Upgrade Requires Reboot | |
| 1007 | Info | Driver Upgrade Succeeded | |
| 1008 | Error | Kernel Unsupported | |
| 1010 | Warning | Trend Micro LightWeight Filter Driver has been disabled | |
| 1011 | Info | Trend Micro LightWeight Filter Driver has been restarted | |
| 1012 | Info | All Trend Micro LightWeight Filter Drivers have been restarted successfully | |
| 1013 | Warning | Trend Micro LightWeight Filter Driver failed to bind on all network interfaces | |
| **Configuration-Related Events** | | | |
| 2000 | Info | Policy Sent | |
| 2001 | Warning | Invalid Firewall Rule Assignment | |
| 2002 | Warning | Invalid Firewall Stateful Configuration | |
| 2003 | Error | Save Security Configuration Failed | |
| 2004 | Warning | Invalid Interface Assignment | |
| 2005 | Warning | Invalid Interface Assignment | |
| 2006 | Warning | Invalid Action | |
| 2007 | Warning | Invalid Packet Direction | |
| 2008 | Warning | Invalid Rule Priority | |
| 2009 | Warning | Unrecognized IP Format | |
| 2010 | Warning | Invalid Source IP List | |
| 2011 | Warning | Invalid Source Port List | |
| 2012 | Warning | Invalid Destination IP List | |

| ID | Severity | Event | Notes |
|---|---|---|---|
| 2013 | Warning | Invalid Destination Port List | |
| 2014 | Warning | Invalid Schedule | |
| 2015 | Warning | Invalid Source MAC List | |
| 2016 | Warning | Invalid Destination MAC List | |
| 2017 | Warning | Invalid Schedule Length | |
| 2018 | Warning | Invalid Schedule String | |
| 2019 | Warning | Unrecognized IP Format | |
| 2020 | Warning | Object Not Found | |
| 2021 | Warning | Object Not Found | |
| 2022 | Warning | Invalid Rule Assignment | |
| 2050 | Warning | Firewall Rule Not Found | |
| 2075 | Warning | Traffic Stream Not Found | |
| 2076 | Warning | Intrusion Prevention Rule Not Found | |
| 2077 | Warning | Pattern List Not Found | |
| 2078 | Warning | Traffic Stream Conversion Error | |
| 2080 | Warning | Conditional Firewall Rule Not Found | |
| 2081 | Warning | Conditional Intrusion Prevention Rule Not Found | |
| 2082 | Warning | Empty Intrusion Prevention Rule | |
| 2083 | Warning | Intrusion Prevention Rule XML Rule Conversion Error | |
| 2085 | Error | Security Configuration Error | |
| 2086 | Warning | Unsupported IP Match Type | |
| 2087 | Warning | Unsupported MAC Match Type | |
| 2088 | Warning | Invalid SSL Credential | |
| 2089 | Warning | Missing SSL Credential | |
| 2090 | Error | Security Configuration Error | |
| 2091 | Error | Security Configuration Error | |
| **Hardware-Related Events** | | | |
| 3000 | Warning | Invalid MAC Address | |
| 3001 | Warning | Get Event Data Failed | |
| 3002 | Warning | Too Many Interfaces | |
| 3003 | Error | Unable To Run External Command | |

| ID | Severity | Event | Notes |
|---|---|---|---|
| 3004 | Error | Unable To Read External Command Output | |
| 3005 | Error | Operating System Call Error | |
| 3006 | Error | Operating System Call Error | |
| 3007 | Error | File Error | |
| 3008 | Error | Machine-Specific Key Error | |
| 3009 | Error | Unexpected Agent/Appliance Shutdown | |
| 3010 | Error | Agent/Appliance Database Error | |
| 3300 | Warning | Get Event Data Failed | Linux error. |
| 3302 | Warning | Get Security Configuration Failed | Linux error. |
| 3303 | Error | File Mapping Error | Linux error. File type error. |
| 3600 | Error | Get Windows System Directory Failed | |
| 3601 | Warning | Read Local Data Error | Windows error. |
| 3602 | Warning | Windows Service Error | Windows error. |
| 3603 | Error | File Mapping Error | Windows error. File size error. |
| 3700 | Warning | Abnormal Restart Detected | Windows error. |
| 3701 | Info | System Last Boot Time Change | Windows error. |
| **Communications-Related Events** | | | |
| 4000 | Warning | Invalid Protocol Header | Content length out of range. |
| 4001 | Warning | Invalid Protocol Header | Content length missing. |
| 4002 | Info | Command Session Initiated | |
| 4003 | Info | Configuration Session Initiated | |
| 4004 | Info | Command Received | |
| 4011 | Warning | Failure to Contact Manager | |
| 4012 | Warning | Heartbeat Failed | |
| **Agent-Related Events** | | | |
| 5000 | Info | Agent/Appliance Started | |
| 5001 | Error | Thread Exception | |
| 5002 | Error | Operation Timed Out | |
| 5003 | Info | Agent/Appliance Stopped | |
| 5004 | Warning | Clock Changed | |
| 5005 | Info | Agent/Appliance Auditing Started | |
| 5006 | Info | Agent/Appliance Auditing Stopped | |
| 5007 | Info | Appliance Protection | |

| ID | Severity | Event | Notes |
|---|---|---|---|
| | | Change | |
| 5008 | Warning | Filter Driver Connection Failed | |
| 5009 | Info | Filter Driver Connection Success | |
| 5010 | Warning | Filter Driver Informational Event | |
| 5100 | Info | Protection Module Deployment Started | |
| 5101 | Info | Protection Module Deployment Succeeded | |
| 5102 | Error | Protection Module Deployment Failed | |
| 5103 | Info | Protection Module Download Succeeded | |
| 5104 | Info | Protection Module Disablement Started | |
| 5105 | Info | Protection Module Disablement Succeeded | |
| 5106 | Error | Protection Module Disablement Failed | |
| 5107 | Info | Agent Self-Protection enabled | |
| 5108 | Info | Agent Self-Protection disabled | |
| 5109 | Error | FIPS verification Error | |
| 5110 | Error | Secure Boot Public Key Not Enrolled | This error can occur if the public key required to check the signature on the Trend Micro kernel module is not successfully enrolled on the agent computer.<br>For details, see "Configure Linux Secure Boot for agents" on page 527. |
| 5111 | Error | Secure Boot 'On' Not Supported | Deep Security Agent does not support this OS with Secure Boot enabled.<br>For details, see "Configure Linux Secure Boot for agents" on page 527. |
| 5200 | Info | File Backup Completed | |
| 5201 | Error | Failure to Backup File | |
| **Logging-Related Events** | | | |
| 6000 | Info | Log Device Open Error | |
| 6001 | Info | Log File Open Error | |

| ID | Severity | Event | Notes |
|---|---|---|---|
| 6002 | Info | Log File Write Error | |
| 6003 | Info | Log Directory Creation Error | |
| 6004 | Info | Log File Query Error | |
| 6005 | Info | Log Directory Open Error | |
| 6006 | Info | Log File Delete Error | |
| 6007 | Info | Log File Rename Error | |
| 6008 | Info | Log Read Error | |
| 6009 | Warning | Log File Deleted Due To Insufficient Space | |
| 6010 | Warning | Events Were Suppressed | |
| 6011 | Warning | Events Truncated | |
| 6012 | Error | Insufficient Disk Space | See "Warning: Insufficient disk space" on page 1333. |
| 6013 | Warning | Agent configuration package too large | |
| **Attack-, Scan-, and Probe-Related Events** | | | |
| 7000 | Warning | Computer OS Fingerprint Probe | |
| 7001 | Warning | Network or Port Scan | |
| 7002 | Warning | TCP Null Scan | |
| 7003 | Warning | TCP SYNFIN Scan | |
| 7004 | Warning | TCP Xmas Scan | |
| **Download Security Update Events** | | | |
| 9050 | Info | Update of Anti-Malware Component on Agent Succeeded | |
| 9051 | Error | Update of Anti-Malware Component on Agent Failed | |
| 9100 | Info | Security Update Successful | |
| 9101 | Error | Security Update Failure | |
| 9102 | Error | Security Update Failure | Specific information recorded in error message. |
| **Relay Events** | | | |
| 9103 | Info | Relay Web Server Disabled | |
| 9104 | Info | Relay Web Server Enabled | |
| 9105 | Error | Enable Relay Web Server Failed | |
| 9106 | Error | Disable Relay Web Server Failed | |
| 9107 | Error | Relay Web Server failed | |
| 9108 | Info | Unable to Connect to Update Source | |
| 9109 | Error | Component Update Failure | |

| ID | Severity | Event | Notes |
|---|---|---|---|
| 9110 | Error | Anti-Malware license is expired | |
| 9111 | Info | Security Update Rollback Success | |
| 9112 | Error | Security Update Rollback Failure | |
| 9113 | Info | Relay Replicated All Packages | |
| 9114 | Error | Relay Failed to Replicate All Packages | |
| 9115 | Info | Failed to download from the Relay Web Server | |
| **Integrity Scan Status Events** | | | |
| 9201 | Info | Integrity Scan Started | |
| 9203 | Info | Integrity Scan Terminated Abnormally | |
| 9204 | Info | Integrity Scan Paused | |
| 9205 | Info | Integrity Scan Resumed | |
| 9208 | Warning | Integrity Scan failed to start | |
| 9209 | Warning | Integrity Scan Stalled | |
| **Smart Protection Server Status Events** | | | |
| 9300 | Warning | Smart Protection Server Disconnected for Web Reputation | See "Troubleshoot "Smart Protection Server disconnected" errors" on page 1310. |
| 9301 | Info | Smart Protection Server Connected for Web Reputation | See "Troubleshoot "Smart Protection Server disconnected" errors" on page 1310. |
| 9302 | Warning | Census, Good File Reputation, and Predictive Machine Learning Service Disconnected | |
| 9303 | Info | Census, Good File Reputation, and Predictive Machine Learning Service Connected | |

## System events

To view system events, go to **Events & Reports > Events**.

To configure system events, go to the **Administration > System Settings > System Events** tab. On this tab you can set whether or not to record individual events and whether or not to forward them to a SIEM server. If you select **Record**, then the event is saved to the database. If you deselect **Record**, then the event does not appear under the **Events & Reports** tab (or anywhere in Deep Security Manager) and it is not forwarded either.

Depending on whether it is a system configuration change or security incident, each log appears in either the **System Events** submenu or the submenu corresponding to the event's protection module, such as **Anti-Malware Events**.

These events sometimes also appear in the **Status** column on **Computers**.

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 0 | Error | Unknown Error | |
| 100 | Info | Deep Security Manager Started | |
| 101 | Info | License Changed | |
| 107 | Info | Rule Update Downloaded and Applied | |
| 108 | Info | Script Executed | |
| 109 | Error | Script Execution Failed | |
| 110 | Info | System Events Exported | |
| 111 | Info | Firewall Events Exported | |
| 112 | Info | Intrusion Prevention Events Exported | |
| 115 | Info | Rule Update Downloaded | |
| 116 | Info | Rule Update Applied | |
| 117 | Info | Deep Security Manager Shutdown | |
| 118 | Warning | Deep Security Manager Offline | |
| 119 | Info | Deep Security Manager Back Online | |
| 120 | Error | Heartbeat Server Failed | The server within Deep Security Manager that listens for incoming agent heartbeats did not start. Check that the manager's incoming heartbeat port number is not in use by another application on the server. Once the port is free, the manager's heartbeat server should bind to it, and this error should be fixed. |
| 121 | Error | Scheduler Failed | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 122 | Error | Manager Message Thread Failed | An internal thread has failed. There is no resolution for this error. If it persists, please contact customer support. |
| 123 | Info | Deep Security Manager Forced Shutdown | |
| 124 | Info | Rule Update Deleted | |
| 130 | Info | Credentials Generated | |
| 140 | Info | Discover Computers | |
| 141 | Warning | Discover Computers Failed | |
| 142 | Info | Discover Computers Requested | |
| 143 | Info | Discover Computers Canceled | |
| 150 | Info | System Settings Saved | |
| 151 | Info | Software Added | |
| 152 | Info | Software Deleted | |
| 153 | Info | Software Updated | |
| 154 | Info | Software Exported | |
| 156 | Error | Agent Installer Digital Signature Verification Failed | '<agent>.zip' has been deleted because the digital signature verification failed. The failure indicates that the file may have been tampered with. Details:<br><detailed_message><br>Please contact Trend Micro support for more help.<br>See "Check digital signatures on software packages" on page 494 for details. |
| 160 | Info | Authentication Failed | |
| 161 | Info | Rule Update Exported | |
| 162 | Info | Log Inspection Events Exported | |
| 163 | Info | Anti-Malware Event Exported | |
| 164 | Info | Security Update Successful | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 165 | Error | Security Update Failed | |
| 169 | Error | Manual Security Update Failed | |
| 170 | Error | Manager Available Disk Space Too Low | The manager does not have enough free disk space to function and will shut down. Either expand the disk space or delete unused files to free some disk space, then "Restart the Deep Security Manager" on page 1560. |
| 171 | Info | Anti-Malware Spyware Item Exported | |
| 172 | Info | Web Reputation Events Exported | |
| 173 | Info | Anti-Malware Identified Files List Exported | |
| 174 | Info | Anti-Malware Unauthorized Change Targeted Item Exported | |
| 175 | Info | Creating Heap Dump | |
| 176 | Info | Heap Dump Created | |
| 177 | Error | Failed to create Heap Dump | |
| 180 | Info | Alert Type Updated | |
| 190 | Info | Alert Started | |
| 191 | Info | Alert Changed | |
| 192 | Info | Alert Ended | |
| 197 | Info | Alert Emails Sent | |
| 198 | Warning | Alert Emails Failed | An alert email could not be sent. Verify that your SMTP settings are correct. |
| 199 | Error | Alert Processing Failed | The current alert status could be inaccurate because an alert was not completely processed. If the problem persists, contact your support provider. |
| 247 | Warning | Agent Integrity Check Failed | |
| 248 | Info | Software Update: Disable Relay Requested | |
| 249 | Info | Software Update: Enable Relay Requested | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 250 | Info | Computer Created | |
| 251 | Info | Computer Deleted | |
| 252 | Info | Computer Updated | |
| 253 | Info | Policy Assigned to Computer | |
| 254 | Info | Computer Moved | |
| 255 | Info | Activation Requested | |
| 256 | Info | Send Policy Requested | |
| 257 | Info | Locked | |
| 258 | Info | Unlocked | |
| 259 | Info | Deactivation Requested | |
| 260 | Info | Scan for Open Ports | |
| 261 | Warning | Scan for Open Ports Failed | |
| 262 | Info | Scan for Open Ports Requested | |
| 263 | Info | Scan for Open Ports Canceled | |
| 264 | Info | Agent Software Upgrade Requested | |
| 265 | Info | Agent Software Upgrade Cancelled | |
| 266 | Info | Warnings/Errors Cleared | |
| 267 | Info | Check Status Requested | |
| 268 | Info | Get Events Requested | |
| 269 | Info | Computer Added to Cloud Connector | |
| 270 | Error | Computer Creation Failed | |
| 271 | Info | Agent Software Upgrade Timed Out | |
| 272 | Info | Appliance Software Upgrade Timed Out | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 273 | Info | Security Update: Security Update Check and Download Requested | |
| 274 | Info | Security Update: Security Update Rollback Requested | |
| 275 | Warning | Duplicate Computer | |
| 276 | Info | Update: Summary Information | |
| 277 | Info | Upgrade on Activation Skipped | The agent was eligible for an automatic upgrade, but the upgrade did not occur. For more information, see "Automatically upgrade agents on activation" on page 1388. |
| 278 | Info | Software Update: Reboot to Complete Agent Software Upgrade | |
| 280 | Info | Computers Exported | |
| 281 | Info | Computers Imported | |
| 287 | Info | Relay Group Assigned to Computer | |
| 290 | Info | Group Added | |
| 291 | Info | Group Removed | |
| 292 | Info | Group Updated | |
| 293 | Info | Interface Renamed | |
| 294 | Info | Computer Bridge Renamed | |
| 295 | Info | Interface Deleted | |
| 297 | Info | Recommendation Scan Requested | |
| 298 | Info | Recommendations Cleared | |
| 299 | Info | Asset Value Assigned to Computer | |
| 300 | Info | Recommendation Scan Completed | |
| 301 | Info | Agent Software Deployment | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | Requested | |
| 302 | Info | Agent Software Removal Requested | |
| 303 | Info | Computer Renamed | |
| 305 | Info | Scan for Integrity Requested | |
| 306 | Info | Rebuild Baseline Requested | |
| 307 | Info | Cancel Update Requested | |
| 308 | Info | Integrity Monitoring Rule Compile Issue | |
| 309 | Info | Integrity Monitoring Rule Compile Issue Resolved | |
| 310 | Info | Directory Added | |
| 311 | Info | Directory Removed | |
| 312 | Info | Directory Updated | |
| 321 | Info | Directory Synchronization Finished | |
| 322 | Error | Directory Synchronization Failed | |
| 323 | Info | Directory Synchronization Requested | |
| 326 | Info | User Synchronization Finished | Synchronization of the user accounts with Microsoft Active Directory has completed. |
| 327 | Error | User Synchronization Failed | |
| 330 | Info | SSL Configuration Created | |
| 331 | Info | SSL Configuration Deleted | |
| 332 | Info | SSL Configuration Updated | |
| 333 | Info | Host Merge Finished | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 334 | Error | Host Merge Failed | |
| 338 | Warning | Directory Synchronization Limit Exceeded | Reached the limit of total group members for Active Directory synchronization. Skipping any remaining members. Consider adjusting the limit in the system setting. |
| 350 | Info | Policy Created | |
| 351 | Info | Policy Deleted | |
| 352 | Info | Policy Updated | |
| 353 | Info | Policies Exported | |
| 354 | Info | Policies Imported | |
| 355 | Info | Scan for Recommendations Canceled | |
| 356 | Error | Secure Boot Public Key Not Enrolled | This error can occur if the public key required to check the signature on the Trend Micro kernel module is not successfully enrolled on the agent computer.<br>For details, see "Configure Linux Secure Boot for agents" on page 527. |
| 357 | Error | Secure Boot 'On' Not Supported | Deep Security Agent does not support this OS with Secure Boot enabled.<br>For details, see "Configure Linux Secure Boot for agents" on page 527. |
| 360 | Info | VMware vCenter Added | |
| 361 | Info | VMware vCenter Removed | |
| 362 | Info | VMware vCenter Updated | |
| 363 | Info | VMware vCenter Synchronization | |
| 364 | Info | VMware vCenter Synchronization Finished | |
| 365 | Error | VMware vCenter Synchronization Failed | |
| 366 | Info | VMware vCenter Synchronization Requested | |
| 367 | Info | VMware vCenter Synchronization Cancelled | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 368 | Warning | Interfaces Out of Sync | Interfaces reported by the Deep Security Virtual Appliance are different than the interfaces reported by the vCenter. This can typically be resolved by rebooting the VM. |
| 369 | Info | Interfaces in Sync | |
| 370 | Info | Filter Driver Installed | |
| 371 | Info | Filter Driver Removed | The VMware ESXi server has been restored to the state it was in before the filter driver software was installed. |
| 372 | Info | Filter Driver Upgraded | |
| 373 | Info | Virtual Appliance Deployed | |
| 374 | Info | Virtual Appliance Upgraded | |
| 375 | Warning | Virtual Appliance Upgrade Failed | |
| 376 | Warning | Virtual Machine Moved to Unprotected ESXi | |
| 377 | Info | Virtual Machine Moved to Protected ESXi | |
| 378 | Warning | Virtual Machine unprotected after move to another ESXi | A VM was moved to an ESXi where there is no Deep Security Virtual Appliance. |
| 379 | Info | Virtual Machine unprotected after move to another ESXi Resolved | |
| 380 | Error | Filter Driver Offline | The filter driver on an ESXi server is offline. Use the VMware vCenter console to troubleshoot problems with the hypervisor and the ESXi. |
| 381 | Info | Filter Driver Back Online | |
| 382 | Info | Filter Driver Upgrade Requested | |
| 383 | Info | Appliance Upgrade Requested | |
| 384 | Warning | Prepare ESXi Failed | |
| 385 | Warning | Filter Driver Upgrade Failed | |
| 386 | Warning | Removal of Filter | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | Driver from ESXi Failed | |
| 387 | Error | Connection to Filter Driver Failure | |
| 388 | Info | Connection to Filter Driver Success | |
| 389 | Error | Multiple Activated Appliances Detected | |
| 390 | Info | Multiple Activated Appliances Detected Resolved | |
| 391 | Error | Network Settings Out of Sync With vCenter Global Settings | |
| 392 | Info | Network Settings in Sync With vCenter Global Settings | |
| 393 | Error | Anti-Malware Engine Offline | The anti-malware protection module is not functioning. This is probably because the VMware environment does not meet the requirements. See "System requirements" on page 383. |
| 394 | Info | Anti-Malware Engine Back Online | |
| 395 | Error | Virtual Appliance is Incompatible With Filter Driver | |
| 396 | Info | Virtual Appliance is Incompatible With Filter Driver Resolved | |
| 397 | Warning | VMware NSX Callback Authentication Failed | |
| 398 | Error | VMware Tools Not Installed | |
| 399 | Info | VMware Tools Not Installed Resolved | |
| 410 | Info | Firewall Rule Created | |
| 411 | Info | Firewall Rule | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | Deleted | |
| 412 | Info | Firewall Rule Updated | |
| 413 | Info | Firewall Rule Exported | |
| 414 | Info | Firewall Rule Imported | |
| 420 | Info | Firewall Stateful Configuration Created | |
| 421 | Info | Firewall Stateful Configuration Deleted | |
| 422 | Info | Firewall Stateful Configuration Updated | |
| 423 | Info | Firewall Stateful Configuration Exported | |
| 424 | Info | Firewall Stateful Configuration Imported | |
| 460 | Info | Application Type Created | An administrator configured a new IPS network application definition. |
| 461 | Info | Application Type Deleted | An administrator removed an IPS network application definition. |
| 462 | Info | Application Type Updated | An administrator changed an existing IPS network application definition. |
| 463 | Info | Application Type Exported | An administrator downloaded an IPS network application definition. |
| 464 | Info | Application Type Imported | An administrator uploaded an IPS network application definition. |
| 470 | Info | Intrusion Prevention Rule Created | |
| 471 | Info | Intrusion Prevention Rule Deleted | |
| 472 | Info | Intrusion Prevention Rule Updated | |
| 473 | Info | Intrusion Prevention Rule Exported | |
| 474 | Info | Intrusion Prevention Rule | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | Imported | |
| 480 | Info | Integrity Monitoring Rule Created | |
| 481 | Info | Integrity Monitoring Rule Deleted | |
| 482 | Info | Integrity Monitoring Rule Updated | |
| 483 | Info | Integrity Monitoring Rule Exported | |
| 484 | Info | Integrity Monitoring Rule Imported | |
| 490 | Info | Log Inspection Rule Created | |
| 491 | Info | Log Inspection Rule Deleted | |
| 492 | Info | Log Inspection Rule Updated | |
| 493 | Info | Log Inspection Rule Exported | |
| 494 | Info | Log Inspection Rule Imported | |
| 495 | Info | Log Inspection Decoder Created | |
| 496 | Info | Log Inspection Decoder Deleted | |
| 497 | Info | Log Inspection Decoder Updated | |
| 498 | Info | Log Inspection Decoder Exported | |
| 499 | Info | Log Inspection Decoder Imported | |
| 505 | Info | Context Created | |
| 506 | Info | Context Deleted | |
| 507 | Info | Context Updated | |
| 508 | Info | Context Exported | |
| 509 | Info | Context Imported | |
| 510 | Info | IP List Created | |
| 511 | Info | IP List Deleted | |
| 512 | Info | IP List Updated | |
| 513 | Info | IP List Exported | |
| 514 | Info | IP List Imported | |
| 520 | Info | Port List Created | |
| 521 | Info | Port List Deleted | |
| 522 | Info | Port List Updated | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 523 | Info | Port List Exported | |
| 524 | Info | Port List Imported | |
| 525 | Info | Scan Cache Configuration Created | |
| 526 | Info | Scan Cache Configuration Exported | |
| 527 | Info | Scan Cache Configuration Updated | |
| 530 | Info | MAC List Created | |
| 531 | Info | MAC List Deleted | |
| 532 | Info | MAC List Updated | |
| 533 | Info | MAC List Exported | |
| 534 | Info | MAC List Imported | |
| 540 | Info | Proxy Created | |
| 541 | Info | Proxy Deleted | |
| 542 | Info | Proxy Updated | |
| 543 | Info | Proxy Exported | |
| 544 | Info | Proxy Imported | |
| 550 | Info | Schedule Created | |
| 551 | Info | Schedule Deleted | |
| 552 | Info | Schedule Updated | |
| 553 | Info | Schedule Exported | |
| 554 | Info | Schedule Imported | |
| 560 | Info | Scheduled Task Created | |
| 561 | Info | Scheduled Task Deleted | |
| 562 | Info | Scheduled Task Updated | |
| 563 | Info | Scheduled Task Manually Executed | |
| 564 | Info | Scheduled Task Started | |
| 567 | Info | Sending Outstanding Alert Summary | |
| 568 | Warning | Failed To Send Outstanding Alert Summary | |
| 569 | Warning | Email Failed | An e-mail notification could not be sent. Verify that your SMTP settings are correct. |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 570 | Info | Sending Report | |
| 571 | Warning | Failed To Send Report | |
| 572 | Error | Invalid Report Jar | |
| 573 | Info | Asset Value Created | |
| 574 | Info | Asset Value Deleted | |
| 575 | Info | Asset Value Updated | |
| 576 | Error | Report Uninstall Failed | |
| 577 | Error | Report Uninstalled | |
| 578 | Warning | Integrity Monitoring Rules Require Configuration | |
| 580 | Warning | Application Type Port List Misconfiguration | |
| 581 | Warning | Application Type Port List Misconfiguration Resolved | |
| 582 | Warning | Intrusion Prevention Rules Require Configuration | |
| 583 | Info | Intrusion Prevention Rules Require Configuration Resolved | |
| 584 | Warning | Application Types Require Configuration | IPS rules require network application definitions, and cannot correctly scan traffic until you define them. |
| 585 | Info | Integrity Monitoring Rules Require Configuration Resolved | |
| 586 | Warning | Log Inspection Rules Require Configuration | |
| 587 | Info | Log Inspection Rules Require Configuration Resolved | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 588 | Warning | Log Inspection Rules Require Log Files | |
| 589 | Info | Log Inspection Rules Require Log Files Resolved | |
| 590 | Warning | Scheduled Task Unknown Type | |
| 591 | Info | Relay Group Created | |
| 592 | Info | Relay Group Updated | |
| 593 | Info | Relay Group Deleted | |
| 594 | Info | Event-Based Task Created | |
| 595 | Info | Event-Based Task Deleted | |
| 596 | Info | Event-Based Task Updated | |
| 597 | Info | Event-Based Task Triggered | |
| 600 | Info | User Signed In | |
| 601 | Info | User Signed Out | |
| 602 | Info | User Timed Out | |
| 603 | Info | User Locked Out | |
| 604 | Info | User Unlocked | |
| 605 | Info | User Session Terminated | |
| 608 | Error | User Session Validation Failed | Deep Security Manager could not confirm that a session was initiated after successful authentication. The user will be redirected to the login page, and asked to re-authenticate. This could be normal if the authenticated session list was cleared. |
| 609 | Error | User Made Invalid Request | Deep Security Manager received invalid request to access audit data (events). Access was denied. |
| 610 | Info | User Session Validated | |
| 611 | Info | User Viewed Firewall Event | |
| 613 | Info | User Viewed Intrusion Prevention Event | |
| 615 | Info | User Viewed System Event | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 616 | Info | User Viewed Integrity Monitoring Event | |
| 617 | Info | User Viewed Log Inspection Event | |
| 618 | Info | User Viewed Identified File Detail | |
| 619 | Info | User Viewed Anti-Malware Event | |
| 620 | Info | User Viewed Web Reputation Event | |
| 621 | Info | User Signed In As Tenant | |
| 622 | Info | Access from Primary Tenant Enabled | |
| 623 | Info | Access from Primary Tenant Disabled | |
| 624 | Info | Access from Primary Tenant Allowed | |
| 625 | Info | Access from Primary Tenant Revoked | |
| 626 | Info | Access from Primary Tenant Expired | |
| 630 | Info | Syslog Configuration Created | |
| 631 | Info | Syslog Configuration Deleted | |
| 632 | Info | Syslog Configuration Updated | |
| 633 | Info | Syslog Configuration Exported | |
| 634 | Info | Syslog Configuration Imported | |
| 650 | Info | User Created | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 651 | Info | User Deleted | |
| 652 | Info | User Updated | |
| 653 | Info | User Password Set | |
| 656 | Info | API Key Created | |
| 657 | Info | API Key Deleted | |
| 658 | Info | API Key Updated | |
| 660 | Info | Role Created | |
| 661 | Info | Role Deleted | |
| 662 | Info | Role Updated | |
| 670 | Info | Contact Created | |
| 671 | Info | Contact Deleted | |
| 672 | Info | Contact Updated | |
| 673 | Info | API Key Locked Out | |
| 674 | Info | API Key Unlocked | |
| 675 | Error | API Key Session Validation Failed | |
| 678 | Info | API Key Expired | |
| 690 | Info | Microservice API Key Created | |
| 691 | Info | Microservice API Key Deleted | |
| 692 | Info | Microservice API Key Updated | |
| 693 | Info | Microservice API Key Locked Out | |
| 694 | Info | Microservice API Key Unlocked | |
| 695 | Error | Microservice API Key Session Validation Failed | |
| 696 | Info | Microservice API Key Expired | |
| 701 | Error | Agent Software Installation Failed | |
| 702 | Info | Credentials Generated | |
| 703 | Error | Credential Generation Failed | |
| 704 | Info | Activated | |
| 705 | Error | Activation Failed | This can occur if agent self-protection is enabled. On the |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | | Deep Security Manager, go to **Computer editor**[1] **> Settings > General**. In **Agent Self Protection**, and then either deselect **Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent** or enter a password for local override. |
| 706 | Info | Software Update: Agent Software Upgraded | |
| 707 | Warning | Software Update: Agent Software Upgrade Failed | Refer to the event details for more information about why the upgrade was not successful. |
| 708 | Info | Deactivated | |
| 709 | Error | Deactivation Failed | |
| 710 | Info | Events Retrieved | |
| 711 | Info | Agent Software Deployed | |
| 712 | Error | Agent Software Deployment Failed | This can occur if agent self-protection is enabled. On the Deep Security Manager, go to **Computer editor**[2] **> Settings > General**. In **Agent Self Protection**, and then either deselect **Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent** or enter a password for local override. |
| 713 | Info | Agent Software Removed | |
| 714 | Error | Agent Software Removal Failed | This can occur if agent self-protection is enabled. On the Deep Security Manager, go to **Computer editor**[3] **> Settings > General**. In **Agent Self Protection**, and then either deselect **Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent** or enter a password for local override. |
| 715 | Info | Agent/Appliance Version Changed | |
| 716 | Info | Reactivation Attempted by Unknown Agent | An agent that is currently unknown to the Deep Security Manager has attempted reactivation. This usually happens when a computer was deleted from Deep Security Manager without first removing the agent on the |

[1] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[3] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | | computer. For more information, see the 'Reactivation Attempted by Unknown Agent' section in Agent settings. |
| 720 | Info | Policy Sent | Agent/Appliance updated. |
| 721 | Error | Send Policy Failed | |
| 722 | Warning | Get Interfaces Failed | |
| 723 | Info | Get Interfaces Failure Resolved | |
| 724 | Warning | Insufficient Disk Space | An agent detected low disk space. Free space on the computer. See "Warning: Insufficient disk space" on page 1333. |
| 725 | Warning | Events Suppressed | |
| 726 | Warning | Get Agent/Appliance Events Failed | Manager was unable to retrieve Events from Agent/Appliance. This error does not mean that the data was lost on the Agent/Appliance. This error is normally caused by a network interruption while events are being transferred. Clear the error and run a Check Status to retry the operation. |
| 727 | Info | Get Agent/Appliance Events Failure Resolved | |
| 728 | Error | Get Events Failed | Manager was unable to retrieve audit data from Agent/Appliance. This error does not mean that the data was lost on the Agent/Appliance. This error is usually caused by a network interruption while events are being transferred. Clear the error and run Get Events Now to retry the operation. |
| 729 | Info | Get Events Failure Resolved | |
| 730 | Error | Offline | Manager cannot communicate with Computer. Usually, however, the offline Agent is still protecting the computer with its last configured settings. See Computer and Agent/Appliance Status and "Offline agent" on page 1697. |
| 731 | Info | Back Online | |
| 732 | Error | Firewall Engine Offline | The Firewall Engine is offline and traffic is flowing unfiltered. This is normally due to an error during installation or verification of the driver on the computer's OS platform. Check the status of the network driver at the computer to ensure it is properly loaded. |
| 733 | Info | Firewall Engine Back Online | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 734 | Warning | Computer Clock Change | A clock change has occurred on the Computer which exceeds the maximum allowed specified in **Computer or Policy editor**[1] > Settings > General > Heartbeat area. Investigate what has caused the clock change on the computer. |
| 735 | Warning | Misconfiguration Detected | The Agent's configuration does not match the configuration indicated in the Manager's records. This is typically because of a recent backup restoration of the Manager or the Agent. Unanticipated misconfiguration warnings should be investigated. |
| 736 | Info | Check Status Failure Resolved | |
| 737 | Error | Check Status Failed | See "Error: Check Status Failed" on page 1318. |
| 738 | Error | Intrusion Prevention Engine Offline | The Intrusion Prevention Engine is offline and traffic is flowing unfiltered. This is normally due to an error during installation or verification of the driver on the computer's OS platform. Check the status of the network driver at the computer to ensure it is properly loaded. |
| 739 | Info | Intrusion Prevention Engine Back Online | |
| 740 | Error | Agent/Appliance Error | |
| 741 | Warning | Abnormal Restart Detected | |
| 742 | Warning | Communications Problem | The Agent is having problems communicating its status to Manager. It usually indicates network or load congestion in the Agent --> Manager direction. Further investigation is warranted if the situation persists |
| 743 | Info | Communications Problem Resolved | |
| 745 | Warning | Events Truncated | |
| 748 | Error | Log Inspection Engine Offline | |
| 749 | Info | Log Inspection Engine Back Online | |
| 755 | Info | Deep Security Manager Version Compatibility | |

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | Resolved | |
| 756 | Warning | Deep Security Manager Upgrade Recommended (Incompatible Security Update (s)) | Each security module rule (such as Firewall, Anti-Malware, and the others) has a specific minimum Deep Security Manager version that's required in order for the rule to run.<br>Your current Deep Security Manager version is less than the rule's minimum supported version. Upgrade your Deep Security Manager to clear the warning and run the rule. |
| 760 | Info | Agent/Appliance Version Compatibility Resolved | |
| 761 | Warning | Agent/Appliance Upgrade Recommended | |
| 762 | Warning | Agent/Appliance Upgrade Required | Your current Deep Security Agent or Deep Security Virtual Appliance version is less than the Deep Security Manager's minimum supported version. Upgrade your Agent/Appliance. |
| 763 | Error | Incompatible Agent/Appliance Version | Your current Deep Security Manager version is less than the Deep Security Agent or Deep Security Virtual Appliance's minimum supported version. Upgrade your manager. |
| 764 | Warning | Agent/Appliance Upgrade Recommended (Incompatible Security Updates) | Each security module rule (such as Firewall, Anti-Malware, and others) has a specific minimum Deep Security Agent or Deep Security Virtual Appliance version required for the rule to run.<br>Your current Deep Security Agent or Deep Security Virtual Appliance version is less than the rule's minimum supported version. Upgrade your Deep Security Agent or Deep Security Virtual Appliance to clear the warning and run the rule. |
| 765 | Error | Computer Reboot Required | |
| 766 | Warning | Network Engine Mode Configuration | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | Incompatibility | |
| 767 | Warning | Network Engine Mode Version Incompatibility | |
| 768 | Warning | Network Engine Mode Incompatibility Resolved | |
| 770 | Warning | Agent/Appliance Heartbeat Rejected | |
| 771 | Warning | Contact by Unrecognized Client | See "Troubleshoot event ID 771 "Contact by Unrecognized Client"" on page 1309. |
| 780 | Info | Recommendation Scan Failure Resolved | |
| 781 | Warning | Recommendation Scan Failure | See "Troubleshooting: Recommendation Scan Failure" on page 649. |
| 782 | Info | Rebuild Baseline Failure Resolved | |
| 783 | Warning | Rebuild Baseline Failure | |
| 784 | Info | Security Update: Security Update Check and Download Successful | |
| 785 | Warning | Security Update: Security Update Check and Download Failed | |
| 786 | Info | Scan For Change Failure Resolved | |
| 787 | Warning | Scan For Change Failure | |
| 790 | Info | Agent-Initiated Activation Requested | |
| 791 | Warning | Agent-Initiated Activation Failure | |
| 792 | Info | Manual Malware Scan Failure Resolved | |
| 793 | Warning | Manual Malware Scan Failure | A Malware Scan has failed. Use the VMware vCenter console to check the status of the VM on which the scan |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | | failed. See also "Anti-Malware scan failures and cancellations" on page 1054. |
| 794 | Info | Scheduled Malware Scan Failure Resolved | |
| 795 | Warning | Scheduled Malware Scan Failure | A scheduled Malware Scan has failed. Use the VMware vCenter console to check the status of the VM on which the scan failed. See also "Anti-Malware scan failures and cancellations" on page 1054. |
| 796 | Warning | Scheduled Malware Scan Task has been Missed | This occurs when a scheduled Malware Scan is initiated on a computer when a previous scan is still pending. This typically indicates that Malware Scans are being scheduled too frequently. |
| 797 | Info | Malware Scan Cancellation Failure Resolved | |
| 798 | Warning | Malware Scan Cancellation Failure | A Malware Scan cancellation has failed. Use the VMware vCenter console to check the status of the VM on which the scan failed. |
| 799 | Warning | Malware Scan Stalled | A Malware Scan has stalled. Use the VMware vCenter console to check the status of the VM on which the scan stalled. |
| 800 | Info | Alert Dismissed | |
| 801 | Info | Error Dismissed | |
| 803 | Warning | Agent Configuration Package too Large | |
| 804 | Error | Intrusion Prevention Rule Compiler Failed | |
| 805 | Error | Intrusion Prevention Rules Failed to Compile | |
| 806 | Error | Intrusion Prevention Rules Failed to Compile | |
| 850 | Warning | Reconnaissance Detected: Computer OS Fingerprint Probe | See "Warning: Reconnaissance Detected" on page 1333 |
| 851 | Warning | Reconnaissance Detected: Network or Port Scan | See "Warning: Reconnaissance Detected" on page 1333 |
| 852 | Warning | Reconnaissance Detected: TCP Null Scan | See "Warning: Reconnaissance Detected" on page 1333 |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 853 | Warning | Reconnaissance Detected: TCP SYNFIN Scan | See "Warning: Reconnaissance Detected" on page 1333 |
| 854 | Warning | Reconnaissance Detected: TCP Xmas Scan | See "Warning: Reconnaissance Detected" on page 1333 |
| 900 | Info | Deep Security Manager Audit Started | |
| 901 | Info | Deep Security Manager Audit Shutdown | |
| 902 | Info | Deep Security Manager Installed | |
| 904 | Info | Diagnostic Logging Enabled | |
| 905 | Info | Diagnostic Logging Completed | |
| 906 | Info | Java Flight Recorder Enabled | Java Flight Recorder has been enabled with parameters values specified in the event description. |
| 907 | Info | Java Flight Recorder Completed | Java Flight Recorder recording session completed. |
| 910 | Info | Diagnostic Package Generated | |
| 911 | Info | Diagnostic Package Exported | |
| 914 | Info | Identified File Deletion Succeeded | |
| 915 | Info | Identified File Deletion Failed | |
| 916 | Info | Identified File Download Succeeded | |
| 917 | Info | Identified File Download Failed | |
| 918 | Info | Identified File Administration Utility Download Succeeded | |
| 919 | Info | Identified File Not Found | |
| 924 | Warning | File cannot be analyzed or | The Anti-Malware module was unable to analyze or quarantine a file because the VM maximum disk space |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | quarantined (VM maximum disk space used to store identified files exceeded) | used to store identified files was reached. To change the maximum disk space for identified files setting, open the computer or policy editor and go to the **Anti-malware > Advanced** tab. |
| 925 | Warning | Maximum disk space used for storing identified files has been exceeded. Older identified files might be purged or newly detected files might not be analyzed or quarantined. | The maximum disk space used for storing identified files has been reached. As a result, the Anti-Malware module may purge older identified files or the Anti-Malware module may be unable to analyze or quarantine a file. To change the maximum disk space for the identified files setting, open the **Computer** or **Policy** editor and select the **Anti-malware > Advanced** tab. |
| 926 | Warning | Smart Protection Server Disconnected for Smart Scan | See "Troubleshoot "Smart Protection Server disconnected" errors" on page 1310. |
| 927 | Info | Smart Protection Server Connected for Smart Scan | |
| 928 | Info | Identified File Restoration Succeeded | |
| 929 | Warning | Identified File Restoration Failed | |
| 930 | Info | Certificate Accepted | |
| 931 | Info | Certificate Deleted | |
| 932 | Warning | Smart Protection Server Disconnected for Web Reputation | See "Troubleshoot "Smart Protection Server disconnected" errors" on page 1310. |
| 933 | Info | Smart Protection Server Connected for Web Reputation | |
| 934 | Info | Software Update: Anti-Malware Windows Platform Update Successful | |
| 935 | Error | Software Update: Anti-Malware Windows Platform Update Failed | See "Anti-Malware Windows platform update failed" on page 1702 |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 936 | Info | Submission of identified file to Deep Discovery Analyzer succeeded | |
| 937 | Info | Submission of identified file to Deep Discovery Analyzer failed | |
| 938 | Info | Identified File Submission Queued | |
| 940 | Info | Auto-Tag Rule Created | |
| 941 | Info | Auto-Tag Rule Deleted | |
| 942 | Info | Auto-Tag Rule Updated | |
| 943 | Info | Tag Deleted | |
| 944 | Info | Tag Created | |
| 945 | Warning | Census, Good File Reputation, and Predictive Machine Learning Service Disconnected | |
| 946 | Info | Census, Good File Reputation, and Predictive Machine Learning Service Connected | |
| 947 | Info | FIPS Mode Enabled | |
| 948 | Info | FIPS Mode Disabled | |
| 949 | Warning | Computer reboot is required to complete the Deep Security Agent installation with Windows installer | A computer reboot is required to complete the Deep Security Agent installation with Windows installer. |
| 950 | Warning | A computer reboot is required to enable Deep Security Agent protection | A computer reboot is required to disable Windows Defender and enable Deep Security Agent protection. |
| 970 | Info | Command Line | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | Utility Started | |
| 978 | Info | Command Line Utility Failed | |
| 979 | Info | Command Line Utility Shutdown | Deep Security Manager was manually stopped. |
| 990 | Info | Manager Node Added | |
| 991 | Info | Manager Node Decommissioned | |
| 992 | Info | Manager Node Updated | |
| 995 | Info | Connection to the Certified Safe Software Service has been restored | |
| 996 | Warning | Unable to connect to the Certified Safe Software Service | |
| 997 | Error | Tagging Error | |
| 998 | Error | System Event Notification Error | |
| 999 | Error | Internal Software Error | |
| 1101 | Error | Plug-in Installation Failed | |
| 1102 | Info | Plug-in Installed | |
| 1103 | Error | Plug-in Upgrade Failed | |
| 1104 | Info | Plug-in Upgraded | |
| 1105 | Error | Plug-in Start Failed | |
| 1106 | Error | Plug-in Uninstall Failed | |
| 1107 | Info | Plug-in Uninstalled | |
| 1108 | Info | Plug-in Started | |
| 1109 | Info | Plug-in Stopped | |
| 1110 | Error | Software Package Not Found | Agent software package was not found or a newer package is required. |
| 1111 | Info | Software Package Found | |
| 1112 | Error | Kernel Unsupported | The Linux driver cannot be installed because your computer may have been upgraded to an unsupported kernel. For more information, see "Linux kernel compatibility" on page 408. |
| 1204 | Info | Identified file | The download request has been sent. Please check for |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | download requested | event ID 1209 for the latest update. Files that are "Ready for download" will be available for 24 hours. |
| 1205 | Info | Identified file download request failed | The download request could not be sent successfully. |
| 1208 | Info | Identified file download request timeout | The download request has timeout due to reaching the 2-day limit. |
| 1209 | Info | Identified file is ready for download | Identified file is ready for download. Please download the file within 24 hours. |
| 1500 | Info | Malware Scan Configuration Created | |
| 1501 | Info | Malware Scan Configuration Deleted | |
| 1502 | Info | Malware Scan Configuration Updated | |
| 1503 | Info | Malware Scan Configuration Exported | |
| 1504 | Info | Malware Scan Configuration Imported | |
| 1505 | Info | Directory List Created | |
| 1506 | Info | Directory List Deleted | |
| 1507 | Info | Directory List Updated | |
| 1508 | Info | Directory List Exported | |
| 1509 | Info | Directory List Imported | |
| 1510 | Info | File Extension List Created | |
| 1511 | Info | File Extension List Deleted | |
| 1512 | Info | File Extension List Updated | |
| 1513 | Info | File Extension List Exported | |
| 1514 | Info | File Extension List Imported | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 1515 | Info | File List Created | |
| 1516 | Info | File List Deleted | |
| 1517 | Info | File List Updated | |
| 1518 | Info | File List Exported | |
| 1519 | Info | File List Imported | |
| 1520 | Info | Manual Malware Scan Pending | |
| 1521 | Info | Manual Malware Scan Started | |
| 1522 | Info | Manual Malware Scan Completed | |
| 1523 | Info | Scheduled Malware Scan Started | |
| 1524 | Info | Scheduled Malware Scan Completed | |
| 1525 | Info | Manual Malware Scan Cancellation In Progress | |
| 1526 | Info | Manual Malware Scan Cancellation | This event can have several causes. See "Anti-Malware scan failures and cancellations" on page 1054. |
| 1527 | Info | Scheduled Malware Scan Cancellation In Progress | |
| 1528 | Info | Scheduled Malware Scan Cancellation | This event can have several causes. See "Anti-Malware scan failures and cancellations" on page 1054. |
| 1529 | Info | Manual Malware Scan Paused | |
| 1530 | Info | Manual Malware Scan Resumed | |
| 1531 | Info | Scheduled Malware Scan Paused | |
| 1532 | Info | Scheduled Malware Scan Resumed | |
| 1533 | Info | A computer reboot is required to complete an Anti-Malware cleanup or restoration task | A computer reboot is required to complete an Anti-Malware cleanup or restoration task. |
| 1534 | Error | Computer reboot required for Anti- | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | Malware protection | |
| 1535 | Info | Anti-Malware cleanup task must be performed manually | |
| 1536 | Info | Quick Malware Scan Pending | |
| 1537 | Info | Quick Malware Scan Started | |
| 1538 | Info | Quick Malware Scan Completed | |
| 1539 | Info | Quick Malware Scan Cancellation In Progress | |
| 1540 | Info | Quick Malware Scan Cancellation | This event can have several causes. See "Anti-Malware scan failures and cancellations" on page 1054. |
| 1541 | Info | Quick Malware Scan Paused | |
| 1542 | Info | Quick Malware Scan Failure Resolved | |
| 1543 | Warning | Quick Malware Scan Failure | See "Anti-Malware scan failures and cancellations" on page 1054. |
| 1544 | Info | Quick Malware Scan Resumed | |
| 1545 | Info | Files could not be scanned for malware | Anti-malware could not scan a file because its file path exceeded the maximum number of characters. Maximum file path length varies by OS and file system. To prevent this problem, try moving the file to a directory path and file name with fewer characters. |
| 1546 | Info | Files could not be scanned for malware | Anti-malware could not scan a file because its location exceeded the maximum directory depth. To prevent this problem, try reducing the number of layers of nested directories. |
| 1547 | Info | Scheduled Malware Scan Task has been cancelled | |
| 1550 | Info | Web Reputation Settings Updated | |
| 1551 | Info | Malware Scan Configuration Updated | |
| 1552 | Info | Integrity Configuration | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | Updated | |
| 1553 | Info | Log Inspection Configuration Updated | |
| 1554 | Info | Firewall Stateful Configuration Updated | |
| 1555 | Info | Intrusion Prevention Configuration Updated | |
| 1556 | Info | Anti-Malware scan exclusion setting update | |
| 1600 | Info | Relay Group Update Requested | |
| 1601 | Info | Relay Group Update Success | |
| 1602 | Error | Relay Group Update Failed | |
| 1603 | Info | Security Update: Security Update Rollback Success | |
| 1604 | Warning | Security Update: Security Update Rollback Failure | |
| 1605 | Info | Successfully send file back up command to host | |
| 1606 | Warning | Failed to send file back up command to host | |
| 1607 | Info | Successfully back up file | |
| 1608 | Error | Failed to back up file | |
| 1650 | Warning | Anti-Malware protection is not enabled or is out of date | |
| 1651 | Info | Anti-Malware module is ready | |
| 1660 | Info | Rebuild Baseline Started | |
| 1661 | Info | Rebuild Baseline Paused | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 1662 | Info | Rebuild Baseline Resumed | |
| 1663 | Warning | Rebuild Baseline Failure | |
| 1664 | Warning | Rebuild Baseline Stalled | |
| 1665 | Info | Rebuild Baseline Completed | |
| 1666 | Info | Scan for Integrity Started | |
| 1667 | Info | Scan for Integrity Paused | |
| 1668 | Info | Scan for Integrity Resumed | |
| 1669 | Warning | Scan for Integrity Failure | |
| 1670 | Warning | Scan for Integrity Stalled | |
| 1671 | Info | Scan for Integrity Completed | |
| 1675 | Error | Integrity Monitoring Engine Offline | |
| 1676 | Info | Integrity Monitoring Engine Back Online | |
| 1677 | Error | Trusted Platform Module Error | |
| 1678 | Info | Trusted Platform Module Register Values Loaded | |
| 1679 | Warning | Trusted Platform Module Register Values Changed | |
| 1680 | Info | Trusted Platform Module Checking Disabled | |
| 1681 | Info | Trusted Platform Module Information Unreliable | |
| 1700 | Info | No Agent Detected | |
| 1800 | Error | Deep Security Protection Module Failure | |
| 1801 | Info | Deep Security Protection Module | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | Back to Normal | |
| 1900 | Info | Cloud Account Added | |
| 1901 | Info | Cloud Account Removed | |
| 1902 | Info | Cloud Account Updated | |
| 1904 | Info | Cloud Account Synchronization Finished | |
| 1905 | Error | Cloud Account Synchronization Failed | |
| 1906 | Info | Cloud Account Synchronization Requested | |
| 1907 | Info | Cloud account Synchronization Cancelled | |
| 1908 | Info | AWS Account Synchronization Requested | |
| 1909 | Info | AWS Account Synchronization Finished | |
| 1910 | Error | AWS Account Synchronization Failed | |
| 1911 | Info | AWS Account Added | |
| 1912 | Info | AWS Account Removed | |
| 1913 | Info | AWS Account Updated | |
| 1914 | Info | Azure Account Added | |
| 1915 | Info | Azure Account Removed | |
| 1916 | Info | Azure Account Updated | |
| 1917 | Info | Azure Account Synchronization Finished | |
| 1918 | Error | Azure Account Synchronization Failed | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 1919 | Info | Azure Account Synchronization Requested | |
| 1920 | Warning | Azure Account Synchronization Completed but with Errors | |
| 1921 | Info | vCloud Account Added | |
| 1922 | Info | vCloud Account Removed | |
| 1923 | Info | vCloud Account Updated | |
| 1924 | Info | vCloud Account Synchronization Finished | |
| 1925 | Error | vCloud Account Synchronization Failed | |
| 1926 | Info | vCloud Account Synchronization Requested | |
| 1927 | Info | Upgrade Connector to AWS Account Requested | |
| 1928 | Warning | AWS Account Update Failed | |
| 1929 | Info | Upgrade Connector to AWS Account Finished | |
| 1930 | Info | AWS Account Migration Requested | |
| 1931 | Info | AWS Account Migration In Progress | |
| 1932 | Info | AWS Account Migration Complete | |
| 1933 | Warning | AWS Account Migration Failed | |
| 1934 | Info | GCP Account Migration Requested | |
| 1935 | Info | GCP Account | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | Migration In Progress | |
| 1936 | Info | GCP Account Migration Complete | |
| 1937 | Warning | GCP Account Migration Failed | |
| 1938 | Info | Azure Account Migration Requested | |
| 1939 | Info | Azure Account Migration In Progress | |
| 1940 | Info | Azure Account Migration Complete | |
| 1941 | Warning | Azure Account Migration Failed | |
| 1950 | Info | Tenant Created | |
| 1951 | Info | Tenant Deleted | |
| 1952 | Info | Tenant Updated | |
| 1953 | Info | Tenant Database Server Created | |
| 1954 | Info | Tenant Database Server Deleted | |
| 1955 | Info | Tenant Database Server Updated | |
| 1956 | Info | Tenant Exported | |
| 1957 | Error | Tenant Initialization Failure | |
| 1958 | Info | Tenant Features Updated | |
| 2000 | Info | Scan Cache Configuration Object Added | |
| 2001 | Info | Scan Cache Configuration Object Removed | |
| 2002 | Info | Scan Cache Configuration Object Updated | |
| 2100 | Info | Deep Security as a Service Subscription Started | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 2101 | Info | Deep Security as a Service Subscription Canceled | |
| 2102 | Info | Cleverbridge Quantity Updated | |
| 2103 | Warning | Cleverbridge Quantity Not Updated | |
| 2104 | Info | Cleverbridge Quantity Reset | |
| 2105 | Warning | Cleverbridge Quantity Not Reset | |
| 2106 | Info | Cleverbridge Billing Date Set | |
| 2107 | Warning | Cleverbridge Billing Date Not Set | |
| 2108 | Info | Deep Security as a Service Subscription Payment Received | |
| 2109 | Warning | Deep Security as a Service Subscription Payment Not Received | |
| 2110 | Info | Cleverbridge Notification Received | |
| 2111 | Info | Deep Security as a Service Subscription Deactivated | |
| 2112 | Info | Account Balance Reset | |
| 2113 | Info | Agent Installation Requested | |
| 2114 | Info | AWS Billing Job Started | |
| 2115 | Info | AWS Billing Job Completed | |
| 2116 | Error | AWS Billing failure | Deep Security Manager sent a billing usage record to AWS using the AWS SDK, which the SDK returned with |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | | an exception. If the problem persists, contact your support provider. |
| 2117 | Info | Entitlement Created | |
| 2118 | Info | Entitlement Updated | |
| 2119 | Error | Agent Activation Prevented Due to AWS Metering Billing Usage Data Submission Failure | |
| 2120 | Error | AWS Billing failure | Deep Security Manager encountered an error while executing an AWS billing job. If the problem persists, contact your support provider. |
| 2123 | Error | Azure Marketplace Billing Job Failed | The job used to send host usage statistics to Azure Marketplace for consumption-based billing failed. See the description in the event for details about the error that caused this event. |
| 2126 | Error | Event Storage Settings Publish Job Failed | |
| 2200 | Info | Software Update: Anti-Malware Module Installation Started | |
| 2201 | Info | Software Update: Anti-Malware Module Installation Successful | This event is also triggered by installing Application Control or Integrity Monitoring because they share the same framework as Anti-Malware. |
| 2202 | Warning | Software Update: Anti-Malware Module Installation Failed | |
| 2203 | Info | Software Update: Anti-Malware Module Download Successful | |
| 2204 | Info | Security Update: Pattern Update on Agents/Appliances Successful | |
| 2205 | Warning | Security Update: Pattern Update on Agents/Appliances Failed | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 2206 | Info | Security Update: Pattern Update on Agents/Appliances Skipped | |
| 2207 | Warning | Submission to Sandbox Analysis daily quota reached | |
| 2209 | Warning | Anti-Malware Engine with Basic Functions | Anti-Malware engine has only basic functions available. See Anti-Malware Engine has only Basic Functions for details. |
| 2210 | Info | Required Host Permission Is Allowed: Anti-Malware | |
| 2211 | Error | Host Permission Required: Anti-Malware | |
| 2300 | Info | Software Update: Web Reputation Module Installation Started | |
| 2301 | Info | Software Update: Web Reputation Module Installation Successful | |
| 2302 | Warning | Software Update: Web Reputation Module Installation Failed | |
| 2303 | Info | Software Update: Web Reputation Download Successful | |
| 2304 | Error | Web Reputation Engine Offline | |
| 2305 | Info | Web Reputation Engine Back Online | |
| 2306 | Warning | Web Reputation Engine Working With Limited Functionality | |
| 2307 | Info | Web Reputation Engine Back Online on all Interfaces | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 2308 | Warning | Web Reputation Engine Disabled | |
| 2309 | Info | Web Reputation Engine Enabled | |
| 2400 | Info | Software Update: Firewall Module Installation Started | |
| 2401 | Info | Software Update: Firewall Module Installation Successful | |
| 2402 | Warning | Software Update: Firewall Module Installation Failed | |
| 2403 | Info | Software Update: Firewall Module Download Successful | |
| 2404 | Warning | Firewall Engine Working With Limited Functionality | |
| 2405 | Info | Firewall Engine Back Online on all Interfaces | |
| 2406 | Warning | Firewall Engine Disabled | |
| 2407 | Info | Firewall Engine Enabled | |
| 2500 | Info | Software Update: Intrusion Prevention Module Installation Started | |
| 2501 | Info | Software Update: Intrusion Prevention Module Installation Successful | |
| 2502 | Warning | Software Update: Intrusion Prevention Module Installation Failed | |
| 2503 | Info | Software Update: Intrusion Prevention Module Download Successful | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 2504 | Warning | Intrusion Prevention Engine Working With Limited Functionality | |
| 2505 | Info | Intrusion Prevention Engine Back Online on all Interfaces | |
| 2506 | Warning | Intrusion Prevention Engine Disabled | |
| 2507 | Info | Intrusion Prevention Engine Enabled | |
| 2600 | Info | Software Update: Integrity Monitoring Module Installation Started | |
| 2601 | Info | Software Update: Integrity Monitoring Module Installation Successful | |
| 2602 | Warning | Software Update: Integrity Monitoring Module Installation Failed | |
| 2603 | Info | Software Update: Integrity Monitoring Module Download Successful | |
| 2604 | Info | A computer reboot is required to complete Integrity Monitoring protection | |
| 2605 | Info | Manager has requested that agent sends Integrity Monitoring baseline in events | |
| 2606 | Info | Agent will send Integrity Monitoring baseline in events | |
| 2700 | Info | Software Update: Log Inspection Module Installation | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | Started | |
| 2701 | Info | Software Update: Log Inspection Module Installation Successful | |
| 2702 | Warning | Software Update: Log Inspection Module Installation Failed | |
| 2703 | Info | Software Update: Log Inspection Module Download Successful | |
| 2800 | Info | Software Update: Software Automatically Downloaded | |
| 2801 | Error | Software Update: Unable to retrieve Download Center inventory | |
| 2802 | Error | Software Update: Unable to download software from Download Center | |
| 2803 | Info | Online Help Update Started | |
| 2804 | Info | Online Help Update Ended | |
| 2805 | Info | Online Help Update Success | |
| 2806 | Warning | Online Help Update Failed | |
| 2900 | Info | Software Update: Relay Module Installation Started | |
| 2901 | Info | Software Update: Relay Module Installation Successful | |
| 2902 | Warning | Software Update: Relay Module Installation Failed | |
| 2903 | Info | Software Update: Relay Module | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | Download Successful | |
| 2904 | Info | VMware NSX Synchronization Finished | |
| 2905 | Error | VMware NSX Synchronization Failed | |
| 2906 | Info | Agent Self-Protection enabled | Agent self-protection was enabled via the Deep Security Manager. |
| 2907 | Info | Agent Self-Protection disabled | |
| 2908 | Info | Agent Self-Protection enabled | Agent self-protection was enabled via the command line on the Deep Security Agent. |
| 2909 | Info | Agent Self-Protection disabled | |
| 2915 | Info | Data migration complete | |
| 2916 | Warning | Data migration finished with error | |
| 2920 | Info | Querying report from DDAn Finished | |
| 2921 | Error | Querying report from DDAn Failed | |
| 2922 | Info | Submission to Deep Discovery Analyzer processed | |
| 2923 | Error | File submission to Deep Discovery Analyzer Failed | |
| 2924 | Info | Security Update: Suspicious Object Check and Update Successful | |
| 2925 | Error | Security Update: Suspicious Object Check and Update Failed | |
| 2926 | Warning | Submission to Deep Discovery Analyzer queued | |
| 2930 | Info | File back up pending | |
| 2931 | Info | Smart Folder | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | Added | |
| 2932 | Info | Smart Folder Removed | |
| 2933 | Info | Smart Folder Updated | |
| 2934 | Error | Failed to send Amazon SNS message | |
| 2935 | Info | System resumed sending SNS messages | |
| 2937 | Info | SAML Identity Provider Created | |
| 2938 | Info | SAML Identity Provider Updated | |
| 2939 | Info | SAML Identity Provider Deleted | |
| 2940 | Info | SAML Service Provider Updated | |
| 2941 | Error | Failed to Update News | The event is not available in Deep Security Manager version 20.0.313 (20 LTS Update 2021-01-18) and later |
| 2942 | Info | Performance Profile Created | |
| 2943 | Info | Performance Profile Updated | |
| 2944 | Info | Performance Profile Deleted | |
| 2945 | Info | System Upgrade Started | |
| 2946 | Info | System Update Succeeded | |
| 2947 | Error | System Upgrade Failed | |
| 2948 | Info | Manager Node Upgrade Started | |
| 2949 | Info | Manager Node Update Succeeded | |
| 2950 | Error | Manager Node Upgrade Failed | A node in a multi-node environment failed to upgrade. |
| 2951 | Error | Failed to send TIC message | Managed Detection and Response events failed to send. |
| 2952 | Info | System resumed sending TIC messages | |
| 2953 | Info | Inactive Agent | Inactive agent cleanup removed computers that have |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | Cleanup Completed Successfully | been offline and inactive for a specified period of time. For more information on inactive agent cleanup, see "Automate offline computer removal with inactive agent cleanup" on page 1395. |
| 2954 | Warning | Dropped events recorded in the future | |
| 2955 | Info | The public CA chain was imported (via the dsm_c command) | |
| 2656 | Info | The public CA chain was deleted (via the dsm_c command) | |
| 2957 | Info | The manager's certificate authority cert was renewed (happens automatically, by default every 10 yrs) | |
| 2958 | Info | The default TLS certificate was renewed (happens automatically, by default every 2 yrs) | |
| 2969 | Info | Scheduled Task Skipped | |
| 2970 | Info | GCP Account Added | GCP Account: <GCPaccountname> successfully added.<br>For details, see "Add a Google Cloud Platform account" on page 614. |
| 2971 | Info | GCP Account Removed | GCP Account: <GCPaccountname> successfully removed.<br>For details, see "Remove a GCP account" on page 617. |
| 2972 | Info | GCP Account Updated | GCP Account: <GCPaccountname> successfully updated.<br>For details, see "Add a Google Cloud Platform account" on page 614. |
| 2973 | Info | GCP Account Synchronization Finished | Synchronize computers completed for GCP Account: <GCPaccountname> |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | | For details, see "Synchronize a GCP account" on page 618. |
| 2974 | Error | GCP Account Synchronization Failed | Deep Security Manager was unable to synchronize computers with GCP Account: <GCPaccountname><br>*<detailed_message>*<br>For example:<br>Root URL is not valid<br>For details, see "Synchronize a GCP account" on page 618. |
| 2975 | Info | GCP Account Synchronization Requested | A request has been made to synchronize computers with GCP Account: <GCPaccountname><br>For details, see "Synchronize a GCP account" on page 618. |
| 2976 | Warning | GCP Account Synchronization Completed but with Errors | The GCP Account <GCPaccountname> synchronization operation completed, but information for the following hosts or groups could not be updated with following message:<br>*<detailed_message>*<br>For example:<br>Project <GCPprojectname>: 403 Required 'compute.machineTypes.list' permission for 'projects/<GCPprojectname>'<br>For details, see "Synchronize a GCP account" on page 618. |
| 2990 | Info | XDR Service Registered | |
| 2991 | Info | XDR Service Deleted | |
| 2993 | Warning | XDR Certificate Expired | |
| 2994 | Warning | XDR Product Connector Missing | |
| 2995 | Info | XDR Certificate Updated | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 2996 | Warning | XDR Certificate Update Failed | |
| 2997 | Warning | Get Host GUID Failed | |
| 2998 | Warning | Invalid Host GUID | |
| 3050 | Info | Software Update: ICAP Scanner Installation Started | |
| 3051 | Info | Software Update: ICAP Scanner Installation Successful | |
| 3052 | Warning | Software Update: ICAP Scanner Installation Failed | |
| 3053 | Info | Software Update: ICAP Scanner Download Successful | |
| 3100 | Info | Software Update: Container Control Module Installation Started | |
| 3101 | Info | Software Update: Container Control Module Installation Successful | |
| 3102 | Warning | Software Update: Container Control Module Installation Failed | |
| 3103 | Info | Software Update: Container Control Module Download Successful | |
| 3104 | Info | Container Control: Authorization Plugin Installation Successful | |
| 3105 | Error | Container Control: Authorization Plugin Installation Failed | |
| 3106 | Info | Container Control: Authorization Plugin Connected to Docker | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 3107 | Error | Container Control: Authorization Plugin Connection to Docker Failed | |
| 3108 | Info | Container Control: Authorization Plugin Configuration Sent Successfully | |
| 3109 | Error | Container Control: Authorization Plugin Failed to Send Configuration | |
| 3110 | Error | Container Control: Authorization Plugin Parse Request Failed | |
| 3111 | Info | User Viewed Container Control Event | |
| 3112 | Info | Container Control Security Events Exported | |
| 3113 | Info | Registry Scanner Created | |
| 3114 | Info | Registry Scanner Deleted | |
| 3115 | Info | Registry Scanner Updated | |
| 3116 | Error | Registry Scanner Disconnected | |
| 3300 | Info | Computer Added to vCenter Account | |
| 3400 | Info | Device Control USB device created. | |
| 3401 | Info | Device Control USB device updated. | |
| 3402 | Info | Device Control USB device deleted. | |
| 3403 | Error | Device Control engine offline | The Device Control Engine is offline, so device policies may not be working and may not being applied. This is normally due to an error during engine initializing or the |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | | platform being offline (the platform is sometimes called the Anti-Malware Solution Platform, or AMSP, and sometimes called the Trend Micro Solution Platform). Check the status of the platform at the computer. |
| 3404 | Info | Device Control engine back online. | |
| 3405 | Info | Device Control event exported. | |
| 3406 | Info | User viewed Device Control event. | |
| 3500 | Info | Service Gateway Added | |
| 3501 | Info | Service Gateway Removed | |
| 3502 | Info | Service Gateway Updated | |
| 3600 | Info | Threat Intelligence Status Publish Job Started | |
| 3601 | Info | Threat Intelligence Status Publish Job Completed | |
| 3602 | Error | Threat Intelligence Status Publish Job Failed | |
| 7000 | Info | Application Control Security Events Exported | An administrator downloaded application control event logs in CSV format. |
| 7007 | Info | User Viewed Application Control Event | An administrator dismissed an application control alert. This is normal unless your system has been compromised by an intruder that has gained an administrator login. |
| 7008 | Error | Application Control Engine Offline | An agent's application control engine failed to come online. This could happen if you have enabled application control on a computer whose kernel is not supported. |
| 7009 | Info | Application Control Engine Online Again | An agent's application control engine restarted. |
| 7010 | Info | Application Control Configuration Updated | Deep Security Manager updated the application control settings on an agent. |
| 7011 | Info | Software Update: Application Control | The agent received a policy from Deep Security Manager where application control was selected, but detected that |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | Module Installation Started | it did not have the application control engine installed or needed to update it, so it began to download it. This is normal when you enable application control on a computer for the first time, or when it has been disabled while application control engine updates were released. |
| 7012 | Info | Software Update: Application Control Module Installation Successful | The agent installed the application control engine. The application control engine is also used by the integrity monitoring feature. |
| 7013 | Error | Software Update: Application Control Module Installation Failed | The agent could not install the application control engine. This is not normal. |
| 7014 | Info | Software Update: Application Control Module Download Successful | The agent finished downloading the application control engine. |
| 7015 | Info | Application Control Ruleset Rules Updated | The legacy REST API was used to allow or block software. This message does not occur when administrators perform the same action in the GUI. |
| 7020 | Info | Application Control Inventory Retrieved | The legacy REST API uploaded a computer's initial allow rules to Deep Security Manager. |
| 7021 | Info | Application Control Inventory Scan Started | The application control engine was enabled, and the agent detected that it did not have any allow rules for that computer, so it began to build initial rules based on the currently installed software. This is normal when you enable application control for the first time. This message does not occur when you use the legacy REST API to replace the allow rules. |
| 7022 | Info | Application Control Inventory Scan Completed | The agent finished building the initial allow rules for that computer. After this, any new software that is detected which is not in the allow or block rules will, if configured, cause and alert. |
| 7023 | Error | Application Control Inventory Scan Failed | The agent could not build the initial allow rules for that computer. This is not normal. |
| 7024 | Info | Application Control Software Changes Detected | An administrator allowed or blocked software in the **Actions** tab, or changed a rule by clicking **Change rule** in an application control log message. This message does not occur when you use the legacy REST API to replace the allow rules. |
| 7025 | Info | Application Control Inventory Scan Requested | You manually forced application control to delete the current rules and rebuild them based on the currently installed software. This could be normal if you needed to change many rules at the same time. |
| 7026 | Info | Application Control | Either an administrator sent or the legacy REST |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | Maintenance Mode Start Requested | API received the command to enable maintenance mode. |
| 7027 | Info | Application Control Maintenance Mode Stop Requested | Either an administrator sent or the legacy REST API received the command to disable maintenance mode. |
| 7028 | Info | Application Control Maintenance Mode Started | Maintenance mode was enabled. While enabled, the agent automatically adds updated or newly installed software to its allow rules, indicating that you know and want to allow the software update. The agent continues to apply block rules during this time. |
| 7029 | Info | Application Control Maintenance Mode Stopped | Maintenance mode was disabled. Once maintenance mode is stopped, all new or changed software will be considered "unrecognized" until you specifically allow or block it. |
| 7030 | Info | Application Control Inventory Scan Cancelled | The agent began to build the initial allow rules, but an administrator canceled the process. |
| 7031 | Error | Sending Application Control Ruleset Failed | An agent could not download a shared ruleset for application control. This can occur if network connectivity is interrupted (such as a firewall or proxy between the agent and relay), or if there isn't enough free disk space on the agent. |
| 7032 | Info | Sending Application Control Ruleset Succeeded | An agent downloaded a shared ruleset for application control. This normally occurs whenever an administrator or the legacy REST API allows or blocks software, or when a different shared ruleset is applied. |
| 7033 | Info | Application Control Ruleset Created | The legacy REST API was used to create an application control ruleset. This message does not occur when administrators perform the same action in the GUI. |
| 7034 | Info | Application Control Ruleset Updated | The legacy REST API was used to allow or block software via an application control ruleset. This message does not occur when administrators perform the same action in the GUI. |
| 7035 | Info | Application Control Ruleset Deleted | The legacy REST API was used to delete an application control ruleset. This message does not occur when administrators perform the same action in the GUI. |
| 7036 | Info | Application Control Maintenance Mode Reset Duration Requested | An administrator changed the time period for when maintenance mode is active. |
| 7037 | Error | Newly applied ruleset will block some running processes on restart | An administrator applied a new ruleset, but some of the currently running processes exist in block rules. Application control will not terminate the processes, but the next time you reboot or restart those services, depending on your configuration, it will either alert you or block them. If the processes are not authorized, you should terminate them manually. If they are authorized, |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| | | | but are missing from the ruleset, you should add them to the ruleset. |
| 7038 | Error | Unresolved software change limit reached | Software changes detected on the file system exceeded the maximum amount. Application control will continue to enforce existing rules, but will not record any more changes, and it will stop displaying any of that computer's software changes. You must resolve and prevent excessive software change. |
| 7040 | Error | Incompatible Application Control Ruleset | An application control ruleset could not be assigned to one or more computers because the ruleset is not supported by the installed version of the agent. Typically, the problem is that a hash-based ruleset (which is compatible only with Deep Security Agent 11.0 or newer) has been assigned to an older Deep Security Agent. Deep Security Agent 10.x supports only file-based rulesets. (For details, see "Differences in how Deep Security Agent 10 and 11 compare files" on page 996.) To fix this issue, upgrade the Deep Security Agent to version 11.0 or newer. Alternatively, if you are using local rulesets, reset application control for the agent. Or if you are using a shared ruleset, use a shared ruleset that was created with Deep Security 10.x until all agents using the shared ruleset are upgraded to Deep Security Agent 11.0 or newer. |
| 7041 | Info | Application Control Ruleset Upgraded | An application control ruleset was upgraded from a file-based ruleset to a hash-based ruleset. For details, see "Differences in how Deep Security Agent 10 and 11 compare files" on page 996. |
| 7042 | Info | Application Control Software Inventory Deleted | |
| 7043 | Info | A computer reboot is required to complete Application Control protection | |
| 7044 | Info | Sending Application Control Ruleset | The Manager is sending Application Control rulesets to the remote agent. |
| 7045 | Error | Failed to send Application Control Ruleset | The Manager failed to send the Application Control rulesets to the remote agent. |
| 7046 | Info | Application Control Trust Rule Created | |
| 7047 | Info | Application Control Trust Rule Updated | |

| ID | Severity | Event | Description or Solution |
|---|---|---|---|
| 7048 | Info | Application Control Trust Rule Deleted | |
| 7049 | Info | Application Control Trust Ruleset Created | |
| 7050 | Info | Application Control Trust Ruleset Updated | |
| 7051 | Info | Application Control Trust Ruleset Deleted | |
| 10001 | Info | AWS Billing Usage Data Submission Success | |
| 10002 | Error | AWS Billing Usage Data Submission Failure | |
| 10003 | Info | AWS Marketplace Billing Usage Data CSV Exported | |
| 10004 | Error | Agent Activation Prevented Due to AWS Marketplace Billing Usage Data Submission Failure | |

## Application Control events

For general best practices related to events, see "About Deep Security event logging" on page 1046.

To see the Application Control events captured by Deep Security, go to **Events & Reports** > **Events** > **Application Control Events** > **Security Events**.

### What information is displayed for Application Control events?

These columns can be displayed on the Application Control Events page. You can click **Columns** to select which columns are displayed in the table.

- **Time**: Time the event took place on the computer.
- **Computer**: The computer on which this event was logged. (If the computer has been removed, this entry will read "Unknown Computer".)

- **Event**: The name of the event.
- **Rules**: View event details and change the rule from Allow to Block or vice versa.
- **Ruleset**: Ruleset that's associated with the event.
- **Action**: The action that caused the event to be triggered.
- **Reason**: The reason the event was triggered.
- **Repeat count**: The number of events that are aggregated.
- **Tag(s):** Event tags associated with this event.
- **Path**: Path to the affected file.
- **File**: File affected by the event.
- **User Name**: User that's responsible for executing the unrecognized software.
- **Event Origin:** The Deep Security component from which the event originated.
- **MD5:** MD5 hash.
- **SHA1:** SHA-1 hash.
- **SHA256:** SHA-256 hash.
- **Group**: The name of the group.
- **Group ID**: The ID of the group.
- **User ID**: User ID of the file owner.
- **Process ID**: ID of process that ran the execution.
- **Process Name**: Process that ran the execution.

### List of all Application Control events

**Note:** For system events related to Application Control, see "System events" on page 1233.

| Events |
|---|
| Execution of Unrecognized Software Allowed |
| Execution of Unrecognized Software Blocked |
| Execution of Software Blocked by Rule |

## Anti-malware events

For general best practices related to events, see "About Deep Security event logging" on page 1046.

To see the anti-malware events captured by Deep Security, go to **Events & Reports** > **Events** > **Anti-Malware Events**.

## Information displayed for anti-malware events

The following columns can be displayed on the **Anti-Malware Events** page. To select which columns to display, click **Columns**.

- **Time**: The time when the event took place on the computer.
- **Computer**: The computer on which this event was logged. If the computer has been removed, this entry reads Unknown Computer.
- **Infected Files**: The location and name of the infected file.
- **Tags**: Event tags associated with this event.
- **Malware**: The name of the malware that was found.
- **Action Taken**: The results of the actions specified in the malware scan configuration associated with the event.
  - **Cleaned**: The message notifying that Deep Security successfully terminated processes or deleted registries, files, cookies, or shortcuts, depending on the type of malware.
  - **Clean Failed**: The message notifying that malware could not be cleaned for a variety of possible reasons. If the clean action (which is only available for a limited subset of viruses) fails, the secondary action is quarantine.
  - **Deleted:** The message notifying that an infected file was deleted.
  - **Delete Failed**: The message notifying that an infected file could not be deleted for a variety of possible reasons. For example, the file is locked by another application, is on a CD, or is in use. If possible, Deep Security will delete the infected file once it is released. Even if the delete action fails, any attempt by the system or the user to interact with the file or execute it will be denied during the real-time scan.
  - **Quarantined**: The message notifying that an infected file was moved to the identified files folder.
  - **Quarantine Failed**: The message notifying that an infected file could not be quarantined for a variety of possible reasons. For example, the file is locked by another application, is on a CD, or is in use. If possible, Deep Security will quarantine the infected file once it is released. It is also possible that the maximum disk space used to store identified files (specified on the **Policy or Computer Editor > Anti-Malware > Advanced** tab) has been exceeded. Even if the quarantine action fails, any attempt by

the system or the user to interact with the file or execute it will be denied during the real-time scan.

  - **Access Denied**: The message notifying that Deep Security has prevented the infected file from being accessed without removing the file from the system.
  - **Passed**: The message notifying that Deep Security did not take any action but logged the detection of the malware.

- **Scan Type**: The type of scan that found the malware (real-time, scheduled, or manual).
- **Event Origin:** Indicates from which part of the Deep Security system the event originated.
- **Reason**: The malware scan configuration that was in effect when the malware was detected.
- **Major Virus Type**: The type of malware detected. The possible values are Joke, Trojan, Virus, Test, Spyware, Packer, Generic, and so on. For information on these types of malware, see the anti-malware event details or see "About Anti-Malware" on page 735
- **Targets**: The file, process, or registry key (if any) that the malware was trying to affect. If the malware was trying to affect more than one, this field would contain the value Multiple.
- **Target Type**: The type of system resource that this malware was trying to affect, such as the file system, a process, or Windows registry.
- **Container ID**: ID of the Docker container where the malware was found.
- **Container Image Name**: The image name of the Docker container where the malware was found.
- **Container Name**: The name of the Docker container where the malware was found.
- **File MD5**: The MD5 hash of the file.

## List of anti-malware events

The following table provides a list of all available anti-malware events:

| ID | Severity | Event |
|---|---|---|
| 9001 | Info | Anti-Malware Scan Started |
| 9002 | Info | Anti-Malware Scan Completed |
| 9003 | Info | Anti-Malware Scan Terminated Abnormally |
| 9004 | Info | Anti-Malware Scan Paused |
| 9005 | Info | Anti-Malware Scan Resumed |
| 9006 | Info | Anti-Malware Scan Cancelled |
| 9007 | Warning | Anti-Malware Scan Cancel Failed |
| 9008 | Warning | Anti-Malware Scan Start Failed |
| 9009 | Warning | Anti-Malware Scan Stalled |

| ID | Severity | Event |
|---|---|---|
| 9010 | Error | File cannot be analyzed or quarantined (VM maximum disk space used to store identified files exceeded) |
| 9011 | Error | Maximum disk space used for storing identified files exceeded. Older identified files might be purged or newly-detected files might not be analyzed or quarantined. |
| 9012 | Warning | Smart Protection Server Disconnected for Smart Scan |
| 9013 | Info | Smart Protection Server Connected for Smart Scan |
| 9014 | Warning | Computer reboot is required for Anti-Malware protection |
| 9016 | Info | Anti-Malware Component Update Successful |
| 9017 | Error | Anti-Malware Component Update Failed |
| 9018 | Error | Files could not be scanned for malware |
| 9019 | Error | Directory could not be scanned for malware |

## Device Control events

For general best practices related to events, see [Events in Workload Security](../events).

To see the Device Control events captured by Workload Security, go to **Events & Reports > Events > Device Control Events > Security Events**.

### What information is displayed for Device Control events?

These columns can be displayed on the Device Control Events page. You can click **Columns** to select which columns are displayed in the table.

- **Time**: The time that the event took place on the computer.
- **Computer**: The computer on which this event was logged. (If the computer has been removed, this entry will read "Unknown Computer".)
- **Device Type**: The device type that was accessed to cause the event; for example, USB.
- **Target**: The file name that was accessed that caused the event to be triggered.
- **Accessed By**: The process name that caused the event to be triggered.
- **Action Taken**: The action that Device Control took.
- **Vendor**: The name of the vendor of the device.
- **Model**: The model name or number of the device.
- **Serial Number**: The serial number of the device.
- **Product**: The device name that was accessed to cause the event.

- **Tag(s)**: Any event tags associated with this event.
- **Event Origin**: The Workload Security component from which the event originated.

## Firewall events

For general best practices related to events, see "About Deep Security event logging" on page 1046.

To see the firewall events captured by Deep Security, go to **Events & Reports** > **Events** > **Firewall Events**.

Firewall event icons:

📄 Single event

🗎 Single event with data

🗐 Folded event

🗐 Folded event with data

> **Note:** Event folding occurs when multiple events of the same type occur in succession. This saves disk space and protects against DoS attacks that may attempt to overload the logging mechanism.

### What information is displayed for firewall events?

These columns can be displayed on the firewall events page. You can click **Columns** to select which columns are displayed in the table.

- **Time:** Time the event took place on the computer.
- **Computer:** The computer on which this event was logged. (If the computer has been removed, this entry will read "Unknown Computer".)
- **Reason:** Log entries on this page are generated either by firewall rules or by firewall stateful configuration settings. If an entry is generated by a firewall rule, the column entry will be prefaced by "Firewall Rule:" followed by the name of the firewall rule. Otherwise the column entry will display the firewall stateful configuration setting that generated the log entry.
- **Tag(s):** Event tags that are applied to this event.

- **Action:** The action taken by the firewall rule or firewall stateful configuration. Possible actions are: Allow, Deny, Force Allow, and Log Only.
- **Rank:** The ranking system provides a way to quantify the importance of intrusion prevention and firewall events. By assigning "asset values" to computers, and assigning "severity values" to intrusion prevention rules and firewall rules, the importance ("rank") of an event is calculated by multiplying the two values together. This allows you to sort events by rank when viewing intrusion prevention or firewall events.
- **Direction:** The direction of the affected packet (incoming or outgoing).
- **Interface:** The MAC address of the interface through which the packet was traveling.
- **Frame Type:** The frame type of the packet in question. Possible values are "IPV4", "IPV6", "ARP", "REVARP", and "Other: XXXX" where XXXX represents the four digit hex code of the frame type.
- **Protocol:** Possible values are "ICMP", "ICMPV6", "IGMP", "GGP", "TCP", "PUP", "UDP", "IDP", "ND", "RAW", "TCP+UDP", AND "Other: nnn" where nnn represents a three digit decimal value.
- **Flags:** Flags set in the packet.
- **Source IP:** The packet's source IP.
- **Source MAC:** The packet's source MAC address.
- **Source Port:** The packet's source port.
- **Destination IP:** The packet's destination IP address.
- **Destination MAC:** The packet's destination MAC address.
- **Destination Port:** The packet's destination port.
- **Packet Size:** The size of the packet in bytes.
- **Repeat Count:** The number of times the event was sequentially repeated.
- **Time (microseconds):** Microsecond resolution for the time the event took place on the computer.
- **Event Origin:** The Deep Security component from which the event originated.

The following columns are also available. They display information for events that are triggered from containers on computers that are protected by Deep Security Agent 12 FR or newer:

- **Interface Type:** Container interface type.
- **Container Name:** Name of the container where the event occurred.
- **Container ID:** Container ID of the container where the event occurred.

- **Image Name:** Image name that was used to create the container where the event occurred.
- **RepoDigest:** A unique digest that identifies the container image.
- **Process Name:** Name of the process (from the container) that caused the event.

> **Note:** **Log-only** rules will only generate a log entry if the packet in question is not subsequently stopped either by a **deny** rule, or an **allow** rule that excludes it. If the packet is stopped by one of those two rules, *those* rules will generate a log entry and *not* the **log-only** rule. If no subsequent rules stop the packet, the log-only rule will generate an entry.

## List of all firewall events

| ID | Event | Notes |
|---|---|---|
| 100 | Out Of Connection | A packet was received that was not associated with an existing connection. |
| 101 | Invalid Flags | Flag(s) set in a packet were invalid. This event can indicate that a flag does not make sense within the context of a current connection (if any), or that a nonsensical combination of flags.<br>"Firewall Stateful Configuration" must be On for connection context to be assessed. |
| 102 | Invalid Sequence | A packet with an invalid sequence number or out-of-window data size was encountered. |
| 103 | Invalid ACK | A packet with an invalid acknowledgment number was encountered. |
| 104 | Internal Error | |
| 105 | CE Flags | A packet has congestion flags set and the policy's Anti Evasion settings use a custom configuration where the TCP Congestion Flags property is set to Log or Deny. (See "Configure anti-evasion settings" on page 844.) |
| 106 | Invalid IP | Packet's source IP was not valid. |
| 107 | Invalid IP Datagram Length | The length of the IP datagram is less than the length specified in the IP header. |
| 108 | Fragmented | A fragmented packet was encountered and fragmented packets are not allowed. |
| 109 | Invalid Fragment Offset | |
| 110 | First Fragment Too Small | A fragmented packet was encountered, and the size of the first fragment is less than the size of a TCP packet (no data).<br>A packet is dropped with this event when the packet header has the following configuration: |

| ID | Event | Notes |
|---|---|---|
| | | - Fragment Offset = 0 (The fragment is the first in the packet)<br>- Total length (maximum combined header length) < 120 bytes (the default allowed minimum fragment size)<br><br>To prevent this event from occurring, configure the policy's Advanced Network Engine settings to use a lower value for the Minimum Fragment Size property, or set it to 0 to turn off this inspection. (See "Advanced Network Engine Options" in "Network engine settings" on page 658.) |
| 111 | Fragment Out Of Bounds | The offsets(s) specified in a fragmented packet sequence is outside the range of the maximum size of a datagram. |
| 112 | Fragment Offset Too Small | A fragmented packet was encountered, the size of the fragment was less than the size of a TCP packet (no data). |
| 113 | IPv6 Packet | An IPv6 Packet was encountered, and IPv6 blocking is enabled. See the "Block IPv6 on Agents and Appliances verions 9 and later" property in the Advanced Network Engine Options (see "Network engine settings" on page 658.) |
| 114 | Max Incoming Connections | The number of incoming connections has exceeded the maximum number of connections allowed. See the "Enable TCP stateful inspection" property in "TCP packet inspection" on page 891. |
| 115 | Max Outgoing Connections | The number of outgoing connections has exceeded the maximum number of connections allowed. See the "Enable TCP stateful inspection" property in "TCP packet inspection" on page 891. |
| 116 | Max SYN Sent | The number of half open connections from a single computer exceeds that specified in the firewall stateful configuration. See the "Limit the number of half-open connections from a single computer to" property in "TCP packet inspection" on page 891. |
| 118 | IP Version Unknown | An IP packet other than IPv4 or IPv6 was encountered. |
| 119 | Invalid Packet Info | |
| 120 | Internal Engine Error | Insufficient system memory. Add more system resources to fix this issue. |
| 121 | Unsolicited UDP | Incoming UDP packets that were not solicited by the computer are rejected. |
| 122 | Unsolicited ICMP | ICMP stateful has been enabled (in firewall stateful configuration) and an unsolicited packet that does not match any Force Allow rules was received. |
| 123 | Out Of Allowed Policy | The packet does not meet any of the Allow or Force Allow rules and so is implicitly denied. |
| 124 | Invalid Port Command | An invalid FTP port command was encountered in the FTP control channel data stream. |
| 125 | SYN Cookie Error | The SYN cookies protection mechanism encountered an error. |

| ID | Event | Notes |
|---|---|---|
| 126 | Invalid Data Offset | Invalid data offset parameter. |
| 127 | No IP Header | The packet IP header is invalid or incomplete. |
| 128 | Unreadable Ethernet Header | Data contained in this Ethernet frame is smaller than the Ethernet header. |
| 129 | Undefined | |
| 130 | Same Source and Destination IP | Source and destination IPs were identical. |
| 131 | Invalid TCP Header Length | |
| 132 | Unreadable Protocol Header | The packet contains an unreadable TCP, UDP or ICMP header. |
| 133 | Unreadable IPv4 Header | The packet contains an unreadable IPv4 header. |
| 134 | Unknown IP Version | Unrecognized IP version. |
| 135 | Invalid Adapter Configuration | An invalid adapter configuration has been received. |
| 136 | Overlapping Fragment | This packet fragment overlaps a previously sent fragment. |
| 138 | Packet on Closed Connection | A packet was received belonging to a connection already closed. |
| 139 | Dropped Retransmit | The network engine detected a TCP Packet that overlaps with data already received on the same TCP connection but does not match the already-received data. (The network engine compares the packet data that was queued in the engine’s connection buffer to the data in the packet that was re-transmitted.)<br>The network engine reconstructs the sequenced data stream of each TCP connection it processes. The sequence number and length in the received packet specify a specific region in this data stream. The note field in the log indicates the location of the changed content in the TCP stream: prev-full, prev-part, next-full and next-part:<br>• "prev-full" and "prev-part": The changed area is in the packet that immediately precedes the retransmitted packet in the sequenced data stream. "prev-full" indicates that the changed area is completely contained in the packet which immediately precedes the |

| ID | Event | Notes |
|---|---|---|
| | | retransmitted packet in the sequenced data stream. Otherwise, the note is "prev-part".<br>- "next-full" and "next-part": The changed area is in the packet that immediately follows the retransmitted packet in the sequenced data stream. "next-full" indicates that the changed area is completely contained in the packet that immediately follows the retransmitted packet in the sequenced data stream. Otherwise, the note is "next-part". |
| 140 | Undefined | |
| 141 | Out of Allowed Policy (Open Port) | |
| 142 | New Connection Initiated | |
| 143 | Invalid Checksum | |
| 144 | Invalid Hook Used | |
| 145 | IP Zero Payload | |
| 146 | IPv6 Source Is Multicast | |
| 147 | Invalid IPv6 Address | |
| 148 | IPv6 Fragment Too Small | |
| 149 | Invalid Transport Header Length | |
| 150 | Out of Memory | |
| 151 | Max TCP Connections | The maximum number of TCP connections has been exceeded. See "Event: Max TCP connections" on page 1327. |
| 152 | Max UDP Connections | |
| 200 | Region Too Big | A region (edit region, uri etc) exceeded the maximum allowed buffering size (7570 bytes) without being closed. This is usually because the data does not conform to the protocol. |
| 201 | Insufficient Memory | The packet could not be processed properly because resources were exhausted. This can be because too many concurrent connections require buffering (max 2048) or matching resources (max 128) at the same time or because of excessive matches in a single IP packet (max 2048) or simply because the system is out of memory. |

| ID | Event | Notes |
|---|---|---|
| 202 | Maximum Edits Exceeded | The maximum number of edits (32) in a single region of a packet was exceeded. |
| 203 | Edit Too Large | Editing attempted to increase the size of the region above the maximum allowed size (8188 bytes). |
| 204 | Max Matches in Packet Exceeded | There are more than 2048 positions in the packet with pattern match occurrences. An error is returned at this limit and the connection is dropped because this usually indicates a garbage or evasive packet. |
| 205 | Engine Call Stack Too Deep | |
| 206 | Runtime Error | Runtime error. |
| 207 | Packet Read Error | Low level problem reading packet data. |
| 257 | Fail Open: Deny | Log the packet that should be dropped but not when Fail-Open feature is on and in Inline mode. |
| 300 | Unsupported Cipher | An unknown or unsupported cipher suite has been requested. |
| 301 | Error Generating Master Key(s) | Unable to derive the cryptographic keys, Mac secrets, and initialization vectors from the master secret. |
| 302 | Record Layer Message (not ready) | The SSL state engine has encountered an SSL record before initialization of the session. |
| 303 | Handshake Message (not ready) | The SSL state engine has encountered a handshake message after the handshake has been negotiated. |
| 304 | Out Of Order Handshake Message | A well formatted handshake message has been encountered out of sequence. |
| 305 | Memory Allocation Error | The packet could not be processed properly because resources were exhausted. This can be because too many concurrent connections require buffering (max 2048) or matching resources (max 128) at the same time or because of excessive matches in a single IP packet (max 2048) or simply because the system is out of memory. |
| 306 | Unsupported SSL Version | A client attempted to negotiate an SSL V2 session. |
| 307 | Error Decrypting Pre-master Key | Unable to un-wrap the pre-master secret from the ClientKeyExchange message. |
| 308 | Client Attempted to Rollback | A client attempted to rollback to an earlier version of the SSL protocol than that which was specified in the ClientHello message. |
| 309 | Renewal Error | An SSL session was being requested with a cached session key that could not be located. |
| 310 | Key Exchange Error | The server is attempting to establish an SSL session with temporarily generated key. |

| ID | Event | Notes |
|---|---|---|
| 311 | Maximum SSL Key Exchanges Exceeded | The maximum number of concurrent key exchange requests was exceeded. |
| 312 | Key Too Large | The master secret keys are larger than specified by the protocol identifier. |
| 313 | Invalid Parameters In Handshake | An invalid or unreasonable value was encountered while trying to decode the handshake protocol. |
| 314 | No Sessions Available | |
| 315 | Compression Method Unsupported | |
| 316 | Unsupported Application-Layer Protocol | An unknown or unsupported SSL Application-Layer Protocol has been requested. |
| 385 | Fail Open: Deny | Log the packet that should be dropped but not when Fail-Open feature is on and in Tap mode. |
| 500 | URI Path Depth Exceeded | Too many "/" separators. Max 100 path depth. |
| 501 | Invalid Traversal | Tried to use "../" above root. |
| 502 | Illegal Character in URI | Illegal character used in uri. |
| 503 | Incomplete UTF8 Sequence | URI ended in middle of utf8 sequence. |
| 504 | Invalid UTF8 encoding | Invalid or non-canonical encoding attempt. |
| 505 | Invalid Hex Encoding | %nn where nn are not hex digits. |
| 506 | URI Path Length Too Long | Path length is greater than 512 characters. |
| 507 | Invalid Use of Character | Use of disabled characters |
| 508 | Double Decoding Exploit | Double decoding exploit attempt (%25xx, %25%xxd, etc). |
| 700 | Invalid Base64 Content | Packet content that was expected to be encoded in Base64 format was not encoded correctly. |
| 710 | Corrupted Deflate/GZIP Content | Packet content that was expected to be encoded in Base64 format was not encoded correctly. |
| 711 | Incomplete | Incomplete Deflate/GZIP content |

| ID | Event | Notes |
|---|---|---|
| | Deflate/GZIP Content | |
| 712 | Deflate/GZIP Checksum Error | Deflate/GZIP checksum error. |
| 713 | Unsupported Deflate/GZIP Dictionary | Unsupported Deflate/GZIP dictionary. |
| 714 | Unsupported GZIP Header Format/Method | Unsupported GZIP header format or method. |
| 801 | Protocol Decoding Search Limit Exceeded | A protocol decoding rule defined a limit for a search or pdu object but the object was not found before the limit was reached. |
| 802 | Protocol Decoding Constraint Error | A protocol decoding rule decoded data that did not meet the protocol content constraints. |
| 803 | Protocol Decoding Engine Internal Error | |
| 804 | Protocol Decoding Structure Too Deep | A protocol decoding rule encountered a type definition and packet content that caused the maximum type nesting depth (16) to be exceeded. |
| 805 | Protocol Decoding Stack Error | A rule programming error attempted to cause recursion or use to many nested procedure calls. |
| 806 | Infinite Data Loop Error | |
| 10002 | Log Reason Reset with Zero Sequence | Multiple TCP Reset (RST) packets with zero sequence have been sent. |

## Intrusion prevention events

For general best practices related to events, see "About Deep Security event logging" on page 1046.

To see the intrusion prevention events captured by Deep Security, go to **Events & Reports** > **Events** > **Intrusion Prevention Events**.

## What information is displayed for intrusion prevention events?

These columns can be displayed on the Intrusion Prevention Events page. You can click **Columns** to select which columns are displayed in the table.

- **Time:** Time the event took place on the computer.
- **Computer:** The computer on which this event was logged. (If the computer has been removed, this entry will read "Unknown Computer".)
- **Reason:** The intrusion prevention rule associated with this event.
- **Tag(s):** Any tags attached with the event.
- **Application Type:** The application type associated with the intrusion prevention rule which caused this event.
- **Action:** What action the intrusion prevention rule took (Block or Reset). If the rule is in **Detect Only** mode, the action is prefaced with "Detect Only:").

  > **Note:** Intrusion prevention rules created before Deep Security 7.5 SP1 could also perform Insert, Replace, and Delete actions. These actions are no longer performed. If an older rule is triggered and attempts to perform those actions, the event will indicate that the rule was applied in detect-only mode.

- **Rank:** The ranking system provides a way to quantify the importance of intrusion prevention and firewall events. By assigning "asset values" to computers, and assigning "severity values" to intrusion prevention rules and firewall rules, the importance ("rank") of an event is calculated by multiplying the two values together. This allows you to sort events by rank when viewing intrusion prevention or firewall events.
- **Severity:** The intrusion prevention rule's severity value.
- **Direction:** The direction of the packet (incoming or outgoing)
- **Flow:** whether the packets(s) that triggered this event was travelling with ("Connection Flow") or against ("Reverse Flow") the direction of traffic being monitored by the intrusion prevention rule.
- **Interface:** The MAC address of the interface through which the packet was passing.
- **Frame Type:** The frame type of the packet in question. Possible values are "IPV4", "IPV6", "ARP", "REVARP", and "Other: XXXX" where XXXX represents the four digit hex code of the frame type.

- **Protocol:** Possible values are "ICMP", "ICMPV6", "IGMP", "GGP", "TCP", "PUP", "UDP", "IDP", "ND", "RAW", "TCP+UDP", AND "Other: nnn" where nnn represents a three digit decimal value.
- **Flags:** Flags set in the packet.
- **Source IP:** The packet's source IP.
- **Source MAC:** The packet's source MAC address.
- **Source Port:** The packet's source port.
- **Destination IP:** The packet's destination IP address.
- **Destination MAC:** The packet's destination MAC address.
- **Destination Port:** The packet's destination port.
- **Packet Size:** The size of the packet in bytes.
- **Repeat Count:** The number of times the event was sequentially repeated.
- **Time (microseconds):** Microsecond resolution for the time the event took place on the computer.
- **Event Origin:** The Deep Security component from which the event originated.

The following columns are also available. They display information for events that are triggered from containers on computers that are protected by Deep Security Agent 12 FR or newer:

- **Interface Type:** Container interface type.
- **Container Name:** Name of the container where the event occurred.
- **Container ID:** Container ID of the container where the event occurred.
- **Image Name:** Image name that was used to create the container where the event occurred.
- **RepoDigest:** A unique digest that identifies the container image.
- **Process Name:** Name of the process (from the container) that caused the event.

### View additional Intrusion Prevention event information

When exporting Intrusion Prevention events, the exported data includes the fields listed above, as well as additional fields, which are not visible from the Deep Security Manager console. The single exception is the **Severity field**, which is not available in the CSV file.

- **Note**: Meaningful string for the event, such as CVE code.
- **End Time**: Time the packet was most recently seen.
- **Position In Buffer**: Position in packet.

- **Position In Stream**: Position of packet in TCP/IP stream.
- **Data Flags**: Refer to the table below for details on Data Flags values:

| Code | Flag | Notes |
|---|---|---|
| 0x01 | dataTruncated | Indicates data could not be logged. |
| 0x02 | logOverflow | Logs overflowed after this entry. |
| 0x04 | suppressed | Logs threshold suppression occurred after this entry. |
| 0x08 | haveData | Packet Data is logged. |
| 0x10 | refData | DataId is logged. Packet payload is not logged in this event. The payload is only logged in the event with the 0x08 flag and the same Data Index. |
| 0x20 | haveRawPkt | Data is the complete, raw packet. |

- **Data Index**: A unique ID for packet data (dataId). All records with the same dataId are from the same packet.
- **Data**: Payload of the packet.
- **Original IP (XFF)**: Displays original IP address of the client. To obtain data for this field, enable the rule **1006450 - Enable X-Forwarded-For HTTP Header Logging**.

The following fields are also available. They display information for events that are triggered from containers on computers that are protected by Deep Security Agent 12 FR or newer:

- **Process ID**: Process ID reported by the container.
- **Thread ID**: Thread ID reported by the container.
- **Image ID**: The local ID of the container image.
- **Pod ID**: The Pod ID (if applicable).

## List of all intrusion prevention events

| ID | Event | Notes |
|---|---|---|
| 200 | Region Too Big | A region (edit region, uri etc) exceeded the maximum allowed buffering size (7570 bytes) without being closed. This is usually because the data does not conform to the protocol. |
| 201 | Insufficient Memory | The packet could not be processed properly because resources were exhausted. This can be because there are too many concurrent connections at the same time or simply because the system is out of memory. |
| 202 | Maximum Edits Exceeded | The maximum number of edits (32) in a single region of a packet was exceeded. |
| 203 | Edit Too Large | Editing attempted to increase the size of the region above the maximum allowed size (8188 bytes). |
| 204 | Max Matches in Packet | There are more than 2048 positions in the packet with pattern match occurrences. An error is returned at this limit and the connection is |

| ID | Event | Notes |
|---|---|---|
| | Exceeded | dropped because this usually indicates a garbage or evasive packet. |
| 205 | Engine Call Stack Too Deep | |
| 206 | Runtime Error | Runtime error. |
| 207 | Packet Read Error | Low level problem reading packet data. |
| 258 | Fail Open: Reset | Log the connection that should be reset but not when Fail-Open feature is on and in Inline mode |
| 300 | Unsupported Cipher | An unknown or unsupported Cipher Suite has been requested. |
| 301 | Error Generating Master Key(s) | Unable to derive the cryptographic keys, Mac secrets, and initialization vectors from the master secret. |
| 302 | Record Layer Message (not ready) | The SSL state engine has encountered an SSL record before initialization of the session. |
| 303 | Handshake Message (not ready) | The SSL state engine has encountered a handshake message after the handshake has been negotiated. |
| 304 | Out Of Order Handshake Message | A well formatted handshake message has been encountered out of sequence. |
| 305 | Memory Allocation Error | The packet could not be processed properly because resources were exhausted. This can be because there are too many concurrent connections at the same time or simply because the system is out of memory. |
| 306 | Unsupported SSL Version | A client attempted to negotiate an SSL V2 session. |
| 307 | Error Decrypting Pre-master Key | Unable to un-wrap the pre-master secret from the ClientKeyExchange message. |
| 308 | Client Attempted to Rollback | A client attempted to rollback to an earlier version of the SSL protocol than that which was specified in the ClientHello message. |
| 309 | Renewal Error | An SSL session was being requested with a cached session key that could not be located. |
| 310 | Key Exchange Error | The server is attempting to establish an SSL session with temporarily generated key. |
| 311 | Maximum SSL Key Exchanges Exceeded | The maximum number of concurrent key exchange requests was exceeded. |
| 312 | Key Too Large | The master secret keys are larger than specified by the protocol identifier. |
| 313 | Invalid Parameters In | An invalid or unreasonable value was encountered while trying to decode the handshake protocol. |

| ID | Event | Notes |
|---|---|---|
| | Handshake | |
| 314 | No Sessions Available | |
| 315 | Compression Method Unsupported | |
| 316 | Unsupported Application-Layer Protocol | An unknown or unsupported SSL Application-Layer Protocol has been requested. |
| 386 | Fail Open: Reset | Log the connection that should be reset but not when Fail-Open feature is on and in Tap mode. |
| 500 | URI Path Depth Exceeded | Too many "/" separators. Max 100 path depth. |
| 501 | Invalid Traversal | Tried to use "../" above root. |
| 502 | Illegal Character in URI | Illegal character used in uri. |
| 503 | Incomplete UTF8 Sequence | URI ended in middle of utf8 sequence. |
| 504 | Invalid UTF8 encoding | Invalid or non-canonical encoding attempt. |
| 505 | Invalid Hex Encoding | %nn where nn are not hex digits. |
| 506 | URI Path Length Too Long | Path length is greater than 512 characters. |
| 507 | Invalid Use of Character | Use of disabled characters |
| 508 | Double Decoding Exploit | Double decoding exploit attempt (%25xx, %25%xxd, etc). |
| 700 | Invalid Base64 Content | Packet content that was expected to be encoded in Base64 format was not encoded correctly. |
| 710 | Corrupted Deflate/GZIP Content | Packet content that was expected to be encoded in Base64 format was not encoded correctly. |
| 711 | Incomplete Deflate/GZIP Content | Incomplete Deflate/GZIP content |
| 712 | Deflate/GZIP Checksum Error | Deflate/GZIP checksum error. |
| 713 | Unsupported Deflate/GZIP | Unsupported Deflate/GZIP dictionary. |

| ID | Event | Notes |
|---|---|---|
| | Dictionary | |
| 714 | Unsupported GZIP Header Format/Method | Unsupported GZIP header format or method. |
| 801 | Protocol Decoding Search Limit Exceeded | A protocol decoding rule defined a limit for a search or pdu object but the object was not found before the limit was reached. |
| 802 | Protocol Decoding Constraint Error | A protocol decoding rule decoded data that did not meet the protocol content constraints. |
| 803 | Protocol Decoding Engine Internal Error | |
| 804 | Protocol Decoding Structure Too Deep | A protocol decoding rule encountered a type definition and packet content that caused the maximum type nesting depth (16) to be exceeded. |
| 805 | Protocol Decoding Stack Error | A rule programming error attempted to cause recursion or use to many nested procedure calls. |
| 806 | Infinite Data Loop Error | |

## Integrity monitoring events

For general best practices related to events, see "About Deep Security event logging" on page 1046.

To see the integrity monitoring events captured by Deep Security, go to **Events & Reports** > **Events** > **Integrity Monitoring Events**.

### What information is displayed for integrity monitoring events?

These columns can be displayed on the Integrity Monitoring Events page. You can click **Columns** to select which columns are displayed in the table.

- **Time:** Time the event took place on the computer.
- **Computer:** The computer on which this event was logged. (If the computer has been removed, this entry will read "Unknown Computer".)

- **Reason:** The integrity monitoring rule associated with this event.
- **Tag(s):** Event tags that are applied to this event.
- **Change:** The change detected by the integrity rule. Can be: Created, Updated, Deleted, or Renamed.
- **Rank:** The ranking system provides a way to quantify the importance of events. By assigning "asset values" to computers, and assigning "severity values" to rules, the importance ("rank") of an event is calculated by multiplying the two values together. This allows you to sort events by rank.
- **Severity:** The integrity monitoring rule's severity value
- **Type:** Type of entity from which the event originated
- **Key:** Path and file name or registry key from which the event originated
- **User:** User ID of the file owner
- **Process:** Process from which the event originated
- **Event Origin:** The Deep Security component from which the event originated

## List of all integrity monitoring events

| ID | Severity | Event | Notes |
|---|---|---|---|
| 8000 | Info | Full Baseline Created | Created when the agent has been requested to build a baseline or went from 0 integrity monitoring rules to n (causing the baseline to be built). This event includes information on the time taken to scan (ms), and number of entities cataloged. |
| 8001 | Info | Partial Baseline Created | Created when the agent had a security configuration where one or more integrity monitoring rules changed. This event includes information on the time taken to scan (ms), and number of entities catalogued. |
| 8002 | Info | Scan for Change Completed | Created when the agent is requested to do a full or partial on-demand scan. This event includes information on the time taken to scan (ms), and number of CHANGES catalogued. (Ongoing scans for changes based on the FileSystem Driver or the notify do not generate an 8002 event.) |
| 8003 | Error | Unknown Environment Variable in Integrity Monitoring Rule | Created when a rule uses a ${env.EnvironmentVar} and "EnvironmentVar" is not a known environment variable. This event includes the ID of the integrity monitoring rule containing the problem, the name of the integrity monitoring rule, and the name of the unknown environment variable. |
| 8004 | Error | Bad Base in Integrity Monitoring Rule | Created when a rule contains an invalid base directory or key. For example, specifying a FileSet with a base of "c:\foo\d:\bar" would generate this event, or the invalid value could be the result of environment variable substitution the yields a bad value. This event includes the ID of the integrity monitoring rule |

| ID | Severity | Event | Notes |
|---|---|---|---|
| | | | containing the problem, the name of the integrity monitoring rule, and the bad base value. |
| 8005 | Error | Unknown Entity in Integrity Monitoring Rule | Created when an unknown EntitySet is encountered in an integrity monitoring rule. This event includes the ID of the integrity monitoring rule containing the problem, the name of the integrity monitoring rule, and a comma-separated list of the unknown EntitySet names encountered. |
| 8006 | Error | Unsupported Entity in Integrity Monitoring Rule | Created when a known but unsupported EntitySet is encountered in an integrity monitoring rule. This event includes the ID of the integrity monitoring rule containing the problem, the name of the integrity monitoring rule, and a comma-separated list of the unsupported EntitySet names encountered. Some EntitySet types such as RegistryKeySet are platform-specific. |
| 8007 | Error | Unknown Feature in Integrity Monitoring Rule | Created when an unknown feature is encountered in an integrity monitoring rule. This event includes the ID of the integrity monitoring rule containing the problem, the name of the integrity monitoring rule, the type of entity set (for example, FileSet), and a comma-separated list of the unknown feature names encountered. Examples of valid feature values are "whereBaseInOtherSet", "status", and "executable". |
| 8008 | Error | Unsupported Feature in Integrity Monitoring Rule | Created when a known but unsupported feature is encountered in an integrity monitoring rule. This event includes the ID of the integrity monitoring rule containing the problem, the name of the integrity monitoring rule, the type of entity set (for example, FileSet), and a comma-separated list of the unsupported feature names encountered. Some feature values such as "status" (used for Windows service states) are platform-specific. |
| 8009 | Error | Unknown Attribute in Integrity Monitoring Rule | Created when an unknown attribute is encountered in an integrity monitoring rule. This event includes the ID of the integrity monitoring rule containing the problem, the name of the integrity monitoring rule, the type of entity set (for example, FileSet), and a comma-separated list of the unknown attribute names encountered. Examples of valid attribute values are "created", "lastModified" and "inodeNumber". |
| 8010 | Error | Unsupported Attribute in Integrity Monitoring Rule | Created when a known but unsupported attribute is encountered in an integrity monitoring rule. This event includes the ID of the integrity monitoring rule containing the problem, the name of the integrity monitoring rule, the type of entity set (for example, FileSet), and a comma-separated list of the unsupported attribute names encountered. Some attribute values such as "inodeNumber" are platform-specific. |
| 8011 | Error | Unknown Attribute in Entity Set in Integrity | Created when an unknown EntitySet XML attribute is encountered in an integrity monitoring rule. This event includes the ID of the integrity monitoring rule containing the problem, the name of the integrity monitoring rule, the type of entity set |

| ID | Severity | Event | Notes |
|---|---|---|---|
| | | Monitoring Rule | (for example,FileSet), and a comma-separated list of the unknown EntitySet attribute names encountered. You would get this event if you wrote <FileSet dir="c:\foo"> instead of <FileSet base="c:\foo"> |
| 8012 | Error | Unknown Registry String in Integrity Monitoring Rule | Created when a rule references a registry key that doesn't exist. This event includes the ID of the integrity monitoring rule containing the problem, the name of the integrity monitoring rule, and the name of the unknown registry string. |
| 8013 | Error | Invalid WQLSet was used. Namespace or WQL query was missing. | Indicates that the namespace is missing from a WQL query because an integrity rule XML is incorrectly formatted. This can occur only in an advanced case, with custom integrity rules that use and monitor WQL queries. |
| 8014 | Error | Invalid WQLSet was used. An unknown provider value was used. | |
| 8015 | Warning | Inapplicable Integrity Monitoring Rule | Can be caused by a number of reasons, such as platform mismatch, nonexistent target directories or files, or unsupported functionality. |
| 8016 | Warning | Suboptimal Integrity Rule Detected | |
| 8050 | Error | Regular expression could not be compiled. Invalid wildcard was used. | |

## Log inspection events

For general best practices related to events, see "About Deep Security event logging" on page 1046.

To see the log inspection events captured by Deep Security, go to **Events & Reports > Events > Log Inspection Events**.

## What information is displayed for log inspection events?

These columns can be displayed on the log inspection events page. You can click **Columns** to select which columns are displayed in the table.

- **Time:** Time the event took place on the computer.
- **Computer:** The computer on which this event was logged. (If the computer has been removed, this entry will read "Unknown Computer".)
- **Reason:** The log inspection rule associated with this event.
- **Tag(s):** Any tags attached with the event.
- **Description:** Description of the rule.
- **Rank:** The ranking system provides a way to quantify the importance of events. By assigning "asset values" to computers, and assigning "severity values" to log inspection rules, the importance ("rank") of an event is calculated by multiplying the two values together. This allows you to sort events by rank.
- **Severity:** The log inspection rule's severity value.
- **Groups:** Group that the rule belongs to.
- **Program Name:** Program name. This is obtained from the syslog header of the event.
- **Event:** The name of the event.
- **Location:** Where the log came from.
- **Source IP:** The packet's source IP.
- **Source Port:** The packet's source port.
- **Destination IP:** The packet's destination IP address.
- **Destination Port:** The packet's destination port.
- **Protocol:** Possible values are "ICMP", "ICMPV6", "IGMP", "GGP", "TCP", "PUP", "UDP", "IDP", "ND", "RAW", "TCP+UDP", AND "Other: nnn" where nnn represents a three digit decimal value.
- **Action:** The action taken within the event
- **Source User:** Originating user within the event.
- **Destination User:** Destination user within the event.
- **Event HostName:** Hostname of the event source.

- **ID:** Any ID decoded as the ID from the event.
- **Status:** The decoded status within the event.
- **Command:** The command being called within the event.
- **URL:** The URL within the event.
- **Data:** Any additional data extracted from the event.
- **System Name:** The system name within the event.
- **Rule Matched:** Rule number that was matched.
- **Event Origin:** The Deep Security component from which the event originated.

### List of log inspection security events

**Note:** For system events related to log inspection, see "System events" on page 1233.

| ID | Severity | Event |
|---|---|---|
| 8100 | Error | Log Inspection Engine Error |
| 8101 | Warning | Log Inspection Engine Warning |
| 8102 | Info | Log Inspection Engine Initialized |

## Web reputation events

For general best practices related to events, see "About Deep Security event logging" on page 1046.

To see the web reputation events captured by Deep Security, go to **Events & Reports** > **Events** > **Web Reputation Events**.

### What information is displayed for web reputation events?

These columns can be displayed on the web reputation events page. You can click **Columns** to select which columns are displayed in the table.

- **Time:** Time the event took place on the computer.
- **Computer:** The computer on which this event was logged. (If the computer has been removed, this entry will read "Unknown Computer".)
- **URL:** The URL that triggered this event.
- **Tag(s):** Event tags associated with this event.

- **Risk:** What was the risk level of the URL that triggered the event ("Suspicious", "Highly Suspicious", "Dangerous", "Untested", or "Blocked by Administrator").
- **Rank:** Rank provides a way to quantify the importance of events. It is calculated by multiplying the asset value of the computer by the severity of the rule. (See "Rank events to quantify their importance" on page 1065.)
- **Event Origin:** Indicates from which part of the Deep Security system the event originated.

### Add a URL to the list of allowed URLs

If you want to add the URL that triggered an event to the list of allowed URLs, right-click the event and select **Add to Allow List**. (To view or edit the **Allowed** and **Blocked** lists, go to the **Exceptions** tab on the main **Web Reputation** page.)

# Troubleshoot common events, alerts, and errors

## Why am I seeing firewall events when the firewall module is off?

If you have Intrusion Prevention or Web Reputation enabled, you may see some Firewall events because the Intrusion Prevention and Web Reputation modules leverage the Firewall’s stateful configuration mechanism to perform inspections.

## Troubleshoot event ID 771 "Contact by Unrecognized Client"

Event ID 771 **Contact by Unrecognized Client** appears on Deep Security Manager if a Deep Security Agent tries to connect to the manager, but the computer's name doesn't exist in the list of protected computers on **Computers**.

Common causes include:

- Cloned VMs or cloud instances if you haven't enabled **Reactivate cloned Agents**.
- Computers deleted from **Computers** *before* deactivating Deep Security Agent, if you haven't enabled **Reactivate unknown Agents**. The agent software continues to try to periodically connect to its manager, causing the event each time until either it is uninstalled, or you reactivate the computer.
- Interrupted sync of a connector such as vCenter, AWS, or Azure. For example, if a VMware ESXi host is not shut down gracefully due to a power failure, then the VM's information may not be correctly synchronized.

Solutions vary by the cause.

### Uninstall Deep Security Agent

If you don't want to protect the unrecognized computer, you can prevent these events by deactivating or uninstalling the Deep Security Agent software. See "Uninstall Deep Security" on page 1554.

### Reactivate the computer or clone

If you want to protect the computer, activate it with Deep Security Manager. Re-activation re-establishes the agent's certificate so that the manager can authenticate it with the list on **Computers**, and recognize the computer. See "Agent-initiated activation (AIA)" on page 1399.

### Fix interrupted VMware connector synchronization

1. On Deep Security Manager, go to **Computers**.
2. Remove the vCenter connector.
3. On VMware vSphere, reset the Deep Security Virtual Appliance (DSVA).

   This will clear the information in:

   ```
   /var/opt/ds_agent/guests
   ```
4. Add the vCenter into the Deep Security Manager again.
5. Re-activate the VMs.

## Troubleshoot "Smart Protection Server disconnected" errors

If you are using the anti-malware or web reputation modules, you may see either a "Smart Protection Server Disconnected for Smart Scan" or "Smart Protection Server Disconnected for Web Reputation" error in the Deep Security Manager console. To fix the error, try the following troubleshooting tips.

### Check the error details

Double-click the error message to display more detailed information, including the URL that the server is trying to contact. The error may include:

- Timeout was reached
- Couldn't resolve hostname

From a command prompt, use nslookup to check whether the DNS name resolves to an IP address. If the URL doesn't resolve, then there is a DNS issue on the local server.

Use a telnet client to test connectivity to the URL on ports 80 and 443. If you can't connect, check that all of your firewalls, security groups, etc. are allowing outbound communication to the URL on those ports.

## Error: Activation Failed

Several events can trigger an "Activation Failed" alert:

- "Protocol Error" below
- "Unable to resolve hostname" on the next page
- "No agent/appliance" on the next page
- "Blocked port" on the next page
- "Duplicate Computer" on page 1313
- "Endpoint behind proxy" on page 1314
- "Reinstallation required" on page 1314

### Protocol Error

This error typically occurs when you use Deep Security Manager to attempt to activate a Deep Security Agent and the manager is unable to communicate with the agent. The communication directionality that the agent uses determines the method that you should use to troubleshoot this error. (See "Agent-manager communication" on page 1374.)

#### Agent-initiated communication

When the agent uses agent-initiated communication, you need to activate the agent from the agent computer. (See "Activate Deep Security Agent" on page 1578.)

> Tip: Ensure that the console allows agent-initiated activation by going to **Administration > System Settings > Agent** and selecting **Allow Agent-Initiated Activation**.

#### Bidirectional communication

Use the following troubleshooting steps when the error occurs and the agent uses bidirectional communication:

1. Ensure that the agent is installed on the computer and that the agent is running.
2. Ensure that the ports are open between the manager and the agent. (See "Port numbers, URLs, and IP addresses" on page 478 and "Create a firewall rule" on page 864.)

### Unable to resolve hostname

The error: Activation Failed (Unable to resolve hostname) could be the result of an unresolvable hostname in DNS or of activating the agent from Deep Security Manager when you are not using agent-initiated activation.

If your agent is in bidirectional or manager-initiated mode, your hostname must be resolvable in DNS. Check the DNS on your Deep Security Manager to ensure it can resolve your hosts.

If you your computers are in cloud accounts, we recommend that you always use agent-initiated activation. To learn how to configure policy rules for agent-initiated communication and deploy agents using deployment scripts, see "Activate and protect agents using agent-initiated activation and communication" on page 1386.

### No agent/appliance

This error message indicates that the agent software has not been installed on the computer that you would like to protect.

### Blocked port

If you are seeing 'Activation Failed' events with the following error messages in the `ds_agent.log`:

```
• 2018-06-25 17:52:14.000000: [Error/1] | CHTTPServer::AcceptSSL (<IP>:<PORT>) - BIO_do_handshake() failed - peer closed connection. | http\HTTPServer.cpp:246:DsaCore::CHTTPServer::AcceptSSL | 1E80:1FEC:ActivateThread
```

```
• 2018-06-25 17:52:14.143355: [dsa.Heartbeat/5] | Unable to reach a manager. | .\dsa\Heartbeat.lua:149:(null) | 1E80:1FEC:ActivateThread
```

```
• 2018-06-25 17:52:14.000000: [Info/5] | AgentEvent 4012 | common\DomainPrivate.cpp:493:DsaCore::DomPrivateData::AgentEventWriteHaveLock | 1E80:1FEC:ActivateThread
```

```
• 2018-06-25 17:52:14.143355: [Cmd/5] | Respond() - sending status line of 'HTTP/1.1 400 OK' | http\HTTPServer.cpp:369:DsaCore::CHTTPServer::Respond | 1E80:1D7C:ConnectionHandlerPool_0011
```

...and the following messages in your packet capture software (pcap):

```
• [TCP Retransmission] <Ephemeral Port> -> 443 [SYN, ECN, CWR] .......
```

```
• [TCP Retransmission] <Ephemeral Port> -> 443 [SYN] .......
```

...it may be because you have blocked a port used by the Deep Security Agents and manager to establish communication. agent-manager communication ports could be any of the following:

| Agent-manager communication type | Source / Port | Destination / Port |
|---|---|---|
| Agent-initiated communication | Deep Security Agent / Ephemeral port | Manager / 4119 |
| Manager-initiated communication | Deep Security Manager / Ephemeral port | Agent / 4118 |

As you can see from the table above, ephemeral ports are used for the source port for outbound communication between agent and manager. If those are blocked, then the agent can't be activated and heartbeats won't work. The same problems arise if any of the destination ports are blocked.

To resolve this issue:

- Remove restrictions on client outbound ports (ephemeral) in your network configuration.
- Allow access to Deep Security Manager on port 4119.
- Allow inbound access to Deep Security Agent on port 4118 if you're using Manager-initiated communication.

For details on ports, see "Port numbers, URLs, and IP addresses" on page 478.

## Duplicate Computer

This error typically occurs when you activate a computer using a name that already exists, or a computer that is already active in a different connector.

To resolve this issue you can use one of the following methods:

- Remove one of the duplicate computers and reactivate the remaining computer if necessary.
- From the Deep Security Manager, go to **Administration > System Settings > Agents** and select your preferences for agent-initiated activation. If a computer with the same name already exists, there are options to re-activate the existing computer, activate a new computer with the same name, or not allow activation. For more details, see "Agent-initiated activation (AIA)" on page 1399.

### Endpoint behind proxy

If you are using a proxy, in the Deep Security Manager go to **Support > Deployment Scripts** and update the fields with your proxy, then reactivate the agent. For more information, see "Use deployment scripts to add and protect computers" on page 1623.

### Reinstallation required

If Deep Security Agent is not activating, you may need to "Uninstall Deep Security Agent" on page 1556, then reinstall Deep Security Agent.

## Error: Agent version not supported

The error message "Agent version not supported" indicates that the agent version currently installed on the computer is not supported by the Deep Security Manager.

Although the unsupported agent will still protect the computer based on the last policy settings it received from the Deep Security Manager, we recommend that you upgrade the agent so that you can react quickly to the latest threats. For more information, see "Upgrade Deep Security Agent" on page 1542.

## Error: Anti-Malware Engine Offline

> **Note:** A common cause for this error is having Secure Boot enabled without a public key enrolled. Before continuing, Secure Boot users should consider checking that a public key is properly enrolled as detailed in the following article: Linux Secure Boot support for agents. If you encounter this error and do not want to use Secure Boot, you can simply disable it to bring the Anti-Malware Engine back online.

This error can occur for a variety of reasons. To resolve the issue, follow the instructions below for the mode of protection that is being used:

- "Agent-based protection" on the next page
- "Agentless protection" on page 1316

For an overview of the Anti-Malware module, see "About Anti-Malware" on page 735.

## Agent-based protection

1. In the Deep Security Manager, check for other errors on the same machine. If errors exist, there could be other issues that are causing your Anti-Malware engine to be offline, such as communications or Deep Security Agent installation failure.
2. Check communications from the agent to the Deep Security Relay and the manager.
3. In the Deep Security Manager, view the details for the agent with the issue. Verify that the policy or setting for Anti-Malware is turned on, and that the configuration for each scan (real-time, manual, scheduled) is in place and active. (See "Enable and configure Anti-Malware" on page 742.)
4. Deactivate and uninstall the agent before reinstalling and re-activating it. See "Uninstall Deep Security" on page 1554 and "Activate the agent" on page 566 for more information.
5. In the Deep Security Manager, go to the **Updates** section for that computer. Verify that the Security Updates are present and current. If not, click **Download Security Updates** to initiate an update.
6. Check if there are conflicts with another anti-virus product, such as OfficeScan. If conflicts exist, uninstall the other product and Deep Security Agent, reboot, and reinstall the Deep Security Agent. To remove OfficeScan, see Manually uninstalling clients or agents in OfficeScan (OSCE).

**If your agent is on Windows:**

1. Make sure the following services are running:
   - Trend Micro Deep Security Agent
   - Trend Micro Solution Platform
2. Check that all the anti-malware related drivers are running properly by running the following commands:

   For all versions of Deep Security Agent:

   - `# sc query AMSP`

   For Deep Security Agent 12.5 or earlier, also check:

   - `# sc query tmcomm`
   - `# sc query tmactmon`
   - `# sc query tmevtmgr`

If a driver is not running, restart the Trend Micro services. If it is still not running, continue with the steps below.

3. Verify the installation method. Only install the MSI, not the zip file.
4. The agent might need to be manually removed and reinstalled. For more information, see Manually uninstalling Deep Security Agent, Relay, and Notifier from Windows
5. The installed Comodo certificate could be the cause of the issue. To resolve the issue, see "Anti-Malware Driver offline" status occurs due to Comodo certificate issue.

**If your agent is on Linux:**

1. To check that the agent is running, enter the following command in the command line:
   - `service ds_agent status`
2. If you are using a Linux server, your kernel might not be supported. For more information, see "Error: Module installation failed (Linux)" on page 1322.

If the problem is still unresolved after following these instructions, create a diagnostic package and contact support. For more information, see "Create a diagnostic package" on page 1723.

## Agentless protection

1. In the Deep Security Manager, verify synchronization to vCenter and NSX. Under the **Computers** section, right click on your vCenter and go to **Properties**. Click **Test Connection**. Then click on the NSX tab and test the connection. Click **Add/Update Certificate** in case the certificate has changed.
2. Log into the NSX manager and verify that it is synching to vCenter properly.
3. Log into your vSphere client and go to **Network & Security > Installation > Service Deployments**. Check for errors with Trend Micro Deep Security and Guest Introspection, and resolve any that are found.
4. In vSphere client, go to **Network & Security > Service Composer**. Verify that the security policy is assigned to the appropriate security group.
5. Verify that your VMware tools are compatible with Deep Security. For more information, see VMware Tools 10.x Interoperability Issues with Deep Security.
6. Verify that the File Introspection Driver (vsepflt) is installed and running on the target VM. As an admin, run `sc query vsepflt` at the command prompt.
7. All instances and virtual machines deployed from a catalog or vApp template from vCloud Director are given the same BIOS UUID. Deep Security distinguishes different VMs by there BIOS UUID, so a duplicate value in the vCenter causes an Anti-Malware Engine Offline error. To resolve the issue, see VM BIOS UUIDs are not unique when virtual machines are deployed from vApp templates (2002506).
8. If the problem is still unresolved, open a case with support with the following information:

- Diagnostic package from each Deep Security Manager. For more information, see "Create a diagnostic package" on page 1723.
- Diagnostic package from the Deep Security Virtual Appliance.
- vCenter support bundle for the effected VMs.

## Error: Device Control Engine Offline

This error can occur for a variety of reasons. To resolve the issue, follow the instructions below.

For an overview of the Device Control module, see "Configure Device Control" on page 898.

1. In the Deep Security Manager console, check for other errors on the same machine. If errors exist, there could be other issues that are causing your Device Control engine to be offline, such as communications or agent installation failure.
2. Check communications from the agent to the Deep Security Relay and Deep Security Manager.
3. In the Deep Security Manager console, view the details for the agent with the issue. Verify that the policy or setting for Device Control is turned on.
4. Deactivate and uninstall the agent before reinstalling and re-activating it. See "Uninstall Deep Security" on page 1554 and "Activate the agent" on page 566 for more information.
5. In the Deep Security Manager console, go to the Updates section for that computer. Verify that the Security Updates are present and current. If not, click Download Security Updates to initiate an update.
6. Check if there are conflicts with another anti-virus product, such as OfficeScan. If conflicts exist, uninstall the other product and Deep Security Agent, reboot, and reinstall the Deep Security Agent. To remove OfficeScan, see Troubleshooting guide for client and agent manual uninstallation issues in OfficeScan.

### If your agent is on Windows

1. Make sure the following services are running:
   - Trend Micro Deep Security Agent
   - Trend Micro Solution Platform

2. Check that all the Device Control related drivers are running properly by running the following commands:

   For all versions of Deep Security Agent:

   - `# sc query AMSP`

If a driver is not running, restart the Trend Micro services. If it is still not running, continue with the following steps.

3. Verify the installation method. Only install the MSI, not the ZIP file.
4. The agent might need to be manually removed and reinstalled. For more information, see Manually uninstalling Deep Security Agent, Relay, and Notifier from Windows

## Error: Check Status Failed

You can check the status of the agent / appliance on a computer from the Deep Security Manager console. On the Computers page, right-click the computer and click **Actions > Check Status**.

If you get a "Check Status Failed" error, open the error message to see a more detailed description.

If description indicates a protocol error, it's usually caused by a communication issue. There are a few possible causes:

- Check whether the computer (or the policy assigned to the computer) is configured for agent-initiated communication or bidirectional communication. The "Check Status" operation will fail if you are using agent-initiated communication.
- Check that the Deep Security Manager can communicate with the agent. The manager should be able to reach the agent. See "Port numbers, URLs, and IP addresses" on page 478.
- Check the resources on the agent computer. Lack of memory, CPU, or disk space can cause this error.

If the description indicates a SQLITE_IOERR_WRITE[778]: disk I/O error, there is likely a problem with the agent computer. The most common problem is that the disk is full or write-protected.

## Error: Installation of Feature 'dpi' failed: Not available: Filter

The error message "Installation of Feature 'dpi' failed: Not available: Filter" indicates that your operating system kernel version is not supported by the network driver. You will typically get this message when installing Intrusion Prevention, Web Reputation, or Firewall because the Deep Security Agent installs a network driver at the same time in order to examine traffic. The same circumstances can cause **engine offline** alerts.

An update may be on its way. Trend Micro actively monitors a variety of operating system vendors for new kernel releases. After completing quality assurance tests, we will release an update with support for these kernels.

Your system will install the required support automatically when an update for your operating system kernel version becomes available.

Contact technical support (sign in Deep Security, and click **Support** in the top right-hand corner) to find out when support for your operating system kernel version will be released.

### Additional information

This only affects Intrusion Prevention, Web Reputation, and Firewall. All other protection modules (Anti-Malware, Integrity Monitoring, and Log Inspection) will operate correctly.

To review supported operating system kernel versions, visit the Deep Security 9.6 Supported Linux Kernels page and look for your operating system distribution.

## Error: Intrusion Prevention Rule Compilation Failed

This error can occur for a variety of reasons. Perform the following to confirm that the error is legitimate:

Resend the policy:

1. On the Deep Security Manager, click **Computers**.
2. Right-click the computer where the error occurred.
3. Go to **Actions > Send Policy**.

Verify status:

1. On the Deep Security Manager, click **Computers**.
2. Right-click the computer where the error occurred.
3. Go to **Actions > Clear Warnings/Errors**.
4. Once the warnings and errors are cleared, go to **Actions > Check Status**.

If the error continues to occur after completing the preceding steps, troubleshoot the issue with the solutions using the following solutions:

- "Apply Intrusion Prevention best practices" on the next page
- "Manage rules" on the next page
- "Unassign application types from a single port" on page 1321

If the error persists, contact technical support.

## Apply Intrusion Prevention best practices

The Intrusion Prevention Rule Compilation Failed error can occur due to a lack of resources on the machine, such as space, memory, or CPU. To help resolve this issue, apply the best practices on "Performance tips for intrusion prevention" on page 848.

## Manage rules

The Intrusion Prevention Rule Compilation Failed error can occur when the number of assigned Intrusion Prevention rules exceeds the recommended count. You should not have more than 400 Intrusion Prevention rules on an endpoint. It is recommended to only apply the Intrusion Prevention rules that a recommendation scan suggests in order to avoid applying unnecessary rules. If you are applying Intrusion Prevention rules manually, apply them to the computer rather than the policy to avoid adding too many application types to a single port.

To resolve the issue, reduce the number of assigned rules, as follows:

1. Access the Intrusion Prevention rules depending on how you assigned them. Do either of the following:
   - At the computer level, go to the **Computers** tab, right-click the computer and select **Details**.
   - At the policy level, go to the **Policies** tab, right-click the policy and select **Details**.
2. Go to **Intrusion Prevention** and click **Scan for Recommendations**.
3. Once the scan is complete, click **Assign/Unassign**. At the top of the window, filter the rules by **Recommended for Unassignment**.
4. To unassign a rule, select the check box next to the rule name. Alternatively, to unassign several rules at once use the Shift or Control keys to select the rules.
5. Right-click the rule or selection of rules to be removed and go to **Unassign Rule(s) > From All Interfaces**, then click **OK**. Close the window.
6. On the **Computers** tab right-click the computer, and go to **Actions > Clear Warnings/Errors**. The Intrusion Prevention engine will automatically attempt a rule compilation. The duration of the process will depend on the heartbeat interval and communication settings between Deep Security Manager and Agent.

Tip: If you applied Intrusion Prevention rules through a policy and are unsure which computers are affected, open the **Policy editor**[1] and go to **Overview > Computer(s) Using This Policy**.

[1] To open the Policy editor, go to the Policies page and double-click the policy that you want to edit (or select the policy and click Details).

### Unassign application types from a single port

The Intrusion Prevention Rule Compilation Failed error can occur when a single port is assigned with too many application types. Currently, a port can only be assigned to sixteen application types.

To resolve the issue, remove an assigned application type from a port, as follows:

1. To determine which rule encountered the issue, double-click the error to open the **Event Viewer**.
2. Go to the **Computers** tab.
3. Right-click the computer with the misconfigured Intrusion Prevention rule and select **Details**.
4. Go to **Intrusion Prevention**.
5. Click **Assign/Unassign**. In the search bar, enter the name of the misconfigured rule.
6. Right-click the rule and select **Application Type Properties**.
7. Deselect the **Inherited** check box.
8. Delete the port and enter a new one.
9. Click **Apply** and **OK**.

## Error: Log Inspection Rules Require Log Files

If a log inspection rule requires you to add the location of the files to be monitored, of if you add an unnecessary log inspection rule and the files do not exist on your machine, the following error will occur in the **Computer**[1] or **Policy editor**[2]:

To resolve the error:

1. Click on the **Log Inspection Rules Require Log Files** error. A window will open with more information about the error. Under **Description**, the name of the rule causing the error will be listed.
2. In the Deep Security Manager, go to **Policies > Common Objects > Rules > Log Inspection Rules** and locate the rule that is causing the error.
3. Double-click the rule. The rule's properties window will appear.
4. Go to the **Configuration** tab.

[1] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2] To open the Policy editor, go to the Policies page and double-click the policy that you want to edit (or select the policy and click Details).

**If the file's location is required:**

1. Enter the location under **Log Files to monitor** and click **Add**.
2. Click **OK**. Once the agent receives the policy, the error will clear.

**If the files listed do not exist on the protected machine:**

1. Go to the **Computer**[1] **or Policy editor**[2] **> Log Inspection**.
2. Click **Assign/Unassign**.
3. Locate the unnecessary rule and uncheck the checkbox.
4. Click **OK**. Once the agent receives the policy, the error will clear.

To prevent this error, run a recommendation scan for suggested rules:

1. On the Deep Security Manager, go to **Computers**.
2. Right-click the computer you'd like to scan and click **Actions > Scan for Recommendations**.
3. View the results on the **General** tab of the protection module in the **Computer**[3] or **Policy editor**[4].

## Error: Module installation failed (Linux)

The error message "Module Installation Failed" indicates that your operating system's kernel version is not supported by the Deep Security network driver, or file system hook. These circumstances can cause **engine offline** alerts. Lack of a compatible network driver is the most common cause of this message.

When you apply intrusion prevention, web reputation, or firewall, the Deep Security Agent installs a network driver so it can examine traffic. Anti-malware and integrity monitoring install a file system hook module. This is required to monitor file system changes in real time. (Scheduled scans do not require the same file system hook.)

An update may be in progress. Trend Micro monitors many vendors for new kernel releases. After completing quality assurance tests, we release an update with support for these kernels. To ask

[1] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2] To open the Policy editor, go to the Policies page and double-click the policy that you want to edit (or select the policy and click Details).

[3] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[4] To open the Policy editor, go to the Policies page and double-click the policy that you want to edit (or select the policy and click Details).

when support for your kernel version will be supported, contact technical support. (When logged in, you can click **Support** in the top right corner.)

Your system will install the module support update automatically when it becomes available.

To view supported operating system kernel versions, see "Linux kernel compatibility" on page 408.

## Error: There are one or more application type conflicts on this computer

The following error message appears in the DPI Events tab in Deep Security Manager when updating the Deep Security Agents:

"There are one or more application type conflicts on this computer. One or more DPI rules associated with one application type are dependent on one or more DPI rules associated with another application type. The conflict exists because the two application types use different ports."

The conflicting application types are:

```
[A] "Web Application Tomcat" Ports: [80,8080,4119]
```

```
[B] "Web Server Common" Ports:
[80,631,8080,7001,7777,7778,7779,7200,7501,8007,
8004,4000,32000,5357,5358,9000]
```

```
[A] "Web Server Miscellaneous" Ports:
[80,4000,7100,7101,7510,8043,8080,8081,8088,8300,8500,
8800,9000,9060,19300,32000,3612,10001,8093,8094]
```

```
[B] "Web Server Common" Ports:
[80,631,8080,7001,7777,7778,7779,7200,7501,8007,
8004,4000,32000,5357,5358,9000]"
```

### Resolution

To resolve the conflict, edit the port numbers used by application types B so that they include the port numbers used by application types A. The two application types (Web Application Tomcat and Web Server Miscellaneous) are both dependent on the application type Web Server Common. This is why the ports listed in the first two application types should also appear in the Web Server Common ports.

If you consolidate the port numbers for these three application types, the result is as follows:

```
80,631,3612,4000,4119,5357,5358,7001,7100,7101,7200,7501,7510,7777,7778,7779,

8004,8007,8043,8080,8081,8088,8093,8094,8300,8500,8800,9000,9060,10001,19300,
32000
```

After adding this to the Web Server Common port list, the following message appears in the **Events** tab:

"The Application Type Port List Misconfiguration has been resolved."

### Consolidate ports

1. Log in to Deep Security Manager and go to **Policies > Rules > Intrusion Prevention Rules**.

2. Search for **Web Server Common** and double-click the Web Server Common application type.
3. Go to **General > Details > Application type > Edit > Web server common**.
4. Go to **General > Connection > Port** and click **Edit** to replace all of the ports with this consolidated entry: `80,631,3612,4000,4119,5357,5358,7001,7100,7101,7200, 7501,7510,7777,7778,7779,8004,8007,8043,8080,8081,8088,8093, 8094,8300,8500,8800,9000,9060,10001,19300,32000`
5. Click **OK**.

A modified port list is excluded from automatic rule updates. When you reset it, any manually modified content is reset.

### Disable the inherit option

It is also recommended that administrators disable the inherit option for DPI for a security profile. Any change you make to the application type will only affect this particular security profile.

1. Log on to Deep Security Manager and go to **Security Profiles**.
2. Double-click a security profile in the right pane.
3. Go to the **DPI** section and deselect **Inherit** .
4. Click **OK**.

Check the IPS rule 1000128:

1. Right-click **Application Type Properties**.
2. Deselect **Inherit**.
3. Verify that the current inherited port list contains the listening port number for the Deep

Security Manager's GUI. If not, add this port to the Web Server Common port group.

4. Click **Inherit**.

## Error: Unable to connect to the cloud account

When adding an Amazon Cloud account, the error "Unable to connect to the cloud account" can occur. The cause can be:

- invalid key ID or secret
- incorrect permissions
- failed network connectivity

### Your AWS account access key ID or secret access key is invalid

**To resolve this:**

Verify the security credentials that you entered.

### The incorrect AWS IAM policy has been applied to the account being used by Deep Security

**To resolve this:**

Go you your AWS account and review the IAM policy for that account.

The AWS IAM policy must have these permissions:

- Effect: Allow
- AWS Service: Amazon EC2
- Select the following Actions:
  - DescribeImages
  - DescribeInstances
  - DescribeTags
- Amazon Resource Name (ARN) to: *

### NAT, proxy, or firewall ports are not open, or settings are incorrect

This can occur in a few cases, including if you are deploying a new Deep Security Manager installation using the AMI on AWS Marketplace.

Your Deep Security Manager must be able to connect to the Internet, specifically to Amazon Cloud, on the required port numbers.

To resolve this:

You may need to:

- configure NAT or port forwarding on a firewall or router between your AMI and the Internet
- get an external IP address for your AMI

The network connection must also be reliable. If it is intermittent, this error message may occur sometimes (but not every time).

## Error: Unable to resolve instance hostname

The error message "Unable to Resolve Instance Hostname" may occur as a result of activating the Agent from Deep Security Manager when you are not using agent-initiated activation.

We recommend that you always use **Agent-Initiated Activation**.To learn how to configure policy rules for agent-initiated communication and deploy agents using deployment scripts, see "Activate and protect agents using agent-initiated activation and communication" on page 1386.

## Alert: Integrity Monitoring information collection has been delayed

This alert indicates that the rate at which integrity monitoring information is collected has been temporarily delayed. The delay is due to an increase in the volume of integrity monitoring data that is being transmitted from agents to Deep Security Manager. During this time the baseline and integrity monitoring event views may not be current for some computers.

This alert is automatically dismissed when the collection of integrity monitoring data is no longer delayed.

For more information about integrity monitoring, see "Set up Integrity Monitoring" on page 901.

## Alert: Manager Time Out of Sync

The system time on the Deep Security Manager operating system must be synchronized with the time on the database computer. This alert appears in the Alert Status widget of the manager console when the computer times are more than 30 seconds out of sync.

To synchronize the times, apply the following configurations:

- Configure the database and all manager nodes to use the same time zone.
- Ensure that the database and all manager nodes are synchronizing time to the same time source.
- If the manager runs on a Linux operating system, ensure the ntpd daemon is running.

## Alert: The memory warning threshold of Manager Node has been exceeded

The **Memory Warning Threshold Exceeded** or **Memory Critical Threshold Exceeded** alerts appear in Deep Security to alert you that a host's memory usage has exceeded a certain amount. A warning alert indicates that 70% of the host's memory is used, and a critical alert indicates that usage has exceeded 85%.

To resolve this issue, determine whether there are processes unexpectedly consuming a large amount of memory:

- If the identified process **is not Deep Security Manager**, remove or eliminate the processes from the host. Deep Security Manager should run on a dedicated host computer.
- If the process **is Deep Security Manager**, increase the amount of the host memory. Refer to "Sizing" on page 467 for guidelines.

**Note:** By default, the maximum heap size of Deep Security Manager is 4 GB. That means Deep Security Manager allocates a maximum 4 GB heap; however, the JVM allocates not only heap but also non-heap. Consequently, the maximum total memory size of the Deep Security Manager process will be larger than 4 GB.

**Note:** If the host is a VM, we strongly suggest that you reserve all guest memory for the VM.

## Event: Max TCP connections

Deep Security is configured to allow a maximum number of TCP connections to protected computers. When the number of connections exceeds the maximum, network traffic is dropped and Max TCP Connections firewall events occur. To prevent dropped connections, increase the maximum allowed TCP connections on the computer where the Max TCP Connection event occurs.

**Note:** The intrusion protection module enables the network engine which enforces the allowed number of TCP connections.

1. In Deep Security Manager, click **Policies**.
2. Determine which policy to configure to affect the computer in question. See "Policies, inheritance, and overrides" on page 634.
3. To open the policy that you want to configure, double-click the policy.
4. In the left-hand pane, click **Settings** and then click the **Advanced** tab.
5. In the **Advanced Network Engine Settings** area, if Inherit is selected clear the checkbox to enable changes.
6. Increase the value of the **Maximum TCP Connections** property to 10000 or more, according to your needs.
7. Click **Save**.

## Warning: Anti-Malware Engine has only Basic Functions

When new kernel versions are released, Trend Micro creates and releases kernel support packages for them. If your kernel version is not supported by the Linux agent, the Linux Anti-Malware Engine provides only basic protection to your computers. The Anti-Malware engine will return back to normal status from the basic function mode when your kernel version is supported.

### Basic functions

| Category | Feature name | Supported |
|---|---|---|
| Scan / Detection | Document exploit protection | ✓ |
| | Predictive machine learning | (1) |
| | Behavior monitoring | |
| | Spyware/Grayware | ✓ |
| | IntelliTrap | ✓ |
| | Scan compressed file | ✓ |
| | Smart scan | ✓ |
| | Connected threat defense | ✓ |

| Category | Feature name | Supported |
|---|---|---|
| Inclusion / Exclusion | Document exploit protection | ✓ |
| | Directories inclusion | ✓ |
| | File inclusion | ✓ |
| | Directories exclusion | ✓ |
| | File exclusion | ✓ |
| | File extension exclusion | ✓ |
| | Process image file exclusion (2) | ✓ |
| Quarantine | Quarantine file | ✓ |
| | Restore file | ✓ |
| Container | Container protection | (3) |

**(1) Predictive machine learning**: Even though this may occasionally work (if Trend Micro can get the process image path), it is not reliable and therefore not supported.
**(2) Process image file exclusion**: This is moved to user-mode match. This mode may have performance impact.
**(3) Container protection**: Trend Micro cannot protect runtime container workloads in this mode.

## Reason IDs

In a case where partial functionality is in operation, to ensure that the Linux agent returns to full functionality, it is necessary to take other steps that depend on the reason ID. The reason ID is included in events forwarded to an external Syslog, SIEM server, or to Amazon SNS. It is also displayed in event description for Linux agent (either Anti-Malware Engine Offline or Anti-Malware Engine with Basic Functions).

- **Reason ID 7**: No driver is available for the particular kernel version causes a driver offline error. To resolve this: **Check if latest Kernel Support Package (KSP) is released for that particular kernel. File a case to request KSP support.**

- **Reason ID 11**: The Trend Micro public key--on the system when SecureBoot is enabled--is **missing**, so loading the driver failed, which caused a driver offline error. To resolve this: "Configure Linux Secure Boot for agents" on page 527.
- **Reason ID 12**: The Trend Micro public key--on the system when SecureBoot is enabled--is **expired**, so loading the driver failed, which caused a driver offline error. To resolve this: "Configure Linux Secure Boot for agents" on page 527.
- For **all other reason IDs**: "Create a diagnostic package" on page 1723 and contact support.

| Reason ID | Event reason | Description |
|---|---|---|
| 1 | Unknown reason | The malware scan failed for an unknown reason. |
| 2 | Incomplete Anti-Malware installation | Incomplete installation of the Anti-Malware service has caused a driver offline error. |
| 3 | Failed process communication between DSA and AM service | The process communication between the Deep Security Agent and Anti-Malware service failed and had caused a driver offline error. |
| 4 | Timeout of restart | Windows Anti-Malware service (AMSP) restarted timeout (that is, the sign check process has hung). |
| 5 | Stopped Anti-Malware service | The Anti-Malware service has stopped unexpectedly and has caused a driver offline error. |
| 6 | Failed sign check | A Windows files (binaries or DLL) sign check failed unexpectedly. |
| 7 | Unavailable kernel version | No driver is available for the particular kernel version and has caused a driver offline error. |
| 8 | Failed driver loading | Load driver via tmhook or bmhook into kernel has failed and has caused a driver offline error. |
| 9 | Failed driver unloading | Unloading a driver from kernel failed and has caused a driver offline error.<br>**Note:** No such scenario is needed, therefore, Trend Micro never reports this code in DsspState on Linux |

| Reason ID | Event reason | Description |
|---|---|---|
| | | platforms. |
| 10 | Failed driver device opening | Opening a driver device file failed and has caused a driver offline error. |
| 11 | Missing machine owner key Trend Micro public key | Missing machine owner key Trend Micro public key on the system when SecureBoot is enabled results in a driver load failed and this has caused a driver offline error. |
| 12 | Expired machine owner key Trend Micro public key | The machine owner key Trend Micro public key on the system is expired when SecureBoot is enabled results in a driver load failed and this has caused a driver offline error. |
| 13 | Signed with unauthorized public key | The driver was signed with an unknown or unsupported public key. |
| 14 | Configuration file disable driver | Agent is set to not load the driver by configuration INI file. This causes a driver offline state. |
| 15 | Policy disable driver | Agent is set to not load the driver by the Deep Security policy. This causes a driver offline state. |

## Warning: Census, Good File Reputation, and Predictive Machine Learning Service Disconnected

The Census, Good File Reputation, and Predictive Machine Learning Services are security services hosted by the Trend Micro Smart Protection Network. They are necessary for the full and successful operation of the Deep Security behavior monitoring, predictive machine learning, and process memory scan features.

The following table maps the services to features.

| Service name | Required for these features |
|---|---|
| Global Census Service | behavior monitoring, predictive machine learning |
| Good File Reputation Service | behavior monitoring, predictive machine learning, process memory scans |

| Service name | Required for these features |
|---|---|
| Predictive Machine Learning Service | predictive machine learning |

If you see the alert...

*Census, Good File Reputation, and Predictive Machine Learning Service Disconnected*

...there are a few causes:

- "Cause 1: The agent or relay-enabled agent doesn't have Internet access" below
- "Cause 2: A proxy was enabled but not configured properly" below

## Cause 1: The agent or relay-enabled agent doesn't have Internet access

If your agent or relay-enabled agent doesn't have access to the Internet, then it can't reach these services.

Solutions:

- Check your firewall policies and ensure that the outbound HTTP and HTTPS ports (by default, 80 or 443) are open.
- If you are unable to open those ports, see "Configure agents that have no internet access" on page 1379 for other solutions.

## Cause 2: A proxy was enabled but not configured properly

The Census, Good File Reputation and Predictive Machine Learning Services can be accessed using a proxy.

To check whether a proxy was enabled and make sure it was configured properly:

1. Open the **Computer or Policy editor**[1].
2. On the left, click Settings.
3. In the main pane, click the General tab.
4. Find the heading titled, **Network Setting for Census, Good File Reputation Service, and Predictive Machine Learning**.

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

5. If a proxy was specified, click **Edit** and make sure its **Proxy Protocol**, **Address**, **Port** and optional **User Name** and **Password** are accurate.

## Warning: Insufficient disk space

An "Insufficient Disk Space" warning indicates that the computer where the Deep Security Agent or Appliance is running is low on disk space and may not be able to store more events. If you open the warning to display its details, it will show you the location of the agent or appliance, how much free space is left, and how much is required by the agent or appliance.

To fix this issue, check the drive or file system that's affected and clear anything you can.

**Note:** The agent or appliance will continue to protect your instance even if the drive is out of space; however, it will stop recording events.

### Tips

- Even though the warning is generated by the Deep Security Agent or Appliance, another program that shares the same file system could be causing the space issue.
- Deep Security Agent automatically truncates and rotates its log files during normal operation. (This truncation and rotation is not related to issues with low disk space.)
- Deep Security Agent will clean up its own log files, but not those of other applications.
- Deep Security Manager does not automatically clear the "Insufficient Disk Space" warnings, but you can manually clear them from Deep Security Manager.

## Warning: Reconnaissance Detected

The reconnaissance scan detection feature serves as an early warning of a potential attack or intelligence gathering effort against a network.

### Types of reconnaissance scans

Deep Security can detect several types of reconnaissance scans:

- **Computer OS Fingerprint Probe:** The agent or appliance detects an attempt to discover the computer's OS.
- **Network or Port Scan:** The agent or appliance reports a network or port scan if it detects that a remote IP is visiting an abnormal ratio of IPs to ports. Normally, an agent or appliance computer will only see traffic destined for itself, so a port scan is the most common type of

probe that will be detected. The statistical analysis method used in computer or port scan detection is derived from the "TAPS" algorithm proposed in the paper "Connectionless Port Scan Detection on the Backbone" presented at IPCCC in 2006.

- **TCP Null Scan:** The agent or appliance detects packages with no flags set.
- **TCP SYNFIN Scan:** The agent or appliance detects packets with only the SYN and FIN flags set.
- **TCP Xmas Scan:** The agent or appliance detects packets with only the FIN, URG, and PSH flags set or a value of 0xFF (every possible flag set).

## Suggested actions

When you receive a Reconnaissance Detected alert, double-click it to display more detailed information, including the IP address that is performing the scan. Then, you can try one of these suggested actions:

- The alert may be caused by a scan that is not malicious. If the IP address listed in the alert is known to you and the traffic is okay, you can add the IP address to the reconnaissance allow list:
  a. In the **Computer or Policy editor**[1], go to **Firewall > Reconnaissance**.
  b. The **Do not perform detection on traffic coming from** list should contain a list name. If a list name hasn't already been specified, select one.
  c. You can edit the list by going to **Policies > Common Objects > Lists > IP Lists**. Double-click the list you want to edit and add the IP address.
- You can instruct the agents and appliances to block traffic from the source IP for a period of time. To set the number of minutes, open the **Computer or Policy editor**[2], go to **Firewall > Reconnaissance** and change the **Block Traffic** value for the appropriate scan type.
- You can use a firewall or Security Group to block the incoming IP address.

**Note:** Deep Security Manager does not automatically clear the "Reconnaissance Detected" alerts, but you can manually clear the issue from Deep Security Manager.

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

For more information on reconnaissance scans, see "Firewall settings" on page 878.

# Configure proxies

## Configure proxies

You can configure proxies between various Trend Micro servers and services.

In this topic:

- "Register a proxy in the manager" below
- "Supported proxy protocols" on the next page
- "Connect to the Primary Security Update Source via proxy" on the next page
- "Connect to Deep Security Relays via proxy" on page 1338
- "Connect to Deep Security Manager via proxy" on page 1337
- "Connect to Deep Security Software Updates, CSSS, and more via proxy" on page 1339
- "Connect to cloud accounts via proxy" on page 1340
- "Connect to the Smart Protection Network via proxy" on page 1340
- "Connect to Workload Security via proxy" on page 1342
- "Remove a proxy " on page 1342

### Register a proxy in the manager

1. In Deep Security Manager, go to **Administration** > **System Settings** > **Proxies**.
2. In the **Proxy Servers** area, click **New > New Proxy Server**.
3. In the **Name** and **Description** fields, enter a friendly name and description for your proxy.
4. For the **Proxy Protocol**, select either **HTTP**, **SOCKS4**, or **SOCKS5**. Not all protocols are supported by all components. See "Supported proxy protocols" on the next page for details.
5. In the **Address** and **Port** fields, enter the IP address or URL of the proxy as well its port. The default values are 8080 or 80 for HTTP, 3128 for the Squid HTTP proxy, and 1080 for SOCKS 4 and 5.
6. Enable **Proxy requires authentication credentials** if you previously set up your HTTP or SOCKS 5 proxy to require authentication from connecting components. Enter those credentials in the **User Name** and **Password** fields.

## Supported proxy protocols

The following table lists the proxy protocols supported by the Trend Micro services and clients. You need this information to register and configure a proxy through dsa_control.

| Service | Origin (client) | HTTP Support | SOCKS4 Support | SOCKS5 Support |
|---|---|---|---|---|
| Deep Security Manager | Agents/Relays | Yes | No | No |
| Deep Security Relays | Agents/Relays | Yes | Yes | Yes |
| Deep Security Software Updates, Certified Safe Software Service (CSSS), News Updates, Product Registration and Licensing | Manager | Yes | No | No |
| Deep Security Protected Product Usage Data Collection | Manager | Yes | No | No |
| Cloud accounts (AWS, Azure, Google Cloud Platform, VMware vCloud) | Manager | Yes | No | No |
| Smart Protection Network - Census, Good File Reputation, and Predictive Machine Learning | Agents | Yes | No | No |
| Smart Protection Network - Global Smart Protection Service | Agents | Yes | No | No |
| Smart Protection Network - Smart Feedback | Manager | Yes | No | Yes |

## Connect to the Primary Security Update Source via proxy

You can connect your agents and relays to your primary security update source via a proxy. By default, the primary security update source is the Trend Micro Update Server (also known as Active Update).

Note that the **agents and appliances**[1] only use the proxy if their assigned relay is not available and they have been granted explicit permission to access the primary update source.

1. Make sure that you are using Deep Security Agent 10.0 or later, as connections through a proxy are not suppored in earlier versions.
2. "Register a proxy in the manager" on the previous page.
3. If you are setting the security update proxy for the default relay group, perform the following:

[1] The Deep Securty Agent and Deep Security Virtual Appliance are the components that enforce the Deep Security policies that you have defined. Agents are deployed directly on a computer. Appliances are used in VMware vSphere environments to provide agentless protection. They are not available with Deep Security as a Service.

- In Deep Security Manager, select the **Administration > System Settings > Proxies** tab.
- In the **Proxy Server Use** area, change the **Primary Security Update Proxy used by Agents, Appliances, and Relays** setting to point to the new proxy.

4. If you are setting the security update proxy for a non-default relay group, perform the following:
   - In Deep Security Manager, select the **Administration > Updates > Relay Management** tab.
   - Select the target relay group. In the **Relay Group Properties** area, change the **Update Source Proxy** setting to point to the new proxy.
5. Click **Save**.
6. Restart the agents.

> **Note:**
> The proxy should not replace the TLS certificate used to communicate with the primary security update source, as this can cause the security update to fail.

## Connect to Deep Security Manager via proxy

Agents connect to their manager during agent activation and heartbeats. There are two ways to connect an agent to its manager via a proxy:

Connect an agent to the manager via a proxy using a deployment script

1. Make sure you are using Deep Security Agent 10.0 or later, as connections through a proxy are not suppored in earlier versions.
2. "Register a proxy in the manager" on page 1335.
3. In the top right of Deep Security Manager, click **Support** > **Deployment Scripts**.
4. From **Proxy to contact Deep Security Manager**, select a proxy.
5. Copy the script or save it.
6. Run the script on the computer. The script installs the agent and configures it to connect to the manager through the specified proxy.

---

Connect an agent to the manager via a proxy using dsa_control

On a Windows agent:

---

- Open a command prompt (`cmd.exe`) as Administrator and enter the following:

  ```
  cd C:\Program Files\Trend Micro\Deep Security Agent\
  ```

  ```
  dsa_control -u myUserName:MTPassw0rd
  ```

  ```
  dsa_control -x dsm_proxy://squid.example.com:443
  ```

On a Linux agent:

- Enter the following:

  ```
  /opt/ds_agent/dsa_control -u myUserName:MTPassw0rd
  ```

  ```
  /opt/ds_agent/dsa_control -x dsm_proxy://squid.example.com:443
  ```

Regardless of the agent platform:

- Make sure the proxy uses one of the "Supported proxy protocols" on page 1336.
- For details on `dsa_control` and its `-u` and `-x` options, see "dsa_control" on page 1565.
- Repeat these commands on each agent that needs to connect through a proxy to the manager.
- Run commands to update the agent's local configuration. No policy or configuration changes are made in the manager as a result of running these commands.

## Connect to Deep Security Relays via proxy

Agents connect to their relay to obtain software and security updates. There are two ways to connect an agent to a relay via a proxy:

Connect an agent to relays via a proxy using a deployment script

1. Make sure you are using Deep Security Agent 10.0 or later, as connections through a proxy are not suppored in earlier versions.
2. "Register a proxy in the manager" on page 1335
3. In the top right of Deep Security Manager, click **Support** > **Deployment Scripts**.
4. From **Proxy to contact Relay(s)**, select a proxy.
5. Copy the script or save it.

6. Run the script on the computer. The script installs the agent and configures it to connect to the relay through the specified proxy.

---

Connect an agent to relays via a proxy using dsa_control

On a Windows agent:

- Open a command prompt (cmd.exe) as Administrator and enter the following commands:

```
cd C:\Program Files\Trend Micro\Deep Security Agent\
```

```
dsa_control -w myUserName:MTPassw0rd
```

```
dsa_control -y relay_proxy://squid.example.com:443
```

On a Linux agent:

- Enter the following:

```
/opt/ds_agent/dsa_control -w myUserName:MTPassw0rd
```

```
/opt/ds_agent/dsa_control -y relay_proxy://squid.example.com:443
```

Regardless of the agent platform:

- Make sure the proxy uses one of the "Supported proxy protocols" on page 1336.
- For details on `dsa_control` and its `-w` and `-y` options, see "dsa_control" on page 1565.
- Repeat these commands on each agent that needs to connect through a proxy to the manager.
- Run commands to update the agent's local configuration. No policy or configuration changes are made in the manager as a result of running these commands.

---

## Connect to Deep Security Software Updates, CSSS, and more via proxy

You can connect your agents to the following Deep Security cloud-based servers and services via a proxy:

- Software Update server (also known as the Download Center)
- Certified Safe Software Service (CSSS), which is a feature of the Integrity Monitoring module
- Product Registration service
- Licensing service
- Deep Security Protected Product Usage Data Collection service (also known as the Telemetry service)

1. "Register a proxy in the manager" on page 1335.
2. In Deep Security Manager, click **Administration** at the top.
3. In the main pane, select the **Proxies** tab.
4. Next to **(Connection to Trend Micro services)**, select your proxy.
5. Click **Save**.
6. "Restart the Deep Security Manager" on page 1560 and all manager nodes so that the CSSS proxy settings take effect.

## Connect to cloud accounts via proxy

You can connect the manager to an AWS, Azure, or GCP cloud account via a proxy. For more on these accounts, see "About adding AWS accounts" on page 582, "Add a Microsoft Azure account to Deep Security" on page 602, and "Add a Google Cloud Platform account" on page 614.

1. "Register a proxy in the manager" on page 1335.
2. In Deep Security Manager, click **Administration** at the top.
3. In the main pane, select the **Proxies** tab.
4. Next to **Deep Security Manager (Cloud Accounts - HTTP Protocol Only)**, select your proxy.
5. Click **Save**.

## Connect to the Smart Protection Network via proxy

Use the following procedure to configure a proxy between agents and the following services in the Smart Protection Network - Global Census, Good File Reputation, Predictive Machine Learning, and the Smart Protection Network itself:

1. "Register a proxy in the manager" on page 1335.
2. In Deep Security Manager, click **Policies** at the top.
3. In the main pane, double-click the policy that you use to protect computers that are behind the proxy.

4. Set up a proxy to the Global Census, Good File Reputation, and Predictive Machine Learning Services as follows:
   a. Click **Settings** on the left.
   b. In the main pane, click the **General** tab.
   c. In the main pane, look for the **Network Setting for Census and Good File Reputation Service, and Predictive Machine Learning** section.
   d. If the **Inherited** check box is selected, the proxy settings are inherited from the parent policy. To change the settings for this policy or computer, clear the check box.
   e. Select **When accessing Global Server, use proxy** and in the list, select your proxy, or select **New** to specify another proxy.
   f. Save your settings.
5. Set up a proxy to the Smart Protection Network for use with Anti-Malware:
   a. Click **Anti-Malware** on the left.
   b. In the main pane, click the **Smart Protection** tab.
   c. Under **Smart Protection Server for File Reputation Service**, if the **Inherited** check box is selected, the proxy settings are inherited from the parent policy. To change the settings for this policy or computer, clear the check box.
   d. Select **Connect directly to Global Smart Protection Service**.
   e. Select **When accessing Global Smart Protection Service, use proxy** and in the list, select your proxy or select **New** to specify another proxy.
   f. Specify your proxy settings and click **OK**.
   g. Save your settings.
6. Set up a proxy to the Smart Protection Network for use with Web Reputation:
   a. Click **Web Reputation**  on the left.
   b. In the main pane, click the **Smart Protection** tab.
   c. Under **Smart Protection Server for Web Reputation Service**, set up your proxy, the same way you did under **Anti-Malware**  in a previous step.
   d. With **Web Reputation** still selected on the left, click the **Advanced** tab.
   e. In the **Ports** section, select a group of port numbers that includes your proxy's listening port number, and then click **Save**. For example, if you're using a Squid proxy server, you would select the **Port List Squid Web Server**. If you don't see an appropriate group of port numbers, go to **Policies** > **Common Objects** > **Lists** > **Port Lists** and then click **New**  to set up your ports.
   f. Save your settings.
7. Send the new policy to your agents. See "Send policy changes manually" on page 633.

Your agents now connect to the Smart Protection Network through a proxy.

## Connect to Workload Security via proxy

1. Register a proxy in the manager.
2. In Deep Security Manager, go to **Administration > Proxies**.
3. Next to **Trend Vision One Endpoint Security Link (HTTP Protocol Only)**, select your proxy.
4. Click **Save**.

## Remove a proxy

To remove a proxy between agent and manager, or agent and relay

- Redeploy agents using new deployment scripts that no longer contain proxy settings. For details, see "Use deployment scripts to add and protect computers" on page 1623.

  or

- Run the following `dsa_control` commands on the agents:

  ```
  dsa_control -x ""
  ```

  ```
  dsa_control -y ""
  ```

  These commands remove the proxy settings from the agent's local configuration. No policy or configuration changes are made in the manager as a result of running these commands.

  For details on `dsa_control` and its `-x` and `-y` options, see "dsa_control" on page 1565.

To remove a proxy between any other components

Run through the instructions on connecting through a proxy, but complete them in reverse, so that you remove the proxy.

# Proxy settings

You can configure proxies between various Trend Micro components. For details, see "Configure proxies" on page 1335.

## Use proxy server

To view and edit the list of available proxies, go to **Administration > System Settings > Proxies**. The following options are available:

- **Primary Security Update Proxy used by Agents, Appliances, and Relays** (see "Connect to the Primary Security Update Source via proxy" on page 1336)
- **Deep Security Manager (Connection to Trend Micro services)** (see "Connect to Deep Security Software Updates, CSSS, and more via proxy" on page 1339)
- **Deep Security Manager (Cloud Accounts - HTTP Protocol Only)** (see "Connect to cloud accounts via proxy" on page 1340)
- **Trend Vision One Endpoint Security Link (HTTP Protocol Only)** (see Connect to Workload Security via proxy)

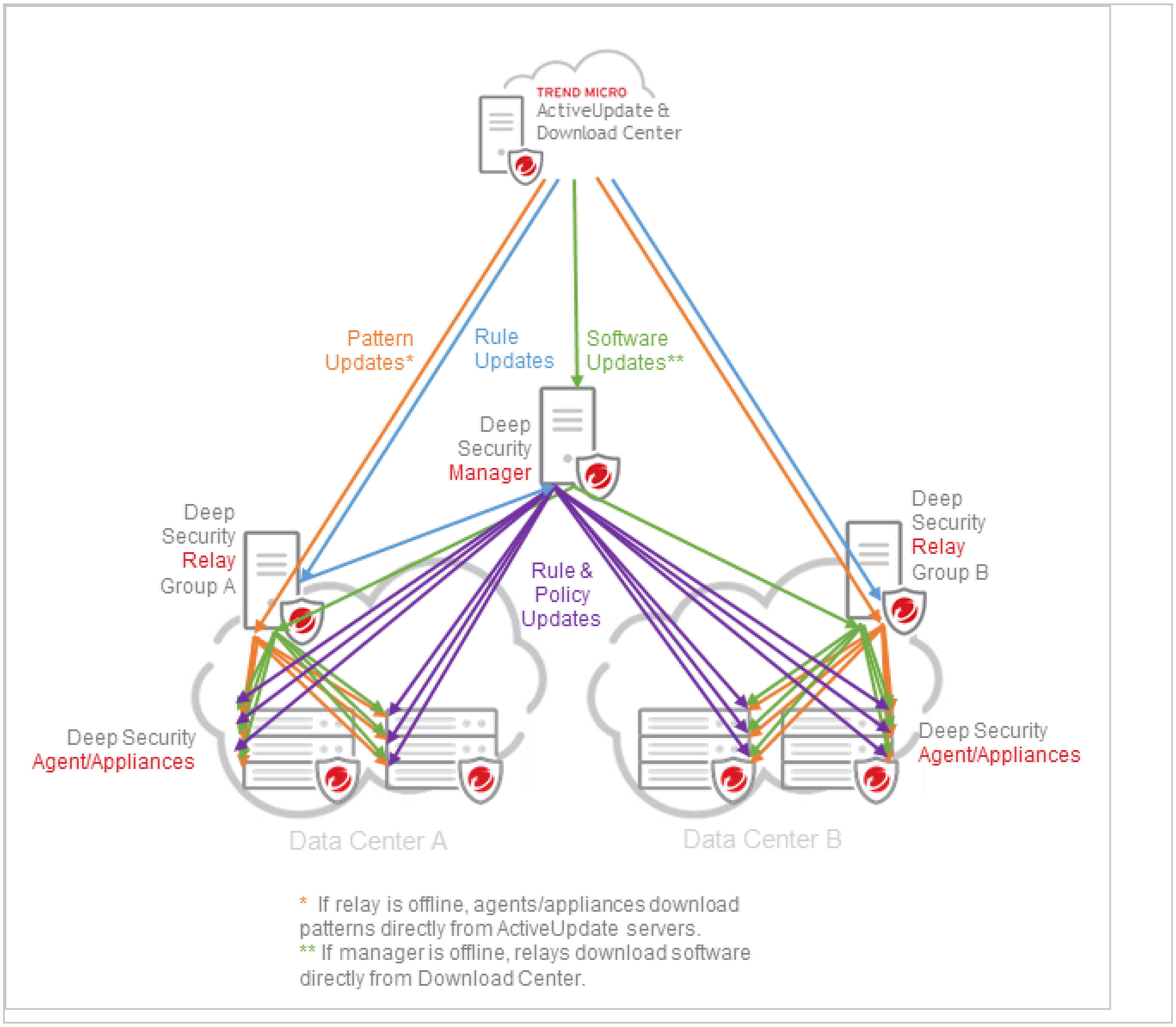
# Configure relays

## How relays work

Relays redistribute both software updates and security updates to your agents to help your deployment perform well at scale. (Alternatively, software updates – but not security updates – can be distributed by a local mirror web server.) Relays can:

- Reduce WAN bandwidth costs by reducing external update traffic
- Speed up update distribution in large scale deployments
- Provide update distribution redundancy

Update sources are different for relays and agents, depending on their parent relay group and the type of update.


TREND MICRO
ActiveUpdate & Download Center
Pattern Updates*
Rule Updates
Software Updates**
Deep Security Manager
Deep Security Relay Group A
Deep Security Relay Group B
Rule & Policy Updates
Deep Security Agent/Appliances
Deep Security Agent/Appliances
Data Center A
Data Center B
* If relay is offline, agents/appliances download patterns directly from ActiveUpdate servers.
** If manager is offline, relays download software directly from Download Center.

Agents get a randomly ordered list of relays for their assigned relay group. When an agent needs to download an update, they try the first relay. If there's no response, the agent tries the next in the list until it can successfully download the update. Because the list is random for each agent, this distributes update load evenly across relays in a group.

**Note:** If relays/agents can't connect to their the manager/relay, they will use their fallback update sources. For best performance, network connectivity between Deep Security components should be reliable.

Unlike other rule updates, Application Control rules are *not* downloaded from Trend Micro. However relays can similarly redistribute shared (not local) Application Control rulesets. See Deploy application control rulesets via relays.

## Relay hierarchy, cost, and performance

Relay groups can be organized in a hierarchy: one or more first-level ("parent") relay groups download updates *directly* from the manager and Primary Security Update Source (usually via their Internet/WAN connection), and then second-level ("child") relay groups download updates *indirectly* via the first-level group, and so on. If you put a child relay on each local network, then agent updates usually use the local network connection – not remote connections to the Internet. This saves external connection bandwidth (a typical performance bottleneck) and makes updates faster, especially for large deployments with many networks or data centers.

Performance and bandwidth usage can be affected by relay group hierarchy. Hierarchy can specify:

- **Update order** – Child relay sub-groups download from their parent group, which must finish its own download first. So a chain of sub-groups can be useful if you want a delay, so that all updates aren't at the exact same time.
- **Cost** – If large distances or regions are between your parent and child relay groups, it might be cheaper for them to download directly instead of via parent relay groups.
- **Speed** – If many or low-bandwidth subnets are between your parent and child relay groups, it might be faster for them to download directly or via a grandparent instead of via parent relay groups. However if too many relays do this, it will consume external connection bandwidth and eventually *decrease* speed.

Hierarchies are set up during relay group creation. For details, see "Create relay groups" on page 1350.

# Deploy additional relays

After deploying your first Deep Security Relay, you should deploy at least one more for redundancy and load-balancing reasons. You may even need to deploy more depending on the size and scope of your deployment.

When deploying relays, you need to do the following:

1. "Plan the best number and location of relays" on the next page
2. "Configure the update source" on page 1348

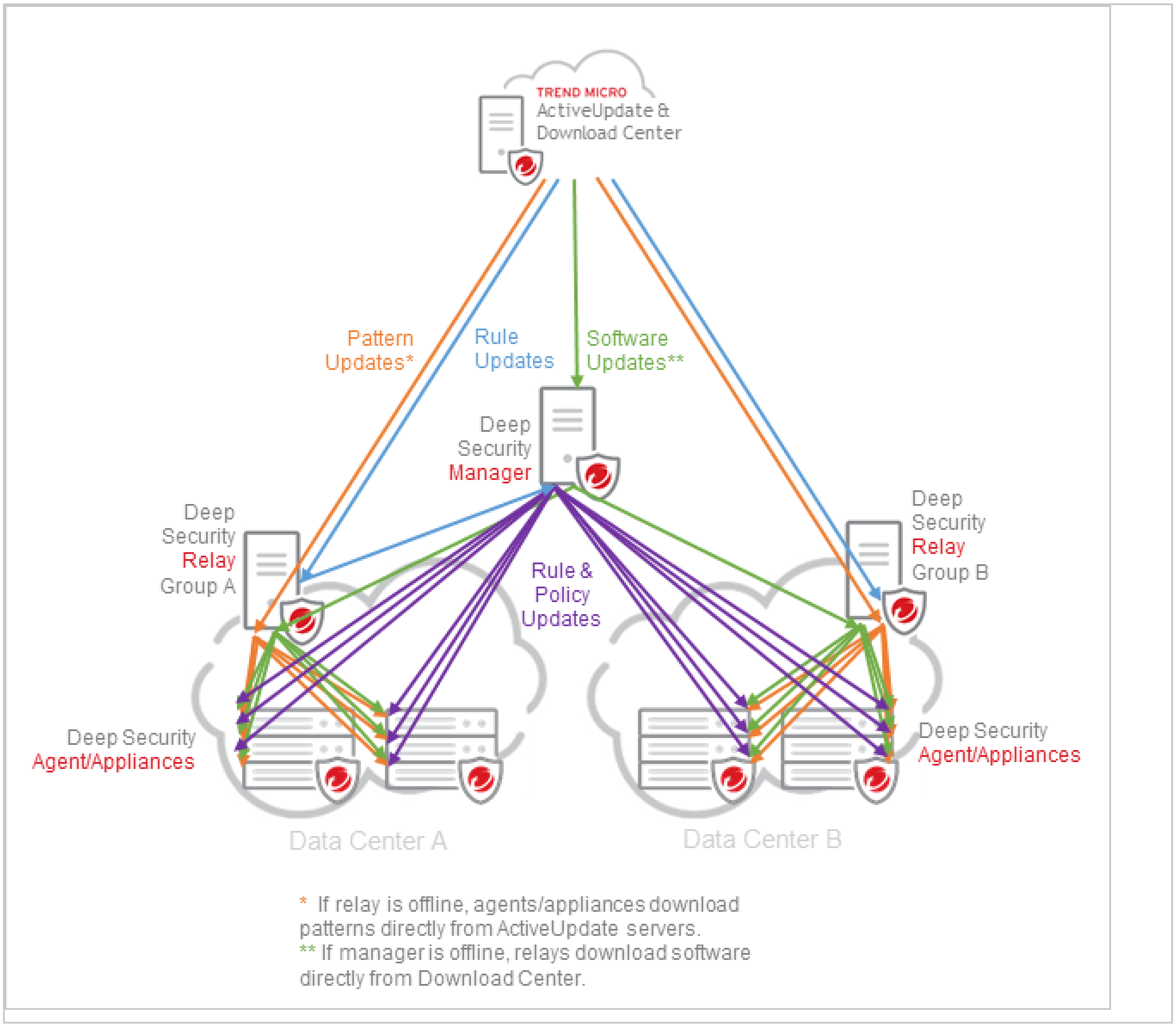
3. "Configure relays" on page 1350

**Warning:** Too many relays on your network decrease performance – not improve it. A relay requires more system resources than an ordinary agent. Extra relays might be competing for bandwidth, too, instead of minimizing external connections. If required, you can convert a relay back to a regular Deep Security Agent. For more information, see "Remove relay functionality from an agent" on page 1353.

## Plan the best number and location of relays

The optimal number and placement of relays depends on the following factors:

- "Geographic region and distance" on the next page
- "Network architecture and bandwidth limits" on the next page
- "Air-gapped environments" on page 1348


TREND MICRO
ActiveUpdate & Download Center
Pattern Updates*
Rule Updates
Software Updates**
Deep Security Manager
Deep Security Relay Group A
Deep Security Relay Group B
Rule & Policy Updates
Deep Security Agent/Appliances
Deep Security Agent/Appliances
Data Center A
Data Center B
* If relay is offline, agents/appliances download patterns directly from ActiveUpdate servers.
** If manager is offline, relays download software directly from Download Center.

### Geographic region and distance

Ideally, each geographic region should have its own relay group with at least two relays.

Agents should use local relays in the same geographic region. Long distance and network latency can slow down update redistribution. Downloading from other geographic regions can also increase network bandwidth and/or cloud costs.

### Network architecture and bandwidth limits

Ideally, each network segment of agents with limited bandwidth should have its own relay group with at least two relays.

Low bandwidth Internet/WAN connections, routers, firewalls, VPNs, VPCs, or proxy devices (which can all define a network segment) can be bottlenecks when large traffic volumes travel between the networks. Bottlenecks slow down update redistribution. Agents therefore usually should use local relays inside the same network segment – not relays outside on bottlenecked external networks.

For example, your relay group hierarchy could minimize Internet and internal network bandwidth usage. Only one parent relay group might use the Internet connection; subgroups would download from the parent, over their local network connection. Agents would download from their local relay group.

Large scale deployments might have many agents connect to each relay. This requires relays on more powerful, dedicated servers, as opposed to more relays on shared servers. For more information, see "Deep Security Agent sizing and resource consumption" on page 470.

#### Air-gapped environments

Most deployments can connect to the Internet. But if your relays cannot connect to the Trend Micro ActiveUpdate server on the Internet because they are on an isolated network (an "air-gapped" deployment), then you need to do the following:

1. Add a separate relay in a demilitarized zone (DMZ) (which can connect to the Internet) to get the security updates.
2. Copy updates from the DMZ relay to your other, air-gapped relays.

For details, see "Configure agents that have no internet access" on page 1379.

## Configure the update source

Before setting up relays, perform the following to define the source of updates and when to bypass the usual relay hierarchy to get updates:

1. Go to **Administration > System Settings > Updates**.

2. Optionally, configure **Primary Security Update Source** and **Secondary Source**.

   By default, the primary source is **Trend Micro Update Server** which is accessed via the Internet. Do not change the setting, unless your support provider has told you to configure **Other update source**. Alternative update source URLs must include "http://" or "https://".

3. Typically, agents connect to a relay to get security updates when Deep Security Manager tells them to. But if computers cannot always connect with the manager or relays (such as during scheduled maintenance times) *and* enough Internet/WAN bandwidth is available, you can select the following:

   - **Allow Agents/Appliances to download security updates directly from Primary Security Update Source if Relays are not accessible**
   - **Allow Agents/Appliances to download security updates when Deep Security Manager is not accessible**

   Tip: If you protect laptops and portable computers, they might sometimes be far from support services. To avoid risk of a potentially problematic security update while they travel, deselect these options.

4. If you require security updates for older agents, select **Allow supported 8.0 and 9.0 Agents to be updated**. By default, Deep Security Manager does not download updates for Deep Security Agent 9.0 and earlier because most of these agents are no longer supported. For details on which older agents are still supported, see "Deep Security LTS lifecycle dates" on page 107.
5. If you would like Deep Security Manager to auto-import agent update builds to your local inventory, select **Automatically download updates to imported software**.

   This setting imports the software to Deep Security Manager but does not automatically update your agent or appliance software. See "Upgrade Deep Security Agent" on page 1542 for more information.

6. Typically, relays connect to Deep Security Manager to get software updates to redistribute. However, if relays cannot always connect with the manager (such as during scheduled maintenance times or when there is an enterprise firewall between the manager and relays), you can select **Allow Relays to download software updates from Trend Micro Download Center when Deep Security Manager is not accessible**. Relays will get software updates directly from the Download Center instead.

   Tip: Hybrid cloud environments often have some agents and relays in a public cloud, while others (and the manager) are inside your private network. To avoid the risk of opening port numbers on your private network firewall, or manually copying software packages to your relays in the cloud, select this option.

7. Configure **Alternate software update distribution server(s) to replace Deep Security Relays** to specify an alternative source for software updates, noting that security updates

still need to come from a relay. Consider an alternative server if your relay has an elastic IP address, if you plan on configuring your relays to only receive security updates (not software updates), or if you want to host software on a web server for efficiency and availability reasons. Enter `https://<IP_or_hostname>:<port>/` replacing `<IP_or_hostname>:<port>` with one of the following:

- The private network IP address and port of the relay that has an elastic IP address.
- The web server and port where you plan to host the Deep Security software.

## Configure relays

After determining the location and the number relays, as well as what update sources they should use, you can do the following:

1. "Create relay groups" below
2. "Enable relays" on the next page
3. "Assign agents to a relay group" on page 1352
4. "Connect agents to a relay's private IP address" on page 1352

### Create relay groups

Relays must be organized into relay groups. The relay groups themselves can be further organized into hierarchies.

If you installed a co-located relay during the Deep Security Manager installation, then it automatically created a default relay group. But if you need more groups for other locations (see "Plan the best number and location of relays" on page 1346), you can create more.

1. Go to **Administration > Updates > Relay Management** to open the **Relay Group Properties** pane.
2. Click **New Relay Group**.
3. Type a **Name** for the relay group.
4. In **Update Source**, select either Primary Security Update Source or, in case of a subgroup, the name of the parent relay group.

   Note that the Default Relay Group is not included in the list of update sources, and therefore cannot be configured as a parent.

   Consider selecting the update source with the best cost and speed. Even if a relay group is part of a hierarchy, sometimes it might be cheaper and faster to download updates from the Primary Security Update Source instead, not the parent relay group.

5. If this relay group must use a proxy when connecting to the Primary Security Update Source, select **Update Source Proxy**. For details, see "Connect to the Primary Security Update Source via proxy" on page 1336.

   Unlike other relay groups, **Default Relay Group** uses **Primary Security Update Proxy used by Agents, Appliances, and Relays** setting available in the **Administration > System Settings > Proxies** tab.

   If this relay group usually connects to a parent relay group, then the subgroup does not use the proxy unless the parent relay group is unavailable and it is configured to fall back to using the Primary Security Update Source.

6. Under **Update Content**, select either **Security and software updates** or **Security updates only**. If you select **Security updates only**, you must configure an alternative software update source. For details, see "Configure the update source" on page 1348.

Tip: To minimize latency and external/Internet bandwidth usage, create a relay group for each geographic region and/or network segment.

## Enable relays

1. Make sure the relay computer meets the requirements. See "Deep Security Agent sizing and resource consumption" on page 470 and "Deep Security Relay requirements" on page 388.
2. Make sure you allow inbound and outbound communication to and from the relay on the appropriate port numbers. See "Deep Security port numbers" on page 478.
3. If the relay must connect through a proxy, see "Connect to the Primary Security Update Source via proxy" on page 1336.
4. Deploy an agent on the chosen computer. See "Get Deep Security Agent software" on page 520 and "Install the agent" on page 548.
5. Enable the agent as a relay:
   a. Log in to Deep Security Manager.
   b. Click **Administration** at the top.
   c. Click **Relay Management** in the left navigation pane.
   d. If you are using Linux, before enabling the relay, create a user **nobody** and a relay group **nogroup**.
   e. Select the relay group into which the relay will be placed. If a relay group does not exist, create one. If you are using Linux, create a user **nobody** and a relay group **nogroup**.
   f. Click **Add Relay**.
   g. In **Available Computers**, select the agent you just deployed.
   h. Click **Enable Relay and Add to Group**.

The agent is enabled as a relay and is displayed with a relay icon ().

**Tip:** To minimize latency and the Internet bandwidth usage, group together relays that are in the same geographic region and network segment.

**Tip:** You can use the search field to filter the list of computers.

## Assign agents to a relay group

You must indicate which relay group each agent should use. Either assign each agent to a relay group manually, or set up an event-based task to assign new agents automatically.

1. Go to **Computers**.
2. Right-click the computer and select **Actions > Assign Relay Group**.

   To assign multiple computers, Shift-click or Ctrl-click computers in the list, and then select **Actions > Assign Relay Group**.
3. Select the relay group that computer should use.

   To minimize latency and external/Internet bandwidth usage, assign agents to relays that are in the same geographic region and/or network segment.

## Connect agents to a relay's private IP address

If your relay has an elastic IP address, agents within an AWS VPC may not be able to reach the relay via that IP address. Instead, they must use the private IP address of the relay group.

1. Go to **Administration** > **System Settings**.
2. In the **System Settings** area, click the **Updates** tab.
3. Under **Software Updates**, in the window **Alternate software update distribution server(s) to replace Deep Security Relays** , type:

   ```
   https://<IP>:<port>/
   ```

   where `<IP>` is the private network IP address of the relay, and `<port>` is the relay port number
4. Click **Add**.
5. Click **Save**.

If your relay group’s private IP changes, you must manually update this setting, as it does not update automatically.

## Remove relay functionality from an agent

You might want to convert a relay back to being an ordinary Deep Security Agent if:

- Too many relays are causing communication delays
- Relays don't meet minimum system requirements to be a Deep Security Relay anymore

1. Go to **Administration > Updates > Relay Management**.
2. Click the arrow next to the relay group whose relay you want to convert back to an agent.
3. Click the computer.
4. Click **Remove Relay**.

   The agent status will change to "Disabling" and the relay functionality will be removed from the agent.

   It can take up to 15 minutes. If the agent is in the "Disabling" state for longer than this, you can deactivate and reactivate the agent to finish removing the relay feature.

# Manage agents (protected computers)

## Computer and agent statuses

On the **Computers** page in Deep Security Manager:

- The **Status** column displays the state of the computer's network connectivity and the state (in parentheses) of the agent providing protection, if present. The status column might also display system or agent events. See "Status column - computer states" on the next page and "Status column - agent or appliance states" on the next page
- The **Task(s)** column displays the state of the tasks. See "Task(s) column" on page 1355.

For a list of the events, see "Agent events" on page 1227 and "System events" on page 1233.

Also on this page:

- "Computer errors" on page 1359
- "Protection module status" on page 1360
- "Perform other actions on your computers" on page 1361

- "Computers icons" on page 1365
- "Status information for different types of computers" on page 1366

## Status column - computer states

| State | Description |
|---|---|
| Activated | The agent is activated. See "Perform other actions on your computers" on page 1361. |
| Discovered | Computer has been added to the computers list via the discovery process. (See "Discover computers" on page 575.) |
| Managed | An agent is present and activated, with no pending operations or errors. |
| Multiple Errors | Multiple errors have occurred on this computer. See the computer's system events for details. |
| Multiple Warnings | Multiple warnings are in effect on this computer. See the computer's system events for details. |
| Reactivation Required | The agent is installed and listening and is waiting to be reactivated a Deep Security Manager. |
| Unmanaged | The computer's agent is not managed by this Deep Security Manager because it hasn't been activated. Deep Security Manager can't communicate with the agent until you activate it. |
| Upgrade Recommended | A newer version of the agent or appliance is available. An software upgrade is recommended. |
| Upgrading Agent | The agent software on this computer is in the process of being upgraded to a newer version. |

## Status column - agent or appliance states

| State | Description |
|---|---|
| Activated | The agent has been successfully activated and is ready to be managed by the Deep Security Manager. |
| Activation Required | An unactivated agent has been detected on the target machine. It must be activated before it can be managed by the Deep Security Manager. |
| Deactivation Required | The manager has attempted to activate an agent that has already been activated by another Deep Security Manager. The original Deep Security Manager must deactivate the agent before it can be activated by the new manager. |
| No Agent | No agent was detected on the computer. |
| Offline | The agent has not connected to the manager for the number of heartbeats specified on **Computer or Policy editor**[1] **> Settings > General**. |

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

| State | Description |
|---|---|
| | This can occur when connectivity is interrupted by a network firewall or proxy, AWS security group, agent software update, or when a computer is powered down for repair.<br>Verify that firewall settings allow the required port numbers, and that the computer is powered on. |
| Online | The agent is online and operating as expected. |
| Unknown | No attempt has been made to determine whether an agent is present. |

## Task(s) column

| State | Description |
|---|---|
| Activating | The manager is activating the agent. |
| Activating (Delayed) | The activation of the agent is delayed by the amount of time specified in the relevant event-based task. |
| Activation Pending | A command to activate the agent has been queued. |
| Agent Software Deployment Pending | An instruction to deploy the agent software is queued to be sent to the computer. |
| Agent Software Removal Pending | An instruction to remove the agent software is queued to be sent to the computer. |
| Application Control Inventory Scan In Progress | An application control inventory scan is being performed. |
| Application Control Inventory Scan Pending (Heatbeat) | An instruction to start an application control inventory scan will be sent from the manager during the next heartbeat. |
| Application Control Inventory Scan Pending (Offline) | The agent is currently offline. The manager will initiate an application control inventory scan when communication is reestablished. |
| Application Control Ruleset Update In Progress | The application control ruleset is being updated. |
| Application Control Ruleset Update Pending (Heartbeat) | An instruction to perform an application control ruleset update will be sent from the manager during the next heartbeat. |
| Application Control Ruleset Update Pending (Offline) | The agent is currently offline. The manager will initiate an application control ruleset update when communication is reestablished. |
| Baseline Rebuild In Progress | The Integrity Monitoring engine is currently rebuilding a system baseline. |
| Baseline Rebuild | A baseline rebuild has been paused |

| State | Description |
|---|---|
| Paused | |
| Baseline Rebuild Pending | An instruction to rebuild a system baseline for Integrity Monitoring is queued to be sent. |
| Baseline Rebuild Pending (Offline) | The agent is currently offline. The Integrity Monitoring engine will rebuild a system baseline when communication between the manager and this computer is reestablished. |
| Baseline Rebuild Queued | The instruction to perform a baseline rebuild is queued. |
| Checking Status | The agent state is being checked. |
| Deactivate Pending (Heartbeat) | A deactivate instruction will be sent from the manager during the next heartbeat. |
| Deactivating | The manager is deactivating the agent. This means that the agent is available for activation and management by another Deep Security Manager. |
| Deploying Agent Software | Agent software is being deployed on the computer. |
| File Backup Cancellation In Progress | A file backup is being canceled. |
| File Backup Cancellation Pending | An instruction to cancel a file backup is queued to be sent. |
| File Backup Cancellation Pending (Offline) | The agent or appliance is currently offline. The manager will initiate the cancellation of the file backup when communication is reestablished. |
| File Backup In Progress | A file backup is being performed. |
| File Backup Pending | An instruction to start a file backup is queued to be sent. |
| File Backup Pending (Offline) | The agent or appliance is currently offline. The manager will initiate a file backup when communication is reestablished. |
| File Backup Queued | The instruction to perform a file backup is queued. |
| Getting Events | The manager is retrieving events from the agent. |
| Integrity Scan In Progress | An Integrity Scan is currently in progress. |
| Integrity Scan Paused | An integrity scan has been paused. |
| Integrity Scan Pending | A command to start an integrity scan is queued to be sent. |
| Integrity Scan Pending (Offline) | The agent is currently offline. The manager will initiate an Integrity Scan when communication is reestablished. |
| Integrity Scan Queued | An instruction to start an integrity scan is queued to be sent. |
| Malware Manual Scan Cancellation | The instruction to cancel a manually-initiated Malware Scan has been sent. |

| State | Description |
|---|---|
| In Progress | |
| Malware Manual Scan Cancellation Pending | The command to cancel a manually-initiated malware scan is queued to be sent. |
| Malware Manual Scan Cancellation Pending (Offline) | The appliance is offline. The instruction to cancel a manually-initiated Malware Scan will be sent when communication is reestablished. |
| Malware Manual Scan In Progress | A manually-initiated Malware Scan is in progress. |
| Malware Manual Scan Paused | A manually-initiated Malware Scan has been paused. |
| Malware Manual Scan Pending | The instruction to perform a manually-initiated Malware Scan has not yet been sent. |
| Malware Manual Scan Pending (Offline) | The agent is offline. The instruction to start a manually-initiated Malware Scan will be sent when communication is reestablished. |
| Malware Manual Scan Queued | The instruction to perform a manually-initiated Malware Scan is queued. |
| Malware Scheduled Scan Cancellation In Progress | The instruction to cancel a scheduled Malware Scan has been sent. |
| Malware Scheduled Scan Cancellation Pending | The instruction to cancel a scheduled Malware Scan is queued to be sent. |
| Malware Scheduled Scan Cancellation Pending (Offline) | The agent is offline. The instruction to cancel a scheduled Malware Scan will be sent when communication is reestablished. |
| Malware Scheduled Scan In Progress | A scheduled Malware Scan is in progress. |
| Malware Scheduled Scan Paused | A scheduled Malware Scan has been paused. |
| Malware Scheduled Scan Pending | The command to cancel a scheduled malware scan has not yet been sent. |
| Malware Scheduled Scan Pending (Offline) | The agent is offline. The instruction to start a scheduled Malware Scan will be sent when communication is reestablished. |
| Malware Scheduled Scan Queued | The instruction to cancel a scheduled Malware Scan is queued. |
| Quick Malware Scan Cancellation In Progress | A quick malware scan is being canceled. |
| Quick Malware Scan Cancellation Pending | An instruction to cancel a quick malware scan is queued to be sent. |
| Quick Malware Scan Cancellation | The agent is currently offline. The manager will initiate the cancellation of a quick malware scan when communication is reestablished. |

| State | Description |
|---|---|
| Pending (Offline) | |
| Quick Malware Scan In Progress | A quick malware scan is being performed. |
| Quick Malware Scan Paused | A quick malware scan has been paused. |
| Quick Malware Scan Pending | An instruction to start a quick malware scan is queued to be sent. |
| Quick Malware Scan Pending (Offline) | The agent is currently offline. The manager will initiate a quick malware scan when communication is reestablished. |
| Quick Malware Scan Queued | The instruction to perform a quick malware scan is queued. |
| Removing Agent Software | The agent software is being removed from the computer. |
| Rollback of Security Update In Progress | A security update is being rolled back. |
| Rollback of Security Update Pending | An instruction to roll back a security update is queued to be sent. |
| Rollback of Security Update Pending (Heartbeat) | An instruction to roll back a security update will be sent from the manager during the next heartbeat. |
| Rollback of Security Update Pending (Offline) | The agent is currently offline. The manager will initiate a rollback of the security update when communication is reestablished. |
| Scan for Recommendations Pending (Heartbeat) | The manager will initiate a recommendation scan at the next heartbeat. |
| Scan for Recommendations Pending (Offline) | The agent is currently offline. The manager will initiate a recommendation scan when communication is reestablished. |
| Scanning for Open Ports | The manager is scanning the computer for open ports. |
| Scanning for Recommendations | A recommendation scan is underway. |
| Security Update In Progress | A security update is being performed. |
| Security Update Pending | An instruction to perform a security update is queued to be sent. |
| Security Update Pending (Heartbeat) | An instruction to perform a security update will be sent from the manager during the next heartbeat. |
| Security Update Pending (Offline) | The agent is currently offline. The manager will initiate a security update when communication is reestablished. |
| Sending Policy | A policy is being sent to the computer. |
| Update of | An instruction to update the configuration to match the policy changes will |

| State | Description |
|---|---|
| Configuration Pending (Heartbeat) | be sent from the manager during the next heartbeat. |
| Update of Configuration Pending (Offline) | The agent is currently offline. The manager will initiate the configuration update to match the policy changes when communication is reestablished. |
| Upgrading Software (In Progress) | A software upgrade is being performed. |
| Upgrading Software (Install Program Sent) | A software upgrade is being performed. The install program has been sent to the computer. |
| Upgrading Software (Pending) | An instruction to perform a software upgrade is queued to be sent. |
| Upgrading Software (Reboot to Complete Upgrade) | A software upgrade has been requested but will not be complete until the agent computer is rebooted. When the computer is in this state, it is still being protected by the older version of the Deep Security Agent. |
| Upgrading Software (Results Received) | A software upgrade is being performed. The results have been received. |
| Upgrading Software (Schedule) | A software upgrade will be performed once the computer's access schedule permits. |

## Computer errors

| State | Description |
|---|---|
| Communication error | General network error. |
| No route to computer | Typically the computer cannot be reached because of a firewall between the manager and computer, or if a router between them is down. |
| Unable to resolve hostname | Unresolved socket address. |
| Activation required | An instruction was sent to the agent when it was not yet activated. |
| Unable to communicate with Agent | Unable to communicate with agent. |
| Protocol Error | Communication failure at the IP, TCP, or HTTP layer.<br>For example, if the Deep Security Manager IP address is unreachable because the connection is being blocked by a firewall, router, or AWS security group, then it would cause a connection to fail. To resolve the error, verify that the activation port number is allowed and that a route exists. |
| Deactivation | The agent is currently activated by another Deep Security Manager. |

| State | Description |
|---|---|
| Required | |
| No Agent | No agent was detected on the target. |
| No valid software version | Indicates that no installer can be found for the platform and version requested. |
| Send software failed | There was an error in sending a binary package to the computer. |
| Internal error | Internal error. Please contact your support provider. |
| Duplicate Computer | Two computers in the Deep Security Manager's computers list share the same IP address. |
| Unresolved software change limit reached | Software changes detected on the file system exceeded the maximum amount. Application control will continue to enforce existing rules, but will not record any more changes, and it will stop displaying any of that computer's software changes.<br>See "Reset Application Control after too much software change" on page 1039. |

## Protection module status

When you hover over a computer name on the **Computers** page, the **Preview** icon (▤) is displayed. Click the icon to display the state of the computer's protection modules.

**On and Off States**:

| State | Description |
|---|---|
| On | Module is configured in Deep Security Manager and is installed and operating on the Deep Security Agent. |
| Off | Module is either not configured in Deep Security Manager, not installed and operating on the Deep Security Agent, or both. |
| Unknown | Indicates an error with the protection modules. |

**Install state**:

| State | Description |
|---|---|
| Not Installed | The software package containing the module has been downloaded in Deep Security Manager, but the module has not been turned on in Deep Security Manager or installed on the agent. |
| Installation Pending | Module is configured in the manager but is not installed on the agent. |
| Installation in Progress | Module is being installed on the agent. |

| State | Description |
|---|---|
| Installed | Module is installed on the agent. This state is only displayed when the state of the module is "Off". (If the state is "On", the module has been installed on the agent.) |
| Matching Module Plug-In Not Found | The version of the software package containing the module imported into the manager does not match the version reported by the agent. |
| Not Supported/Update Not Supported | A matching software package was found on the agent, but it does not contain a module supported by the platform. "Not Supported" or "Update Not Supported" is displayed depending on whether there is already a version of this module installed on the agent. |

## Perform other actions on your computers

On the **Computers** page, the **Actions** button provides several actions that you can perform on the selected computers.

| Action | Description |
|---|---|
| Check Status | Checks the status of a computer without performing a scan or activation attempt. |
| Activate/Reactivate | Activates or reactivates the agent on the computer. See "Activate the agent" on page 566 |
| Deactivate | You may want to transfer control of a computer from one Deep Security Manager installation to another. If so, the agent has to be deactivated and then activated again by the new manager. |
| Assign Policy | Opens a window with a list that allows you to assign a policy to the computer. The name of the policy assigned to the computer will appear in the **Policy** column on the **Computers** page.<br>**Note:** If you apply other settings to a computer (for example, adding additional Firewall Rules, or modifying Firewall Stateful Configuration settings), the name of the policy will be in bold, indicating that the default settings have been changed. |
| Send Policy | When you use Deep Security Manager to change the configuration of an agent or appliance on a computer (apply a new intrusion prevention rule, change logging settings, etc.), the Deep Security |

| Action | Description |
|---|---|
| | Manager has to send the new information to the agent or appliance. This is a Send Policy instruction. Policy updates usually happen immediately but you can force an update by clicking **Send Policy**. |
| Download Security Update | Downloads the latest security update from the configured relay to the agent or appliance. See "Apply security updates" on page 1533. |
| Rollback Security Update | Rolls back the latest security update for the agent or appliance. |
| Get Events | Override the normal event retrieval schedule (usually every heartbeat) and retrieve the event logs from the computer(s) now. |
| Clear Warnings/Errors | Use this command to clear all warnings and errors for the computer. This command is useful in these situations:<br>• If the agent for the computer has been reset locally<br>• If the computer has been removed from the network before you had a chance to deactivate or delete it from the list of computers |
| Upgrade Agent Software | To upgrade an agent, you first need to import a newer version of the agent software package into the Deep Security Manager (see "About upgrades" on page 1529). |
| Scan for Recommendations | Deep Security Manager can scan computers and then make recommendations for Security Rules. The results of a recommendation scan appear in the computer's **Details** window in the **Rules** pages. See "Manage and run recommendation scans" on page 639. |
| Clear Recommendations | Clears rule recommendations resulting from a recommendation scan on this computer. Clearing also removes the computer from those listed in an alert produced as a result of a recommendation scan.<br>**Note:** This action will not un-assign any rules that were assigned |

| Action | Description |
|---|---|
| | because of past recommendations. |
| Full Scan for Malware | Performs a full malware scan on the selected computers. The actions taken by a full scan depend on the **Malware Manual Scan Configuration** in effect on this computer. See "Configure malware scans and exclusions" on page 745. |
| Quick Scan for Malware | Scans critical system areas for currently active threats. Quick Scan looks for currently-active malware but does not perform deep file scans to look for dormant or stored infected files. On larger drives, Quick Scan is significantly faster than a Full Scan.<br>**Note:** Quick Scan is only available on-demand. You cannot schedule a Quick Scan as part of a scheduled task. |
| Scan for Open Ports | Performs a port scan on all selected computers and checks the agent installed on the computer to determine whether its state is either Deactivation Required, Activation Required, Agent Reactivate Required, or Online. The scan operation, by default, scans ports 1-1024. This range can be changed in **Computer or Policy editor**[1] **> Settings > General**.<br>**Note:** The agent's listening port number for heartbeats is always scanned regardless of port range settings. When the Manager connects to communicate with the agent, it uses that port number. If communication direction is set to "Agent/Appliance Initiated" for a computer (**Computer or Policy editor**[2] **> Settings > General > Communication Direction**), however, that port number will not be open. For a list of ports used, see "Deep Security port numbers" |

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

| Action | Description |
|---|---|
| | on page 478.<br>Note:<br>N |

| Action | Description |
|---|---|
| | ew computers on the network will not be detected. To find new computers, use the **Discover** tool. |
| Cancel Currently Executing Port Scans | If you have initiated a set of port scans to a large number of computers or over a large range of ports and the scan is taking too long, use the **Cancel Currently Executing Port Scans** option to cancel the scans. |
| Scan for integrity | Integrity Monitoring tracks changes to a computer's system and files. It does by creating a baseline and then performing periodic scans to compare the current state of the computer to the baseline. For more information see "Set up Integrity Monitoring" on page 901. |
| Rebuild Integrity Baseline | Rebuilds a baseline for Integrity Monitoring on this computer. |
| Assign Asset Value | Asset values allow you to sort computers and events by importance. The various security rules have a severity value. When rules are triggered on a computer, the severity values of the rules are multiplied by the asset value of the computer. This value is used to rank events in order of importance. See "Rank events to quantify their importance" on page 1065. |
| Assign a Relay Group | To select a relay group for this computer to download updates from, right-click the computer and choose **Actions > Assign a Relay Group**. |

## Computers icons

Ordinary computer

Deep Security Relay (a computer with a Relay-enabled Agent)

Docker host (physical computer)

Azure virtual machine with Docker

Amazon EC2 with Docker

Amazon WorkSpace (started)

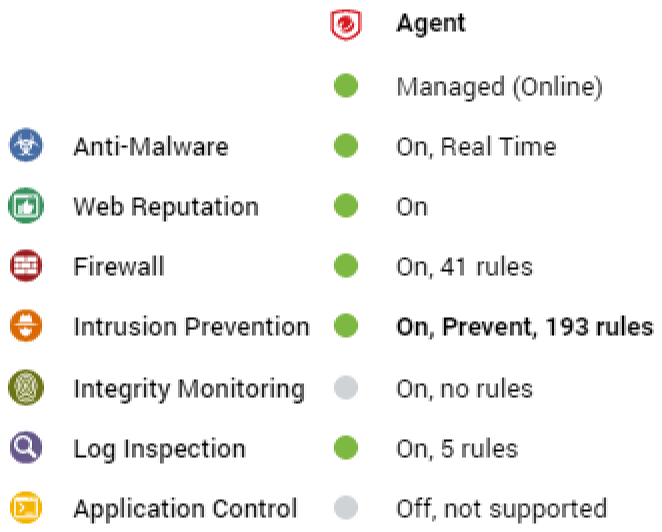
## Status information for different types of computers

The circular icon indicates the overall status for the agent or the module:

- Green: No issues
- Yellow: An issue has been found
- Red: A critical issue has been found
- Gray: Unable to find or to check for issues. It may be that a module has been turned off, or that even though the module has been turned on, there are no rules associated with the module and the module can therefore not report any result.

### Ordinary computer

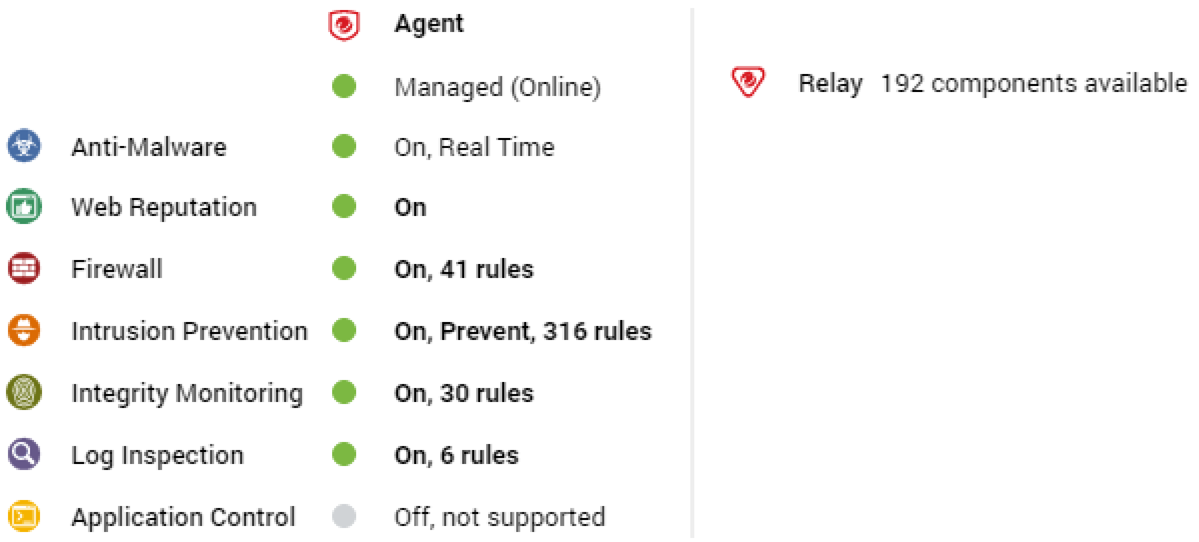
The preview pane for an ordinary computer displays the presence of an agent, it status, and the status of the protection modules.



| | | |
|---|---|---|
| | | **Agent** |
| | ● | Managed (Online) |
| Anti-Malware | ● | On, Real Time |
| Web Reputation | ● | On |
| Firewall | ● | On, 41 rules |
| Intrusion Prevention | ● | **On, Prevent, 193 rules** |
| Integrity Monitoring | ○ | On, no rules |
| Log Inspection | ● | On, 5 rules |
| Application Control | ○ | Off, not supported |

### Relay

The preview pane for a Deep Security relay-enabled agent displays its status, the number of security update components it has available for distribution, and the status of the protection modules provided by its embedded Deep Security agent.

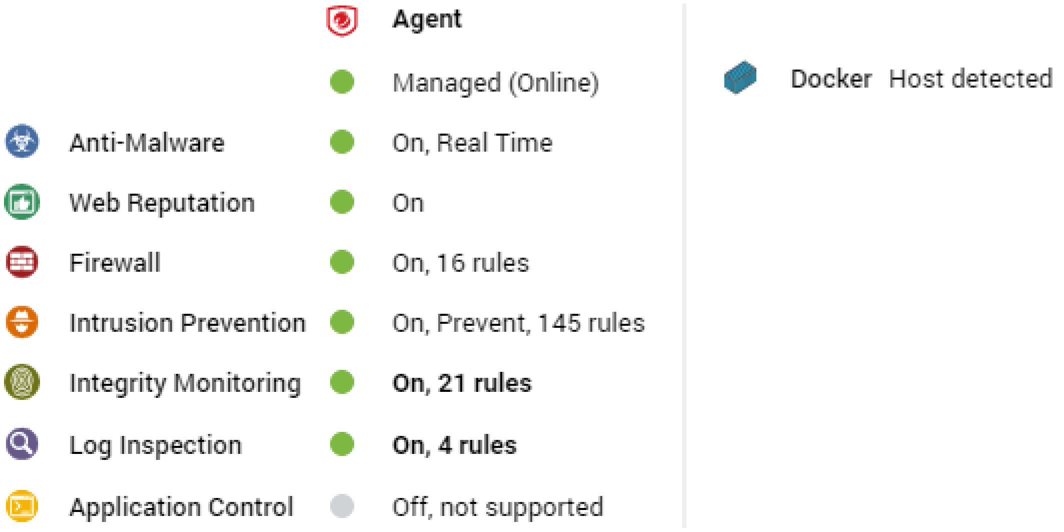


| | | |
|---|---|---|
| | | **Agent** |
| | ● | Managed (Online) |
| Anti-Malware | ● | On, Real Time |
| Web Reputation | ● | **On** |
| Firewall | ● | **On, 41 rules** |
| Intrusion Prevention | ● | **On, Prevent, 316 rules** |
| Integrity Monitoring | ● | **On, 30 rules** |
| Log Inspection | ● | **On, 6 rules** |
| Application Control | ○ | Off, not supported |

**Relay** 192 components available

## Docker, Podman, and CRI-O hosts

The preview pane for a host displays the presence of an agent and its status, the status of the protection modules, and the host status.



| | | |
|---|---|---|
| | | **Agent** |
| | ● | Managed (Online) |
| Anti-Malware | ● | On, Real Time |
| Web Reputation | ● | On |
| Firewall | ● | On, 16 rules |
| Intrusion Prevention | ● | On, Prevent, 145 rules |
| Integrity Monitoring | ● | **On, 21 rules** |
| Log Inspection | ● | **On, 4 rules** |
| Application Control | ○ | Off, not supported |

**Docker** Host detected

# Configure agent version control

Agent version control is a feature that gives you and your security operations team control over the specific versions of the Deep Security Agent that will be deployed when:

- using deployment scripts
- upgrading the agent through an upgrade alert, button, check box or other widget in the manager (the exceptions are listed in the FAQ)
- upgrading the agent through the agent upgrade on activation feature

This allows security operations teams who do not have control over Deep Security Manager's local inventory of agents or the relays the ability to declare exactly what agents will be used at any given time.

As new agents are released by Trend Micro, your security operations team can test them in controlled environments before changing the version control settings to expose the new agents to downstream applications teams in their production environment.

Topics:

## Set up agent version control

1. Before you begin, import the agent versions you want to use.
2. Go to Deep Security Manager.
3. Click **Administration** at the top.
4. On the left, expand **Updates > Software > Agent Version Control**.

   All the agent platforms appear in the main pane.

5. (Optional) Use the **Show/Hide Platforms** section on the right to restrict the agent platforms that are visible.
6. Make your agent version selections and click **Save**. Follow this guidance:

   **Note:** Only agent versions 9.0 or later are displayed. For Solaris specifically, only versions 11.0 or later are displayed. If you want to deploy earlier agents, you'll have to use the `agentVersion=` setting available in the deployment scripts. For details, see "Use deployment scripts to add and protect computers" on page 1623.

| Column | Description |
|---|---|
| PLATFORM | This column lists the platforms for which Deep Security |

| Column | Description |
|---|---|
| | Agent software is available. |
| VERSION CONTROL | This column is where you select which version of the agent will be used by deployment scripts and so on. It has the following options:<br>• **Latest**: Indicates to use the latest agent software build available in your local inventory, either long-term support (LTS) or feature release (FR). The logic to determine the latest agent is based on the agent version number: the highest version is used. For example, a Deep Security 12 update agent with version 12.0.0.460 is higher than the Deep Security 12 General Availability (GA) agent. However, the Deep Security 12 feature release agents with version 12.5.0.350 is considered later than an LTS agent with version 12.0.0.460. In summary, choose **Latest** if you want the latest LTS or FR agent for the platform. For details on LTS and FR releases, see "Deep Security 20 release strategy and lifecycle policy" on page 101.<br>• **Latest LTS**: (default) Indicates to use the latest long-term support (LTS) software build available in your local inventory. Latest LTS can be the original LTS release, or can be an update to the original LTS release. Any FRs in your inventory are ignored. LTS build versions always have ‘0’ as the minor version number. For details on LTS and FR releases, see "Deep Security 20 release strategy and lifecycle policy" on page 101.<br>• *<agent_version>* for example, `11.0.0.760`: Indicates to use a specific agent version available in your local inventory. Other agents in your inventory are ignored. If no agent version appears in the list, it's because there is no agent in your local inventory that matches the OS. To fix this issue, import an agent to your inventory. |

| Column | Description |
|---|---|
| | **Note:** The latest version of the agent is sometimes a few releases behind your manager version. For example, the latest LTS for Windows Server 2003 is `10.0.0.3377` as of this writing. Although a release may be behind your manager's, it is still supported if you can see it on the Agent Version Control page. For details, see "Agent platform support policy" on page 106. |
| RESULTING AGENT | This column shows the agent that will be deployed based on your selection under **VERSION CONTROL**.<br>If the column shows an **N/A (No agent in inventory)** message, it's because there is no agent in your local inventory that matches the selection in VERSION CONTROL. To fix this issue, import an agent to your inventory or change the VERSION CONTROL selection. |

## Use agent version control with URL requests

Agent version control provides the ability to control what agents are returned when any URL request is made to Deep Security Manager to download the agent. For details, see "Using agent version control to define which agent version is returned" on page 1633.

## Agent version control FAQs

How does version control interact with agent import?

> Prior to the introduction of agent version control, the primary way to control the agent version was to selectively import only those agents that you were confident you wanted to deploy. Once the agents were imported, the latest one for each platform was distributed to relays. The latest agents were then picked up from the relays by features like upgrade on activation and deployment scripts.

If you want to continue on this functionality (pre-12 functionality):

1. As before, import the agents you want to deploy to your inventory, and remove the old ones. See "Get Deep Security Agent software" on page 520 for details.
2. Go to the **Agent Version Control** page and make sure all platforms are set to the default, **Latest**. For instructions, see "Set up agent version control" on page 1368.

   The **Latest** setting instructs the manager to continue using the latest agents in its local inventory, and you can continue to use your existing processes without any changes.

Is version control supported in multi-tenant deployments?

Yes.

You, as the primary tenant (t0), must import newer agent versions into your local inventory, and then allow each of your tenants to make decisions about what agents they want to deploy using the **Agent Version Control** page. If a tenant only wants to use LTS agents, or lock in to a specific agent version, they can do so independent of other tenants.

Do I need to update my deployment scripts to use this feature?

Yes.

To update your deployment scripts:

1. In Deep Security Manager 12 or later, go to **Support > Deployment Scripts** and generate new deployment scripts. For instructions, see "Use deployment scripts to add and protect computers" on page 1623.
2. Re-distribute and re-run the new scripts as necessary.

The latest deployment scripts pass additional information to Deep Security Manager (for example, tenant information and platform information) that is required for the version control feature to work properly.

What happens if I don't update existing deployment scripts?

If you have existing deployment scripts that you generated prior to the availability of the agent version control feature, and you do not take any action to update them, they will default to **Latest**. This default will be used for any older deployment scripts regardless of how you have set your agent version control settings. Replace the older deployment scripts with new deployment scripts to leverage the settings you define in the agent version control settings.

Deployment scripts that are generated after the availability of the agent version control feature will use your agent version control settings.

What features are out of scope (exceptions)?

By design, the features listed below are out of scope for the agent version control feature. These features are typically accessed by the Deep Security Manager administrator directly, in many cases to test a specific agent version in a development or staging environment prior to deploying the agent version into production.

We have left full access to all agent versions accessible in these specific scenarios:

- the **Computer** details page > **Upgrade Agent** button
- the **Computers > Actions > Upgrade Agent Software** page

  Selecting either of the above options launches a wizard with a drop-down list that always defaults to 'Use latest version for platform' regardless of your version control settings. For details, see "Upgrade the agent from the Computers page" on page 1544.

- agent upgrades that are not initiated directly from Deep Security Manager. For example, if you export an agent package, transfer it to the server, and initiate the upgrade from the command line, the agent version control settings will not be involved in this upgrade.

# Configure teamed NICs

"Teamed NICs" or "link aggregation" describes forming a network link on a computer by using multiple network interface cards (NICs) together. This is useful to increase the total network bandwidth, or to provide link redundancy.

You can configure teamed NICs on Windows or Solaris so that they are compatible with Deep Security Agent.

## Windows

On Windows, when you team NICs, it creates a new virtual interface. This virtual interface adopts the MAC address of its first teamed physical interface.

By default, during installation or upgrade, the Windows Agent will bind to *all* virtual and physical interfaces. This includes the virtual interface created by NIC teaming. However, Deep Security Agent doesn't function properly if multiple interfaces have the same MAC address, which happens with NIC teaming on Windows

To avoid that, bind the agent *only* to the teamed virtual interface - *not* the physical interfaces.

**Note:** NIC teaming with Deep Security Agent requires Windows 2003 requires SP 2 or later.

**Warning:** Don't add or remove network interfaces from a teamed NIC *except* immediately before running the installer. Otherwise network connectivity may fail or the computer may not be correctly detected with Deep Security Manager. The agent's network driver is bound to network interfaces when you install or upgrade; the agent does not continuously monitor for changes after.

## Solaris

IPMP failover (active-standby) mode in Solaris allows two NICs to have the same hardware (MAC) address. Since the Deep Security Agent identifies network adapters by their MAC address, such duplication prevents the agent from functioning properly.

To avoid that, manually assign a unique MAC address to each network adapter.

For example, you could use ifconfig to view the current MAC addresses:

```
# ifconfig -a
hme0: flags=1000843<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
inet 10.20.30.40 netmask 0
ether 8:0:20:f7:c3:f

hme1: flags=1000842<BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 8
inet 0.0.0.0 netmask 0
ether 8:0:20:f7:c3:f
```

The "ether" line displays the adapter's MAC address. If any interfaces have the same MAC addresses, and are connected to the same subnet, you must manually set new unique MAC addresses:

```
# ifconfig <interface> ether <new MAC address>
```

Although the chance of a MAC address conflict is extremely small, you should verify that there isn't one by using the snoop command to search for the MAC address, then use the ping command to test connectivity to the subnet's broadcast address.

> **Note:** On Solaris, if multiple interfaces are on the same subnet, the operating system may route packets through any of the interfaces. Because of this, Deep Security's firewall stateful configuration options and IPS rules should be applied to all interfaces equally.

# Agent-manager communication

Deep Security Manager and the agent communicate using the latest mutually-supported version of TLS.

Topics in this article:

- "Configure the heartbeat" below
- "Configure communication directionality" on the next page
- "Supported cipher suites for agent-manager communication" on page 1377

## Configure the heartbeat

A heartbeat is a periodic communication between Deep Security Manager and Deep Security Agent. During a heartbeat, the manager collects the following information:

- The status of the drivers (on-line or off-line)
- The status of the agent (including clock time)
- The agent logs since the last heartbeat
- Data to update counters
- A fingerprint of the agent security configuration (used to determine if it is up to date)

The heartbeat can be configured on a base or parent policy, on a subpolicy, or on an individual computer.

You can configure the following properties of the heartbeat:

- **Heartbeat Interval:** The amount of time that passes between heartbeats.
- **Number of Heartbeats that can be missed before an alert is raised:** The number of consecutively missed heartbeats that triggers an alert. For example, a value of 3 causes the manager to trigger an alert on the fourth missed heartbeat.

  If the computer is a server, too many missed heartbeats in a row may indicate a problem with the agent, or the computer itself. However, if the computer is a laptop or any other system that is likely to experience a sustained loss of connectivity, this option should be set to Unlimited.

- **Maximum change (in minutes) of the local system time on the computer between heartbeats before an alert is raised:** On Windows, for agents that can detect changes to the system clock, these events are reported to the manager as the agent event 5004. If the change exceeds the clock change listed here, then an alert is triggered. For agents that do not support this capability, the manager monitors the system time reported by the agent at each heartbeat operation and triggers an alert if it detects a change greater than the permissible change specified in this setting.

  Note that once a **Computer-Clock-Changed** alert is triggered, it must be dismissed manually.

- **Raise Offline Errors For Inactive Virtual Machines:** Defines whether or not an offline error is raised when the virtual machine is stopped.

To perform configurations:

1. Open the **Policy editor**[1] or the **Computer editor**[2] for the policy or computer to configure.
2. Go to **Settings > General > Heartbeat.**
3. Change the properties as required.
4. Click **Save** .

## Configure communication directionality

**Note:** Bidirectional communication is enabled by default.

[1] To open the Policy editor, go to the Policies page and double-click the policy that you want to edit (or select the policy and click Details).

[2] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

You can define the artifact that initiates communication. This artifact can be the agent, or the manager. Communication includes the heartbeat and all other communications. The following options are available:

- **Bidirectional**: Typically, the agent initiates the heartbeat and also listens on the agent's listening port number for connections from the Deep Security Manager (see "Deep Security port numbers" on page 478). The manager can contact the agent to perform required operations. The manager can apply changes to the security configuration of the agent.
- **Manager Initiated**: The manager initiates all communication with the agent. These communications include security configuration updates, heartbeat operations, and requests for event logs. If you select this option, it is strongly recommended that you "Protect Deep Security Agent" on page 1492 so that it only accepts connections from known Deep Security Managers.
- **Agent Initiated**: The agent does not listen for connections from the manager. Instead, they contact the manager on the port number where the manager listens for the agent heartbeats (see "Deep Security port numbers" on page 478). Once the agent has established a TCP connection with the manager, all normal communication takes place: the manager first asks the agent for its status and for any events. This is the heartbeat operation. If there are outstanding operations that need to be performed on the computer (for example, the policy needs to be updated), these operations are performed before the connection is closed. Communications between the manager and the agent only occur on every heartbeat. If an agent's security configuration has changed, it is not updated until the next heartbeat.

  **Note:** For instructions on how to configure agent-initiated activation and use deployments scripts to activate agents, see "Activate and protect agents using agent-initiated activation and communication" on page 1386.

To enable communications between the manager and the agents, the manager automatically implements a hidden firewall rule (priority four, Bypass) that opens the listening port number for heartbeats on the agents to incoming TCP/IP traffic. By default, it accepts connection attempts from any IP address and any MAC address. You can restrict incoming traffic on this port by creating a new priority 4, Force Allow or Bypass firewall rule that only allows incoming TCP/IP traffic from specific IP or MAC addresses, or both. This new firewall rule would replace the hidden firewall rule if the settings match the following settings:

- **action**: force allow or bypass
- **priority**: 4 - highest

- **packet's direction**: incoming
- **frame type**: IP
- **protocol**: TCP
- **packet's destination port**: the agent's listening port number for heartbeat connections from the manager, or a list that includes the port number (see agent listening port number)

To perform configurations:

1. Open the **Policy editor**[1] or the **Computer editor**[2] for the policy or computer to configure.
2. Go to **Settings > General > Communication Direction.**
3. In the **Direction of Deep Security Manager to Agent/Appliance communication** menu, select one of the three options: **Manager Initiated**, **Agent/appliance Initiated**, **Bidirectional**, or select **Inherited**. If you select **Inherited**, the policy or computer inherits the setting from its parent policy. Selecting one of the other options overrides the **Inherited** setting.
4. Click **Save**.

Agents look for the Deep Security Manager on the network by the manager's hostname. Therefore, the manager's hostname must be in your local DNS for agent--initiated or bidirectional communication to work.

## Supported cipher suites for agent-manager communication

Deep Security Manager and the agent communicate using the latest mutually-supported version of TLS.

The Deep Security Agent supports the following cipher suites for communication with the manager:

- "Deep Security Agent 9.6 cipher suites" on the next page
- "Deep Security Agent 10.0 cipher suites" on the next page
- "Deep Security Agent 11.0, 12.0, and 20 cipher suites" on the next page

For specifics on the cipher suites supported by Deep Security Manager, contact Trend Micro.

[1] To open the Policy editor, go to the Policies page and double-click the policy that you want to edit (or select the policy and click Details).

[2] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

The cipher suites consist of a key exchange asymmetric algorithm, a symmetric data encryption algorithm and a hash function.

## Deep Security Agent 9.6 cipher suites

Deep Security Agent 9.6 supports the following TLS 1.0 cipher suites:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

## Deep Security Agent 10.0 cipher suites

Deep Security Agent 10.0 supports the following TLS 1.2 cipher suites out-of-the-box:

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256

Deep Security Agent 10.0 Update 16 and later supports the following TLS 1.2 cipher suites, and only these suites, if strong cipher suites are enabled:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

## Deep Security Agent 11.0, 12.0, and 20 cipher suites

Deep Security Agent 11.0 and later supports the following TLS 1.2 cipher suites:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

In FIPS mode, the following TLS 1.2 suites are supported:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256

# Configure agents that have no internet access

If your agents or relays do not have access to the internet (air-gapped agents), then they cannot access some of the security services provided by the Trend Micro Smart Protection Network. These security services are necessary for the full and successful operation of the Deep Security Anti-Malware and Web Reputation modules.

The Trend Micro Smart Protection Network security services include the following:

| Service name | Required for these features |
|---|---|
| Smart Scan Service | Smart Scan |
| Web Reputation Service | Web Reputation |
| Global Census Service | behavior monitoring, predictive machine learning |
| Good File Reputation Service | behavior monitoring, predictive machine learning, process memory scans |
| Predictive Machine Learning Service | predictive machine learning |

In addition to these services, the agent and relay-enabled agent need access to the Trend Micro Update Server (also called Active Update), which is not part of the Smart Protection Network, but is a component that is hosted by Trend Micro and accessed over the internet.

If any of your agents or relay-enabled agents cannot reach these services, you have several solutions.

## Solutions

- Solution 1: "Use a proxy" on the next page
- Solution 2: "Install a Smart Protection Server locally " on the next page
- Solution 3: "Get updates in an isolated network" on page 1381
- Solution 4: "Disable features that use Trend Micro security services" on page 1384

## Use a proxy

If your agents or relay-enabled agents cannot connect to the internet, you can install a proxy that can. Your Deep Security Agents and relays connect to the proxy, and the proxy then connects outbound to the Trend Micro security services in the Smart Protection Network.

With a proxy, each Smart Scan or Web Reputation request goes out over the internet to the Smart Protection Network. Consider instead using a Smart Protection Server inside your LAN to keep these requests within your network and reduce extranet bandwidth usage.

To use a proxy, see "Configure proxies" on page 1335.

## Install a Smart Protection Server locally

If your agents and relay-enabled agents cannot connect to the internet, you can install a Smart Protection Server in your local area network (LAN) to which your agents and relay-enabled agents can connect. The local Smart Protection Server periodically connects outbound over the internet to the Smart Protection Network to retrieve the latest Smart Scan Anti-Malware patterns and Web Reputation information. This information is cached on the Smart Protection Server and queried by your agents and relay-enabled agents. The Smart Protection Server does not push updates to the agents or relay-enabled agents.

If you decide to use this solution, keep in mind the following:

- The functionality is limited. Only the Smart Scan and Web Reputation modules are supported with a local Smart Protection Server.
- Use the proxy solution if you need Behavior Monitoring, Predictive Machine Learning, and Process Memory scanning. See "Use a proxy" above for details. If you decide not to use these features, you must disable them to prevent a query failure and to improve performance. For instructions, see "Disable features that use Trend Micro security services" on page 1384

To deploy a Smart Protection Server, install it manually. See the Smart Protection Server documentation for details.

This scenario applies when only an agent and relay-enabled agent are air-gapped, but Deep Security Manager has internet access or proxy access, as described in "Port numbers, URLs, and IP addresses" on page 478. If Deep Security Manager is also air-gapped, you need to use a proxy to receive security updates from the Trend Micro Active Update Server. Alternatively, use Solution 3 "Get updates in an isolated network" on the next page.

## Get updates in an isolated network

If your Deep Security Manager is in an isolated network without connection to the internet and your agents or relay-enabled agents cannot connect to the internet, you can install an additional stand-alone Deep Security Manager with database and a relay-enabled agent in your demilitarized zone (DMZ) or another area where internet access is available.

Once all the components are installed, you can configure the relay-enabled agent in the DMZ to automatically obtain the latest malware scan updates from the Update Server on the internet. These updates must be extracted to a `.zip` file, and then manually copied to your air-gapped relay.

If you decide to use this solution, keep in mind the following:

- The `.zip` file contains traditional (large) malware patterns, which give you basic Anti-Malware capabilities.
- The `.zip` file also contains Deep Security Rule Updates, which are used for Intrusion Prevention, Integrity Monitoring, and Log Inspection. You can also choose to obtain those updates separately. See "Get rules updates in an isolated network" on page 1383.
- The following advanced Anti-Malware features are not available: Smart Scan, behavior monitoring, predictive machine learning, process memory scans, and Web Reputation. These features require access to Trend Micro security services.
- You should disable advanced Anti-Malware features, since they cannot be used.
- You should have a plan in place to periodically update the `.zip` file on your air-gapped relay to ensure you always have the latest malware patterns.

To deploy this solution, follow these steps:

1. Install Deep Security Manager and its associated database in your DMZ. These internet-facing components can be referred to as DMZ manager and DMZ database.
2. Install an agent in your DMZ and configure it as a relay. This agent can be referred to the DMZ relay. For information on setting up relays, see "Deploy additional relays" on page 1345.
   The following is now installed:
   - DMZ manager
   - DMZ database
   - DMZ relay
   - air-gapped manager

- air-gapped database
- air-gapped relay
- multiple air-gapped agents

3. On the DMZ relay, create a `.zip` file containing the latest malware patterns by running this command:

   ```
   dsa_control -b
   ```
   The command line output shows the name and location of the `.zip` file that was generated.

4. Copy the `.zip` file to the air-gapped relay. Place the file in the relay's installation directory:
   - On Windows, the default directory is `C:\Program Files\Trend Micro\Deep Security Agent`.
   - On Linux, the default directory is `/opt/ds_agent`.

   Do not rename the .zip file.

5. On the air-gapped manager, initiate a security update download:
   a. Click **Computers** at the top.
   b. In the list of computers, find your air-gapped relay where you copied the `.zip` file, right-click it and select **Download Security Update**.
   The air-gapped relay checks its configured update source (typically the Update Server on the internet). Since it cannot connect to this server, it checks the `.zip` file in its installation directory. When it finds the `.zip` file, it extracts it and imports the updates. The updates are then disseminated to the air-gapped agents that are configured to connect to the relay.
   c. Delete the `.zip` file after the updates are imported to the air-gapped relay.
6. Configure the air-gapped relay to connect to itself instead of the Update Server (to prevent connection error alerts):
   a. Log in to the air-gapped manager.
   b. Click **Administration** on the top.
   c. On the left, click **System Settings**.
   d. In the main pane, select the **Updates** tab.
   e. Under **Primary Security Update Source**, select **Other update source** and enter `https://localhost:[port]` where `[port]` is the configured port number for security updates, by default `4122`.
   f. Click **OK**.
   The air-gapped relay no longer tries to connect to the Update Server on the internet.
7. Optionally, to improve performance, "Disable features that use Trend Micro security services" on page 1384.

8. On a periodic basis, download the latest updates to your DMZ relay, zip them, copy them to your air-gapped relay, and initiate a security update download on the relay.

You have now deployed a Deep Security Manager, associated database, and relay in your DMZ from which to obtain malware scan updates.

To upgrade this solution, perform the upgrade in the following order:

1. DMZ manager (and its database, if the database software also needs to be upgraded)
2. DMZ relay
3. air-gapped manager (and its database, if the database software also needs to be upgraded)
4. air-gapped relay
5. air-gapped agents

> **Warning:** If you do not upgrade relays first, security component upgrades and software upgrades may fail.

For details on upgrading, see "Upgrade Deep Security Relay" on page 1541, and "Upgrade Deep Security Agent" on page 1542.

## Get rules updates in an isolated network

The `.zip` file you created contains the Deep Security Rule Updates that are used for Intrusion Prevention, Integrity Monitoring, and Log Inspection. However, if you would like to get those updates separately:

1. On the DMZ manager, go to **Administration > Updates > Security > Rules**.
2. Click a rule update `.dsru` file and click **Export**. The file is downloaded locally.
3. Repeat the export for each `.dsru` file that you want to apply to the air-gapped manager.
4. Copy the `.dsru` files to the air-gapped manager.
5. On the air-gapped manager, go to **Administration > Updates > Security > Rules**.
6. Click **Import**, select the `.dsru` file, and click **Next**.
7. The manager validates the file and displays a summary of the rules it contains. Click **Next**.

   A message displays, saying that the rule update was imported successfully.

8. Click **Close**.
9. Repeat the import for each `.dsru` file that you want to apply to the air-gapped manager.

## Disable features that use Trend Micro security services

You can disable features that use Trend Micro security services. Doing so improves performance because the air-gapped agent no longer tries (and fails) to query the services.

**Note:** Without Trend Micro security services, your malware detection is downgraded significantly, ransomware is not detected at all, and process memory scans are also affected. It is therefore strongly recommended that you use one of the other solutions to allow access to Trend Micro security services. If this is impossible, only then should you disable features to realize performance gains.

- To disable Smart Scans:
  a. Open the **Computer or Policy editor**[1] .
  b. On the left, click **Anti-Malware**.
  c. In the main pane, click **Smart Protection**.
  d. Under **Smart Scan**, deselect **Inherited** (if it is selected), and then select **Off**.
  e. Click **Save**.
- To disable Web Reputation:
  a. Open the **Computer or Policy editor**[2].
  b. On the left, click **Web Reputation**.
  c. In the main pane, make sure the **General** tab is selected.
  d. From the **Configuration** list, select **Off**.
  e. Click **Save**.
- To disable Smart Feedback:
  a. In Deep Security Manager, click **Administration** at the top.
  b. Click **System Settings** on the left.
  c. In the main pane, select the **Smart Feedback** tab.

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

[2] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

   d. Deselect **Enable Trend Micro Smart Feedback (recommended)**.
   e. Click **Save**.

- To disable Process Memory scans:
   a. In Deep Security Manager, click **Policies** at the top.
   b. On the left, expand **Common Objects > Other**, and then click **Malware Scan Configurations**.
   c. Double-click a malware scan configuration with a **SCAN TYPE** of **Real-Time**.
   d. On the **General** tab, under **Process Memory Scan**, deselect **Scan process memory for malware**.
   e. Click **OK**.
- To disable Predictive Machine Learning:
   a. Make sure you still have a real-time malware scan configuration open.
   b. On the **General** tab, under **Predictive Machine Learning**, deselect **Enable Predictive Machine Learning.**
   c. Click **OK**.
- To disable Behavior Monitoring:
   a. Make sure you still have a real-time malware scan configuration open.
   b. On the **General** tab, under **Behavior Monitoring**, deselect **Enable Behavior Monitoring**.
   c. Click **OK**.

To improve performance, you can disable the census and grid (Good File Reputation) queries on Deep Security Manager. If you leave them enabled, a significant amount of unnecessary background processing takes place.

- To disable the census query using the command line, execute the following:

```
dsm_c -action changesetting -name
settings.configuration.enableCensusQuery -value false
```

- To disable the census query from the UI:
   a. Go to **Computer > Settings > General > Network Setting for Census, Good File Reputation, and Predictive Machine Learning Services**.
   b. For **Enable Census query**, select **No**.

- Disable the grid query using the command line, execute the following:

  ```
  dsm_c -action changesetting -name settings.configuration.enableGridQuery
  -value false
  ```

- To disable the grid query from the UI:
  1. Go to **Computer > Settings > General > Network Setting for Census, Good File Reputation, and Predictive Machine Learning Services**.
  2. For **Enable Good file reputation query**, select **No**.

## Activate and protect agents using agent-initiated activation and communication

When you enable agent-initiated activation (AIA), instead of the Deep Security Manager contacting the agents directly, the agents initiate communication with the manager and establish an encrypted TCP connection over the manager heartbeat port (4120 by default).

Enabling AIA can prevent communication issues between the manager and agents, and simplify agent deployment when used with deployment scripts. Trend Micro recommends that you use AIA if:

- Your network environment prevents the manager from initiating connections to agents.
- You need to deploy many agents at once.
- You are protecting computers in cloud accounts.

**Note:** Before enabling AIA, ensure that agents can reach the manager URL and heartbeat port. You can find the manager URL(s) and heartbeat port under **Administration > System Information > System Details > Manager Node**.

### Enable agent-initiated activation and communication

Proceed with the following steps:

1. "Create or modify policies with agent-initiated communication enabled" on the next page.
2. "Enable agent-initiated activation" on the next page.
3. "Assign the policy to agents" on the next page.
4. "Use a deployment script to activate the agents" on the next page.

## Create or modify policies with agent-initiated communication enabled

For your agents to continue initiating communication with the manager after activation, you'll need to enable agent-initiated communication on any policies the agents will use. You can do this by either modifying an existing policy or by creating a new one, which you'll assign to the agents.

> Tip: You can quickly create a new policy from an existing policy by right-clicking it and selecting **Duplicate**.

1. On the **Policies** page, double-click the policy.
2. Go to **Settings > General**.
3. Under Communication Direction, select **Agent/Appliance Initiated**.
4. Click **Save**.

## Enable agent-initiated activation

1. Go to **Administration > System Settings > Agents**.
2. Select **Allow Agent-Initiated Activation**.
3. Select **Allow Agent to specify hostname**.
4. From the **If a computer with the same name exists** list, select **Re-activate the existing computer**.
5. Click **Save**.

> **Note:** For a full description of each AIA setting, see the Agent-Initiated Activation section of "Agent settings" on page 1399.

## Assign the policy to agents

You can either assign the policy to the agents during the deployment script configuration, or by using an event-based task after the deployment script has been run.

If all the agents will use the same policy, you can assign the policy in the deployment script as part of the next step. If groups of agents need to use different policies, create an event-based task to assign the policies before proceeding with the next step.

## Use a deployment script to activate the agents

See the Generate a deployment section of "Generate a deployment script" on page 1623 to learn how to use a deployment script to activate the agents. If you are assigning a policy during deployment script configuration, you'll select it from the **Security Policy** list.

# Automatically upgrade agents on activation

'Upgrade on activation' is a feature that can be used to automatically upgrade Deep Security Agents to a newer version of software based on a check of the agent version during the activation process. This feature is especially useful if you want to distribute the agent using the baking process (see "Install the agent on an AMI or WorkSpace bundle" on page 560). When agents are baked it can be difficult for you to update your ‘golden’ images each time a new version of the Deep Security Agent is released. In this case, 'upgrade on activation' can be used so that each time the older agent from the baked image activates, Deep Security Manager instructs the agent to upgrade to the version you specify as part of the activation process keeping the running agents used in your environment up-to-date.

**Note:** This feature complies with your agent version control settings.

**Note:** This feature is currently available only on Linux and Windows computers. Support for Unix is planned for a future release.

This feature works with these operating systems:

- Red Hat Enterprise Linux
- Ubuntu
- CentOS
- Debian
- Amazon Linux
- Oracle Linux
- SUSE Linux Enterprise Server
- Cloud Linux
- Windows

## Enable automatic agent upgrade

1. Make sure the latest agent software and kernel support packages are available in Deep Security Manager. You can configure Deep Security Manager to automatically download software updates, or import them manually. For details, see "Get Deep Security Agent software" on page 520.
2. Go to **Administration > System Settings > Agents**.

3. Under **Agent Upgrade**, select any of the following: **Automatically upgrade Linux agents on activation**, **Automatically upgrade Windows agents on activation**, **Automatically upgrade Unix agents on activation**.
4. Click **Save**.

## Check that agents were upgraded successfully

The **Version** column on the **Computers** page displays the installed Deep Security Agent version for each computer.

In addition, when an automatic agent upgrade is triggered, "System events" on page 1233 are generated that you can use to track the status of the upgrade. You can check for these system events:

| ID | Event | Description |
|---|---|---|
| 264 | Agent Software Upgrade Requested | An agent software upgrade has been triggered, either manually or by an automatic agent upgrade. |
| 277 | Upgrade on Activation Skipped | The agent was eligible for an automatic upgrade, but the upgrade did not occur.<br>The event details list the existing agent version and the attempted upgrade version, along with the reason the upgrade failed. The reasons can be:<br>• Upgrade on activation was skipped for this computer because there is a pending reboot request. Please restart the computer to resolve this issue. The upgrade request will be serviced during the next activation after the reboot.<br>• Upgrade on activation is not currently supported for use on Windows servers when the target version to upgrade to is earlier than Deep Security Agent 12. There are improvements in the 12 agent that are required for this feature. Please update the agent version control configuration to use a 12 or later agent for this platform to allow the upgrade to succeed.<br>• The agent was not upgraded automatically because a |

| ID | Event | Description |
|---|---|---|
| | | required Linux kernel support file was not found. Deep Security Manager usually downloads required Linux kernel support packages automatically, but you can also download and import packages to Deep Security Manager manually and then upgrade the agent. See "Get Deep Security Agent software" on page 520.<br>• The agent was not upgraded automatically because the upgrade on activation feature does not support the currently installed OS. You may be able to upgrade the agent manually. See "Install the agent" on page 548. |
| 706 | Software Update: Agent Software Upgraded | The upgrade was successful. |
| 707 | Software Update: Agent Software Upgrade Failed | The upgrade was not successful. Refer to the event details for more information about why it was not successful. |

## Using Deep Security with iptables

When Deep Security Agent 10.1 or earlier was installed on Linux, it disabled the iptables service to avoid firewall conflicts unless you added a configuration file that prevented that change. However, the iptables service is used for more than just firewall (for example, Docker manages iptables rules as part of its normal operation), so disabling it sometimes had negative consequences.

With Deep Security 10.2 and higher (including Deep Security 11), the functionality around iptables has changed. Deep Security Agent no longer disables iptables. (If iptables is enabled, it stays enabled after the agent installation. If iptables is disabled, it stays disabled.) However, if the iptables service is running, Deep Security Agent and Deep Security Manager require certain iptables rules, as described below.

## Rules required by Deep Security Manager

If iptables is enabled on the computer where Deep Security Manager is being installed, there are two required iptables rules. By default, these rules are added when Deep Security Manager starts up and removed when the manager is stopped or uninstalled. Alternatively, you can "Prevent Deep Security from automatically adding iptables rules" below and add them manually instead:

- Allow incoming traffic on port 4119. This is required for access to the Deep Security Manager web UI and API.
- Allow incoming traffic on port 4120. This is required to listen for agent heartbeats. (For more information, see "Agent-manager communication" on page 1374.)

**Note:** These are the default port numbers - yours may be different. For a complete list of ports used in Deep Security, see "Port numbers, URLs, and IP addresses" on page 478.

## Rules required by Deep Security Agent

If iptables is enabled on the computer where Deep Security Agent is being installed, iptables may require additional rules. By default, these rules are added when Deep Security Agent starts up and removed when the agent is stopped or uninstalled. Alternatively, you can "Prevent Deep Security from automatically adding iptables rules" below and add them manually instead:

- Allow incoming traffic on port 4118. This is required when the agent uses manager-initiated or bidirectional communication. (For more information, see "Agent-manager communication" on page 1374.)
- Allow incoming traffic on port 4122. This is required when the agent is acting as a relay, so that the relay can distribute software updates. (For more information, see "Deploy additional relays" on page 1345.)

**Note:** These are the default port numbers - yours may be different. For a complete list of ports used in Deep Security, see "Port numbers, URLs, and IP addresses" on page 478.

## Prevent Deep Security from automatically adding iptables rules

You can prevent Deep Security Manager and Deep Security Agent from modifying iptables if you would rather add the required rules manually. To prevent the automatic modification of iptables, create the following file on the computers where you plan to install Deep Security Manager and Deep Security Agent:

`/etc/do_not_open_ports_on_iptables`

# Enable or disable agent self-protection

Deep Security Agent self-protection prevents local users from tampering with the agent. When enabled, if a local user tries to tamper with the agent, a message such as "Removal or modification of this application is prohibited by its security settings" is displayed.

The agent self-protection is supported on Windows and on Linux. The latter requires the Deep Security Agent version 20.0.0-5953 or later.

To update or uninstall Deep Security Agent or relay, or if you are a local user trying to create a diagnostic package for support from the command line, as described in Create a diagnostic package and logs, you must temporarily disable agent self-protection.

On Windows, Anti-Malware protection must be enabled to prevent local users from stopping the agent, as well as from modifying agent-related files and Windows registry entries. On Linux, at least one of the following must be enabled: Anti-Malware, Application Control, Integrity Monitoring with Real Time. Self-protection is not required to prevent uninstalling the agent.

Before stopping Deep Security Agent, its self-protection, which is, essentially, a safeguard against unauthorized modifications, must be disabled to avoid problems and ensure a smooth operation.

You can configure agent self-protection using either Deep Security Manager or the command line on the agent's computer.

## Configure self-protection through Deep Security Manager

1. Open the Computer or Policy editor[1] where you want to enable agent self-protection.
2. Select **Settings > General**.
3. In the **Agent Self-Protection** section, select **Yes** to prevent local users from uninstalling, stopping, or otherwise modifying the agent.

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

4. For **Local override requires password**, select **Yes** and type an authentication password. The authentication password is highly recommended because it prevents an unauthorized use of the dsa_control command. After specifying the password, it must be entered with the `dsa_control` command using the `-p` or `--passwd=` option whenever a command is executed on the agent. Note that the password cannot be longer than 32 characters; if this length is exceeded, the password is automatically truncated.
5. Click **Save**.
6. To disable self-protection, select **No**, and then click **Save**.

## Configure self-protection using the command line

You can enable and disable self-protection using the command line, with one limitation: you cannot specify an authentication password. You need to use Deep Security Manager for that (see "Configure self-protection through Deep Security Manager" on the previous page).

### Use the command line on Windows

1. Log in to the Windows agent locally.
2. Open the command prompt (`cmd.exe`) as an Administrator.
3. Change the current directory to the Deep Security Agent installation folder. The following shows the default installation folder:

   ```
   cd C:\Program Files\Trend Micro\Deep Security Agent
   ```

4. Enter one of the following commands:

   To enable agent self-protection, enter:

   ```
   dsa_control --selfprotect=1
   ```

   To disable agent self-protection, enter:

   `dsa_control --selfprotect=0 -p <password>`, where `-p <password>` is the authentication password, if one was previously specified in Deep Security Manager. For details, see "Configure self-protection through Deep Security Manager" on the previous page.

## Use the command line on Linux

1. Open the command prompt as an Administrator.
2. Change the current directory to the Deep Security Agent installation folder. The following shows the default installation folder:

   ```
   cd /opt/ds_agent
   ```

3. Enter one of the following commands:

   To enable agent self-protection, enter:

   ```
   dsa_control --selfprotect=1
   ```

   To disable agent self-protection, enter:

   `dsa_control --selfprotect=0 -p <password>`, where `-p <password>` is the authentication password, if one was specified previously in Deep Security Manager. For details, see "Configure self-protection through Deep Security Manager" on page 1392 Note that the password cannot be longer than 32 characters; if this length is exceeded, the password is automatically truncated..

# Limitations on Linux

- The agent service should not be stopped when the system is shutting down or rebooting. Stopping the service may prevent it from working properly after the reboot.
- The status of the agent service may be inconsistent. If you try to stop the agent service running the command stop, the result returned as successful, however the agent service still runs as normal.
- If there is a running process that has the same name as an agent process in the system, it is added to the self-protection list. The protected process is protected from tampering.
- The agent service cannot be killed when Out-Of-Memory (OOM) happens.
- Oracle 6 (32-bit) platform does not support self protection.
- If you have enabled secure boot and self-protection is not working, check your machine's

kernel version. If the kernel version is 5.4 or earlier, upgrade to a kernel version that is later than 5.4.

### Troubleshooting

You can restore the service status to normal as follows:

1. Stop agent self-protection.
2. Restart the agent service.

The agent self-protection resumes after the agent service restarts.

## Are offline agents still protected by Deep Security?

Agents showing as Offline in the Deep Security Manager are still protected according to their last known configuration. However, they cannot receive any software, security or policy updates until communication with the Deep Security Manager is restored.

For more information on how to bring an agent out of offline status, see "Offline agent" on page 1697.

## Automate offline computer removal with inactive agent cleanup

If your Deep Security deployment has a large number of offline computers not communicating with the Deep Security Manager, first try using a connector (see "About adding AWS accounts" on page 582, "Add a Microsoft Azure account to Deep Security" on page 602, or "Add a Google Cloud Platform account" on page 614). When you use a connector, the complete life cycle of your computers is managed automatically, meaning that computers deleted from your cloud accounts are also automatically removed from Deep Security. If you can't use a connector in your environment, you can automate the removal of inactive computers using **inactive agent cleanup**. Inactive agent cleanup will check hourly for computers that have been offline and inactive for a specified period of time (from 2 days to 12 months) and remove them.

**Note:** Inactive agent cleanup will remove a maximum of 1000 offline computers at each hourly check. If there are more offline computers than this, 1000 will be removed at each consecutive check until all of the offline computers have been removed.

After enabling inactive agent cleanup, you can also

- "Ensure computers that are offline for extended periods of time remain protected with Deep Security" below (optional but recommended).
- "Set an override to prevent specific computers from being removed" on the next page (optional).
- "Check the audit trail for computers removed by an inactive cleanup job" on the next page.

**Note:** Inactive agent cleanup does not remove offline computers that have been added by a cloud connector.

## Enable inactive agent cleanup

1. Go to the **Administration** page.
2. Under **System Settings > Agents > Inactive Agent Cleanup**, select **Delete Agents that have been inactive for**.
3. From the list, select the period that a computer must be inactive before being removed.
4. "Ensure computers that are offline for extended periods of time remain protected with Deep Security" below (optional but recommended).
5. Click **Save**.

### Ensure computers that are offline for extended periods of time remain protected with Deep Security

If you have offline computers that are active but communicate irregularly with the Deep Security Manager, inactive agent cleanup will remove them if they don't communicate within the period of inactivity you defined. To ensure that these computers reconnect to Deep Security Manager, we recommend enabling both **Agent-Initiated Activation** and **Reactivate unknown Agents**. To do so, under **System Settings > Agents > Agent Initiated Activation**, first select **Allow Agent-Initiated Activation** and then select **Reactivate Unknown Agents**.

**Note:** When a removed computer reconnects, it will not have a policy, and will be added as a new computer. Any direct links to the computer will be removed from the Deep Security Manager event data.

**Tip:** You can automatically assign a policy assigned to a computer upon agent-initiated activation with an event-based task.

### Set an override to prevent specific computers from being removed

You can set an override at the computer or policy level to explicitly prevent computers from being removed by inactive agent cleanup.

To set an override

1. Open the **Computer or Policy editor**[1] for the computer or policy you want to set an override on.
2. Go to **Settings > General**.
3. Under **Inactive Agent Cleanup Override**, select **Yes**.
4. Click **Save**.

## Check the audit trail for computers removed by an inactive cleanup job

When an inactive agent cleanup job runs, system events will be generated that you can use to track removed computers.

You'll need to check the following system events:

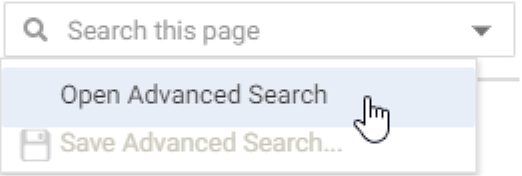
- "2953 - Inactive Agent Cleanup Completed Successfully" on the next page
- "251 - Computer Deleted" on the next page
- "716 - Reactivation Attempted by Unknown Agent" on the next page (if 'Reactivate Unknown Agents' is enabled)

### Search system events

To view the system events generated by an inactive agent cleanup job, you need to create a search that filters for them:

[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

1. Go to the **Events and Reports** page.
2. In the top-right corner, click the Search field list and select **Open Advanced Search**.



3. For the **Period**, select **Custom Range** from the list.
4. For **From**, enter the date and time just before the inactive agent cleanup job was first run. For **To**, enter the date and time just after the cleanup job finished.
5. For the **Search**, select **Event ID** and **In**, and then enter **2953, 251**. You can optionally enter **716** and any of the event IDs (**130, 790, 350, 250**) associated with computer reactivation.

This will display all the system events generated by an inactive agent cleanup job. You can sort the events by time, event ID or event name by clicking on the corresponding column. You can then double-click an event to get more information about it, as detailed below.

## System event details

### 2953 - Inactive Agent Cleanup Completed Successfully

This event is generated when the inactive agent cleanup job runs and successfully removes computers. The description for this event will tell you how many computers were removed.

> **Note:** If more than one check is needed to remove all computers, a separate system event will be generated for each check.

### 251 - Computer Deleted

In addition to the 'Inactive Agent Cleanup Completed Successfully' event, a separate 'Computer Deleted' event is generated for each computer that was removed.

### 716 - Reactivation Attempted by Unknown Agent

If **Reactivate Unknown Agents** is enabled, this event will be generated for an activated computer that was removed when it attempts to reconnect to the Deep Security Manager. Each reactivated computer will also generate the following system events:

- **130** - Credentials Generated
- **790** - Agent-Initiated Activation Requested
- **350** - Policy Created (if you've enabled an event-based task that assigns a policy)

- **250** - Computer Created
  or
  **252** - Computer Updated

# Agent settings

Deep Security Agent-related settings are located on **Administration > System Settings > Agents**. They include the following.

> **Tip:** You can automate agent-related system setting changes using the Deep Security API. For examples, see Configure Policy, Computer, and System Settings.

## Hostnames

**Update the "Hostname" entry if an IP is used as a hostname and a change in IP is detected on the computer after Agent/Appliance-initiated communication or discovery:** Updates the IP address displayed in the computer's "Hostname" property field if an IP change is detected.

> **Note:** Deep Security Manager identifies protected computers by using a unique fingerprint, not their IP addresses or hostnames.

## Agent-initiated activation (AIA)

You can activate new agents in the Deep Security Manager using a cloud connector or by manually adding a new computer on **Computers**. Alternatively, you can allow agents to automatically activate themselves. See also "Activate and protect agents using agent-initiated activation and communication" on page 1386.

**Allow Agent-Initiated Activation:** Allow agents to connect to the manager to activate themselves. Then select which computers are allowed to perform agent-initiated activation.

- **For Any Computers:** Any computer, whether it is already listed on **Computers** or not.

  > **Warning:** To prevent unauthorized agent activations, don't enable this option if your network allows connections to Deep Security Manager from untrusted networks such as the Internet. To similarly protect Deep Security Agent from unauthorized managers, only allow agent activation with your authenticated manager.

- **For Existing Computers:** Only computers already listed on **Computers**.
- **For Computers on the following IP List:** Only computers whose IP address has a match on the specified IP list.

Also configure initiation behavior:

- **Policy to assign (if Policy not assigned by activation script):** Security policy to assign to the computer during activation. This setting only applies if no policy is specified in the agent's activation script or an AIA event-based task.
- **Allow Agent to specify hostname**: Allow the agent to specify its hostname by providing it to Deep Security Manager during activation.

- **If a computer with the same name already exists:** How to handle the activation attempt if the new computer is trying to use the same agent GUID or certificate as an existing computer:

  - **Do not allow activation**: Don't activate the computer.
  - **Activate a new Computer with the same name**: Using a new name, create a new computer object and activate the computer.
  - **Re-activate the existing Computer**: Keeping the same name, reuse the existing computer object and activate the computer.

  This setting only applies to physical computers, Azure virtual machiness (VMs), Google Cloud Platform (GCP) VMs, or VMware VMs. (AWS provides a unique instance ID that Deep Security Manager uses to differentiate all AWS instances, so this setting is ignored for those computers.)

- **Reactivate cloned Agents:** Reactivate clones as new computers; assign the the policy selected in Policy to assign (if Policy not assigned by activation script). This can be useful when re-imaging computer hard disks, or deploying new VM instances or AMI, using a "golden image" that has an already-activated Deep Security Agent. It ensures that each computer has a unique agent GUID, despite being deployed by copying the same software image.

  Clones are detected after the initial activation, during their first heartbeat. If the same agent GUID is being used on different computers, the manager detects the clones and reactivates those computers.

> **Note:** If you disable this option, clones will *not* be automatically reactivated. You'll need to activate them either manually through the manager or using an activation script.

This setting only applies to AWS instances, Azure virtual machines (VMs), Google Cloud Platform (GCP) VMs, or VMware VMs that you added using **Computers > Add Account**.

- **Reactivate unknown Agents:** Reactivate deleted (but previously activated) computers as new computers if they connect again. The original computer's assigned policies or rules will not be assigned to the computer again by default. You should assign it again manually or use a tool such as an event-based task to assign it automatically. This setting is useful together with inactive agent cleanup: any accidentally removed computers can automatically re-activate. See also "Automate offline computer removal with inactive agent cleanup" on page 1395.

  Previously known agents are detected after the initial activation, during their next heartbeat. If a heartbeat has an agent GUID (indicating prior activation) but its computer is not currently listed on **Computers**, the manager reactivates the computer.

  > **Note:** Previous event messages will still link to the old computer object, not this new one.

- **Agent activation token:** Optional. Agent activation secret. If specified, agents must provide the same value when activating.

  > **Note:** If Deep Security Manager is multi-tenant, this setting applies only to the primary tenant.

  To configure this, you can use the `token` parameter in the agent activation script such as:

  ```
  /opt/ds_agent/dsa_control -a dsm://172.16.0.5:4120/ "token:secret"
  ```

## Agent Upgrade

**Automatically upgrade agents on activation:** During activation, upgrade Deep Security Agent to the latest software version that's compatible with Deep Security Manager. Linux computers only. See also "Automatically upgrade agents on activation" on page 1388.

## Inactive Agent Cleanup

If you have many offline computers (that is, computers not communicating with Deep Security Manager), you can automatically remove them from **Computers** using inactive agent cleanup. This setting is useful together with reactivating currently unknown agents. See also "Automate offline computer removal with inactive agent cleanup" on page 1395.

**Delete Agents that have been inactive for:** How much time a computer must be inactive in order to be removed.

## Data Privacy

**Allow packet data capture in network events:** This setting determines whether the agent captures and sends packet data to Deep Security Manager as part of Intrusion Prevention and Firewall events. The options for this setting are:

- **Yes (excluding encrypted traffic):** This is the default option. All unencrypted packet data is sent to Deep Security Manager.
- **Yes (all traffic):** All packet data is sent to Deep Security Manager, including encrypted packet data. The resource requirements for capture of packet data on encrypted connections is higher than for unencrypted connections. If you select this option and encounter problems with performance on your workloads, consider switching to the option that excludes encrypted traffic.
- **No:** Packet data is not captured or transmitted from the agent to Deep Security Manager. Customers in regulated environments or who are concerned about the transmission of network content to Deep Security Manager can disable this setting. For more information about data transmitted to Deep Security Manager, see the Deep Security 20.0 Data Collection Notice.

**Note:** This feature is supported with Deep Security Agent 12.5.0.1001 or later.

## Agentless vCloud Protection

**Allow Appliance protection of vCloud VMs:** Allow virtual machines in VMware vCloud to be protected by Deep Security Virtual Appliance instead of (or in addition to) Deep Security Agent. If Deep Security Manager is multi-tenant, tenants configure the security policies of those VMs.

# User mode solution

User mode provides event generation and basic functions for Anti-Malware without any driver requirements. This solution allows some protection for systems that lack the driver support required to run in kernel mode, and provides the auto option to automatically enable the best protection available at any given time.

For details on basic functions, see Anti-Malware Engine has only Basic Functions.

## Available modes

The following modes are available:

- Kernel mode generates events and provides full Anti-Malware functionality, but can only be enabled on systems with the required driver support.
- User mode generates events and enables basic functions for Anti-Malware without any driver requirements. This mode can be enabled to run on a system without using drivers, even if the system supports the drivers required to run in kernel mode.
- Auto mode switches between kernel mode and user mode to provide the best protection available at any given time. Kernel mode is prioritized, but Deep Security Agent switches to user mode automatically during any driver support gaps that prevent kernel mode operation. If a system that lacks the required drivers to run in Kernel mode later obtains them (from a system update, for example), then the agent automatically switches to use Kernel mode and give the system full protection from Anti-Malware.

## Use drivers for system protection

If you choose to use drivers for system protection, you can configure the driver mode as follows:

1. Go to **Computer** (or **Policy**) **> System > General > Choose whether to use Drivers for System Protection**
2. Select either **Auto**, **Kernel Mode**, or **User Mode** from the menu.
3. Click **Save**.

## Supported agents

| Operating System | Feature support in User mode |
|---|---|
| | Anti-Malware |
| AlmaLinux 9 (64-bit) | ✓ |
| Amazon Linux (64-bit) | |
| Amazon Linux 2 (64-bit) | ✓ |
| Amazon Linux 2 (AWS Arm-based Graviton 2) | |
| Amazon Linux 2 (AWS Arm-based Graviton 3) | |
| Amazon Linux 2023 (64-bit) | ✓ |
| Debian 8 (64-bit) | |
| Debian 9 (64-bit) | |
| Debian 10 (64-bit) | ✓ |
| Debian 11 (64-bit) | ✓ |
| Debian 12 (64-bit) | ✓ |
| Oracle Linux 6 (32-bit) | |
| Oracle Linux 6 (64-bit) | |
| Oracle Linux 7 (64-bit) | |
| Oracle Linux 8 (64-bit) | ✓ |
| Oracle Linux 9 (64-bit) | ✓ |
| Red Hat Enterprise Linux 6 (32-bit) | |
| Red Hat Enterprise Linux 6 (64-bit) | |

| Operating System | Feature support in User mode |
|---|---|
| | Anti-Malware |
| Red Hat Enterprise Linux 7 (64-bit) | |
| Red Hat Enterprise Linux 8 (64-bit) | |
| Red Hat Enterprise Linux 8 (AWS ARM-Based Graviton 2) | |
| Red Hat Enterprise Linux 8.6 (PowerPC little-endian) | |
| Red Hat Enterprise Linux 9 (64-bit) | ✓ |
| Red Hat Enterprise Linux Workstation 7 (64-bit) | |
| SUSE Linux Enterprise Server 12 (64-bit) | |
| SUSE Linux Enterprise Server 12 (PowerPC little-endian) | |
| SUSE Linux Enterprise Server 15 (64-bit) | ✓ |
| SUSE Linux Enterprise Server 15 (PowerPC little-endian) | |
| Ubuntu 16.04 (64-bit) | |
| Ubuntu 18.04 (64-bit) | |
| Ubuntu 18.04 (AWS ARM-Based Graviton 2) | |
| Ubuntu 20.04 (64-bit) | ✓ |
| Ubuntu 20.04 (AWS ARM-Based Graviton 2) | |
| Ubuntu 22.04 (64-bit) | ✓ |
| Ubuntu 22.04 (AWS ARM-Based Graviton 2) | |

## Deep Security notifier

The Deep Security notifier is a Windows taskbar application that communicates the state of the Deep Security Agent and Deep Security Relay to client machines. The notifier displays popup user notifications in the taskbar notification area when the Deep Security Agent blocks malware or prevents access to malicious web pages.

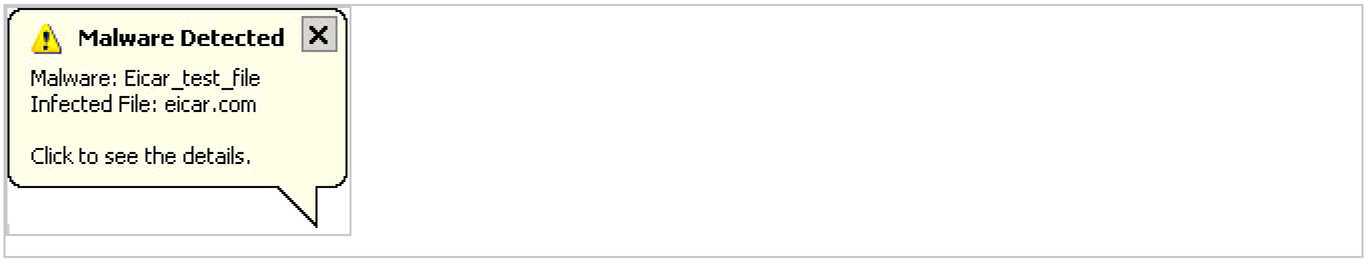
The notifier has a small footprint on the client machine, requiring less than 1MB of disk space and 1MB of memory. When the notifier is running, the notifier icon ( ) appears in the taskbar. The notifier is automatically installed by default with the Deep Security Agent on Windows computers. Use the **Administration > Updates > Software > Local** page to import the latest version for distribution and upgrades.

On computers running a relay-enabled agent, the notifier displays the components that are being distributed to agents or appliances, *not* which components are in effect on the local computer.

## How the notifier works

When malware is detected or a malicious site is blocked, the Deep Security Agent sends a message to the notifier, which displays a popup message in the notification area of the taskbar.

If malware is detected, the notification area displays a pop-up message similar to the following:

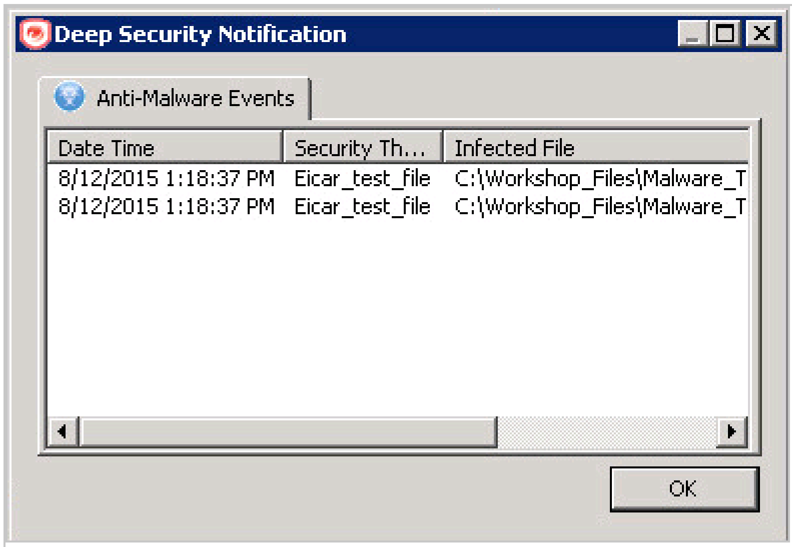


**Malware Detected**

Malware: Eicar_test_file
Infected File: eicar.com

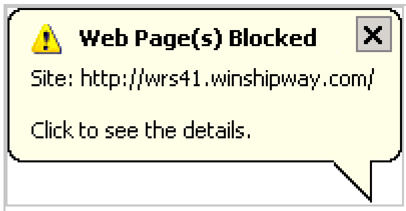
Click to see the details.

If the user clicks on the message, a dialog with detailed information about anti-malware events is displayed:



| Date Time | Security Th... | Infected File |
|---|---|---|
| 8/12/2015 1:18:37 PM | Eicar_test_file | C:\Workshop_Files\Malware_T |
| 8/12/2015 1:18:37 PM | Eicar_test_file | C:\Workshop_Files\Malware_T |

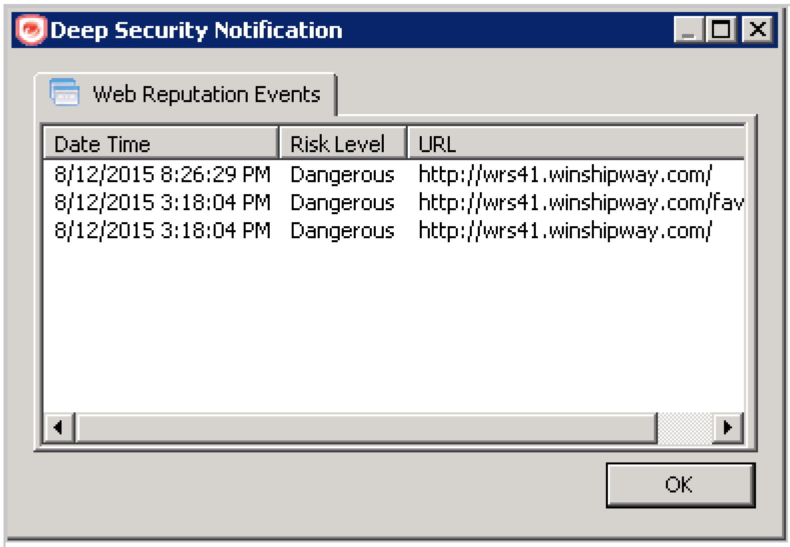
When a malicious web page is blocked, the notification area displays a pop-up message similar to the following:


Web Page(s) Blocked

Site: http://wrs41.winshipway.com/

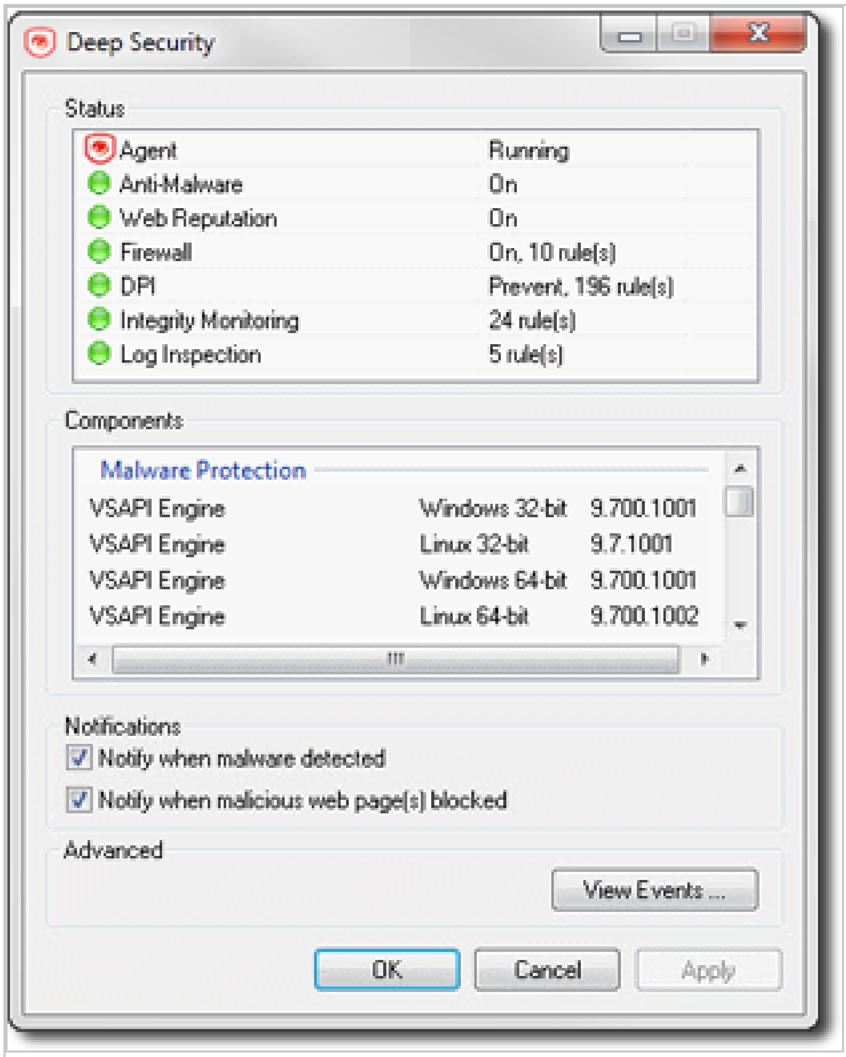
Click to see the details.

If the user clicks on the message, a dialog with detailed information about web reputation events is displayed:



| Date Time | Risk Level | URL |
|---|---|---|
| 8/12/2015 8:26:29 PM | Dangerous | http://wrs41.winshipway.com/ |
| 8/12/2015 3:18:04 PM | Dangerous | http://wrs41.winshipway.com/fav |
| 8/12/2015 3:18:04 PM | Dangerous | http://wrs41.winshipway.com/ |

The notifier also provides a console utility for viewing the current protection status and component information, including pattern versions. The console utility allows the user to turn on and off the popup notifications and access detailed event information.



Deep Security

Status

| | |
|---|---|
| Agent | Running |
| ● Anti-Malware | On |
| ● Web Reputation | On |
| ● Firewall | On, 10 rule(s) |
| ● DPI | Prevent, 196 rule(s) |
| ● Integrity Monitoring | 24 rule(s) |
| ● Log Inspection | 5 rule(s) |

Components

Malware Protection

| | | |
|---|---|---|
| VSAPI Engine | Windows 32-bit | 9.700.1001 |
| VSAPI Engine | Linux 32-bit | 9.7.1001 |
| VSAPI Engine | Windows 64-bit | 9.700.1001 |
| VSAPI Engine | Linux 64-bit | 9.700.1002 |

Notifications

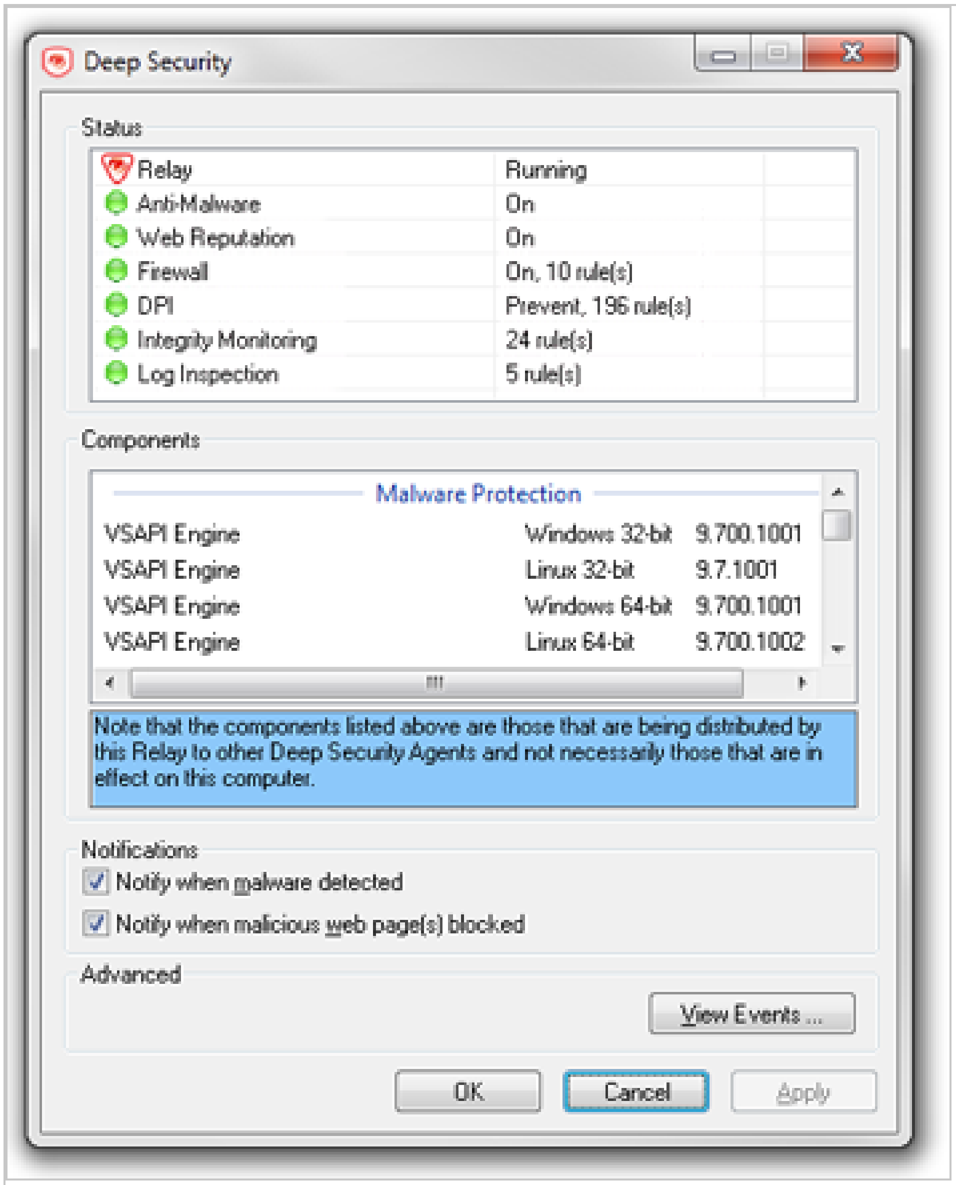
☑ Notify when malware detected

☑ Notify when malicious web page(s) blocked

Advanced

You can also turn off pop-up notifications for certain computers or for computers that are assigned a particular policy by going to the Deep Security Manager **Computer/Policy editor > Settings > General** and settings **Suppress all pop-up notifications on host** to **Yes**. The messages still appear as alerts or events in Deep Security Manager.

When the notifier is running on a computer hosting Deep Security Relay, the notifier's display shows the components being distributed by the relay and not the components that in effect on the computer.



Status

| | |
|---|---|
| Relay | Running |
| ● Anti-Malware | On |
| ● Web Reputation | On |
| ● Firewall | On, 10 rule(s) |
| ● DPI | Prevent, 196 rule(s) |
| ● Integrity Monitoring | 24 rule(s) |
| ● Log Inspection | 5 rule(s) |

Components

Malware Protection

| | | |
|---|---|---|
| VSAPI Engine | Windows 32-bit | 9.700.1001 |
| VSAPI Engine | Linux 32-bit | 9.7.1001 |
| VSAPI Engine | Windows 64-bit | 9.700.1001 |
| VSAPI Engine | Linux 64-bit | 9.700.1002 |

Note that the components listed above are those that are being distributed by this Relay to other Deep Security Agents and not necessarily those that are in effect on this computer.

Notifications

☑ Notify when malware detected

☑ Notify when malicious web page(s) blocked

Advanced

## Trigger a manual scan on Windows OS

If an agent is enabled to trigger a manual scan in the notifier application, the notifier console includes a panel titled **Scan**. The notifier uses the scan configuration assigned from the **Computer** editor or the **Policy** editor, in the editor's Anti-Malware tab, in the General horizontal tab, in the **Manual Scan** section. For details, see Create or edit a malware scan configuration.

A scan cannot be triggered:

- When the agent is being upgraded.
- When there is an ongoing server-side scan already taking place.
- If the scan configuration is empty.

To start a manual scan by the agent on Windows OS:

1. In the **Scan** panel, click **Scan**.
2. Select the folders to scan and click **Scan**:
    - For a Full Scan, select **This PC** to start a scan of all files.
    - For a Custom Scan, select one or more files or folders to start a scan.

Once the scan is completed, the Scan Result displays the number of detected malware items. To view details of these items, click **View Events** in the notifier's **Advanced** panel.

An ongoing scan is halted if it has been triggered on a computer that is not available. For example, the user logs out of the computer after the scan has been started.

# Manage users

## Add and manage users

Deep Security has users, roles, and contacts that can be created and managed under **Administration > User Management**.

- **Users** are Deep Security account holders who can sign in to the Deep Security Manager with a unique user name and password. You can "Synchronize users with an Active Directory" below or "Add or edit an individual user" on the next page
- **Roles** are a collection of permissions to view data and perform operations within Deep Security Manager. Each user is assigned a role. See "Define roles for users" on page 1415.
- **Contacts** do not have a user account and cannot sign in to Deep Security Manager but they can be designated as the recipients of email notifications and scheduled reports. See "Add users who can only receive reports" on page 1430.

### Synchronize users with an Active Directory

If you use Active Directory to manage users, you can synchronize Deep Security with the Active Directory to populate the user list. Users can then sign into Deep Security Manager using the password stored in the directory.

To successfully import an Active Directory user account into Deep Security as a Deep Security user or contact, the Active Directory user account must have a **userPrincipalName** attribute value. The **userPrincipalName** attribute corresponds to an Active Directory account holder's User logon name.

If you are using Deep Security in FIPS mode, you must import the Active Directory's SSL certificate before synchronizing with the Directory. See "Manage trusted certificates" on page 1525.

1. In Deep Security Manager go to **Administration > User Management > Users**.
2. Click **Synchronize with Directory** to open the **Synchronize with Directory** dialog.
3. Type the address of the directory server.
4. Enter your access credentials, which should at a minimum have the Active Directory READ permission. Note that members of the Domain User group have READ permissions by default.
5. Click **Next** to trigger an attempt to connect to the Active Directory.
6. Use the next dialog to enter an Active Directory group name or part of a group name into the search field, and then press enter. Move the group to the **Groups to synchronize** pane using the **>>** button.

The imported list of users are locked out of the Deep Security Manager by default. You have to modify their properties to allow them to sign in to the Deep Security Manager.

If you delete a user from Deep Security Manager who was added as a result of synchronizing with an Active Directory and then resynchronize with the directory, the user will reappear in your user list if they are still in the Active Directory.

## Add or edit an individual user

1. In Deep Security Manager go to **Administration > User Management > Users**.
2. Click **New** to add a new user or double-click an existing user account to edit its settings.
3. Specify the general properties for the user, including:
   - **Username:** The username that the user will enter on the Deep Security Manager login screen.
   - **Password** and **Confirm Password:** Note the password requirements listed in the dialog box. You can password requirements in the user security settings (see "Enforce user password rules" on page 1519).
   - **Name:** (Optional) The name of the account holder.

- **Description:** (Optional) A description of the account.
- **Role:** Use the list to assign a predefined role to this user. You can also assign a role to a user from the Users list, by right-clicking a user and then clicking **Assign roles**.

  Deep Security Manager is preconfigured with two roles: Full Access and Auditor. The Full Access role grants users all possible privileges for managing the Deep Security system, such as creating, editing, and deleting computers, computer groups, policies, rules, and so on. The auditor role gives users the ability to view all of the information in the Deep Security system but not the ability to make any modifications except to their personal settings (password, contact information, view preferences, and so on). Roles with various levels of system access rights can be created and modified on the Roles page or by selecting **New** in the **Role** list.

- **Language:** The language that will be used in the interface when this user logs in.
- **Time zone:** Time zone where the user is located. This time zone is used when displaying dates and times in the Deep Security Manager.
- **Time format:** Time format used to display time in the Deep Security Manager. You can use 12-hour or 24-hour format.
- **Password never expires:** When this option is selected, the user's password will never expire. Otherwise, it will expire as specified in the user security settings (see "Enforce user password rules" on page 1519).

4. If you want to enable multi-factor authentication (MFA), click **Enable MFA**. If MFA is already enabled for this user, you can select **Disable MFA** to disable it. For details, see "Set up multi-factor authentication" on page 1521.
5. Click the **Contact information** tab and enter any contact information that you have for the user and also indicate if they are your primary contact or not. You can also check the **Receive Alert Emails** check box to include this user in the list of users who receive email notifications when alerts are triggered.
6. You can also edit the settings on the **Settings** tab. However, increasing some of these values will affect Deep Security Manager performance. If you make changes and aren't happy with the results, you can click **Reset to Default Settings** (at the bottom of the tab) to reset all settings on this page to their default values:

   **Module**

   - **Hide Unlicensed Modules:** This setting determines whether unlicensed modules will be hidden rather than simply grayed out for this User. This option can be set globally on the **Administration > System Settings > Advanced** tab.

### Refresh Rate

- **Status Bar:** This setting determines how often the status bar of the Deep Security Manager refreshes during various operations such as discovering or scanning computers.
- **Alerts List/Summary:** How often to refresh the data on the **Alerts** page in the **List** view or **Summary** view.
- **Computers List:** How often to refresh the data on the **Computers** page.

  The **Last Successful Update** column value is not recalculated unless the page is manually reloaded.

- **Computer Details:** The frequency with which an individual computer's property page refreshes itself with the latest information (if required).

### List Views

- **Remember last Tag filter on each page:** Events pages let you filter displayed events by tags. This List Views setting determines if the Tag filter setting is retained when you navigate away from and return to an **Events** page.
- **Remember last Time filter on each page:** Events pages let you filter displayed events by time period and computers. These List Views settings determine if the Period and Computer filter settings are retained when you navigate away from and return to an **Events** page.
- **Remember last Computer filter on each page:** Events pages let you filter displayed events by time period and computers. These List Views settings determine if the Period and Computer filter settings are retained when you navigate away from and return to an **Events** page.
- **Remember last Advanced Search on each page:** If you have performed an Advanced Search on an **Events** page, this setting determines whether or not the search results are kept if you navigate away and then return to the page.
- **Number of items to show on a single page:** Screens that display lists of items display a certain number of items per Page. To view the next page, you must use the pagination controls. Use this setting to change the number of list items displayed per page.
- **Maximum number of items to retrieve from database:** This setting limits the number of items that can retrieved from the database for display. This prevents the possibility of

Deep Security Manager getting bogged down trying to display an excessive number of results from a database query. If a query produces more than this many results, a message appears at the top of the display informing you that only a portion of the results are being displayed.

**Note:** Increasing these values affects the Deep Security Manager performance.

**Reports**

- **Enable PDF Encryption:** When this option is selected, reports exported in PDF format are password-protected with the **Report Password**.

## Change a user's password

To change a user's password, click **Administration > User Management > Users**, right-click the user, and click **Set Password**. You will be prompted for the old password as well as the new password.

## Lock out a user or reset a lockout

If a user enters the wrong password too many times when trying to sign in, they will be locked out automatically. If you have resolved the situation and want to allow the user the log in, see "Unlock a locked out user name" on page 1432.

## View system events associated with a user

To see any system events associated with a user, click **Administration > User Management > Users**, right-click the user, and click **View System Events**.

## Delete a user

To remove a user account from Deep Security Manager, click **Administration > User Management > Users**, click the user, and then click **Delete**.

If you delete a user from Deep Security Manager who was added as a result of synchronizing with an Active Directory and then resynchronize with the directory, the user will reappear in your user list if they are still in the Active Directory.

# Define roles for users

Deep Security uses role-based access control (RBAC) to restrict user permissions to parts of Deep Security. Access rights and editing privileges are attached to roles and not to users. Once you have installed Deep Security Manager, you should create individual accounts for each user and assign each user a role that will restrict their activities to all but those necessary for the completion of their duties. To change the access rights and editing privileges of an individual user, you must assign a different role to the user or edit the role.

The access that roles have to computers and policies can be restricted to subsets of computers and policies. For example, users can be permitted to view all existing computers, but only permitted to modify those in a particular group.

Deep Security has two preconfigured roles:

- **Full Access:** The full access role grants the user all possible privileges in terms of managing the Deep Security system including creating, editing, and deleting computers, computer groups, policies, rules, malware scan configurations, and others.
- **Auditor:** The auditor role gives the user the ability to view all the information in the Deep Security system but without the ability to make any modifications except to their own personal settings, such as password, contact information, dashboard layout preferences, and others.

Depending on the level of access granted, controls in Deep Security Manager could be visible and modifiable, visible but disabled, or invisible (hidden). For a list of the rights granted in the preconfigured roles, as well as the default rights settings when creating a new role, see "Default settings for full access, auditor, and new roles" on page 1422.

You can create new roles that can restrict users from editing or even seeing Deep Security objects such as specific computers, the properties of security rules, or the system settings.

Before creating user accounts, identify the roles that your users will take, then itemize to which Deep Security objects those roles will require access and what the nature of that access should be (viewing, editing, creating, and so on). After you have created roles, you can start creating user accounts and assigning them specific roles.

> **Note:** Do not create a new role by duplicating and then modifying the full access role. To ensure that a new role only grants the rights you intend, create the new role by clicking **New** in the toolbar. The rights for a new role are set at the most restrictive settings by default. You can

then proceed to grant only the rights that are required. If you duplicate the full access role and then apply restrictions, you risk granting some rights that you did not intend.

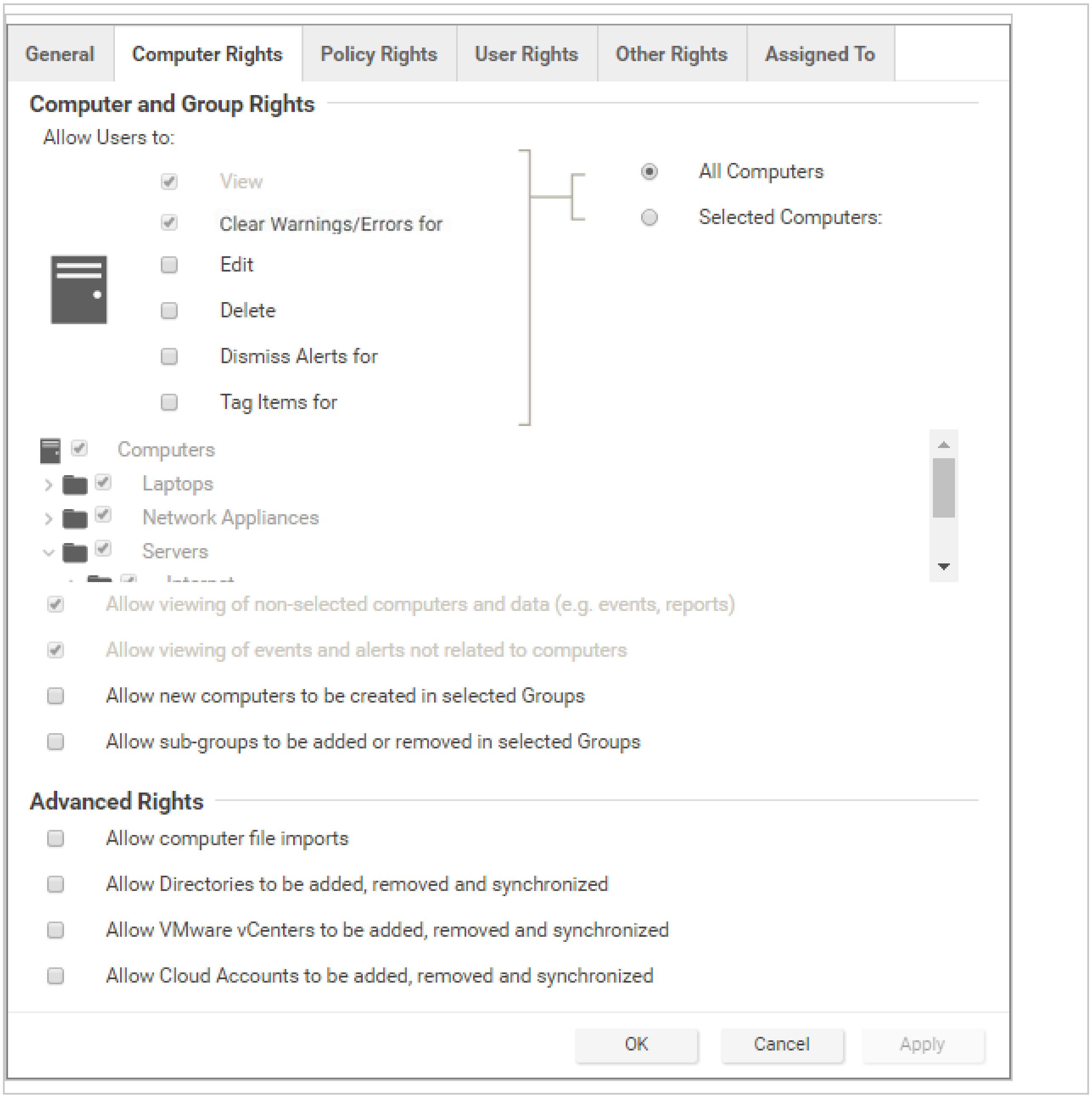
Clicking **New** ( ) or **Properties** ( ) displays the **Role Properties** dialog with six tabs: **General, Computer Rights, Policy Rights, User Rights, Other Rights,** and **Assigned To**.

## Add or edit a role

1. In Deep Security Manager, navigate to **Administration > User Management > Roles**.
2. Click **New** to add a new role or double-click an existing role to modify its settings.
3. Specify the general properties for the role, including the following:
    - **Name**: Supply a name of the role, which will appear on the **Roles** page and in the list of available roles when adding a user.
    - **Description**: Describe the role (optional).
    - **Access Type**: Select whether users with this role will have access to Deep Security Manager, the Deep Security Manager Web service API (applies to the legacy SOAP and REST APIs, which you can enable through **Administration > System Settings > Advanced > SOAP Web Service API**), or both.
    - **Migrate to Trend Vision One Endpoint Security**: Define whether users with this role will have access to Trend Vision One Endpoint Security link, process migration tasks, or both.
    - **Authentication**: Define whether the users with this role will authenticate via a standard or RADIUS-based authentication method. If it is the latter, you need to create a RADIUS configuration to be assigned to the role. This configuration must have a name, a communication server name and port number, and a shared secret defined.
4. Use the **Computer Rights** pane to confer viewing, editing, deleting, warnings and errors clearing, alerts dismissal, event tagging rights to users in a role. These rights can apply to all computers and computer groups or they can be restricted to specific computers. To restrict access, select the type of action the users are allowed to perform. If the action applies to **Selected Computers** only, then select the computer groups and computers to which users in this role will have access.

   These rights restrictions affect not only the user's access to computers in Deep Security Manager, but also what information is visible, including events and alerts. In addition, email notifications will only be sent if they relate to data to which the user has access rights.

Note that when the rights to clear warnings and errors are granted, the role is considered as an editor, not a viewer.



**Computer and Group Rights**

Allow Users to:

☑ View

☑ Clear Warnings/Errors for

□ Edit

□ Delete

□ Dismiss Alerts for

□ Tag Items for

● All Computers

○ Selected Computers:

☑ Computers

☑ Laptops

☑ Network Appliances

☑ Servers

☑ Allow viewing of non-selected computers and data (e.g. events, reports)

☑ Allow viewing of events and alerts not related to computers

□ Allow new computers to be created in selected Groups

□ Allow sub-groups to be added or removed in selected Groups

**Advanced Rights**

□ Allow computer file imports

□ Allow Directories to be added, removed and synchronized

□ Allow VMware vCenters to be added, removed and synchronized

□ Allow Cloud Accounts to be added, removed and synchronized

Four basic options are available:

- **Allow viewing of non-selected computers and data:** If users in this role have restricted edit, delete, or dismiss-alerts rights, you can still allow them to view but not change information about other computers by checking this box.

- **Allow viewing of events and alerts not related to computers:** Set this option to allow users in this role to view non-computer-related information (for example, system events, like users being locked out, new firewall rules being created, IP Lists being deleted, and so on)

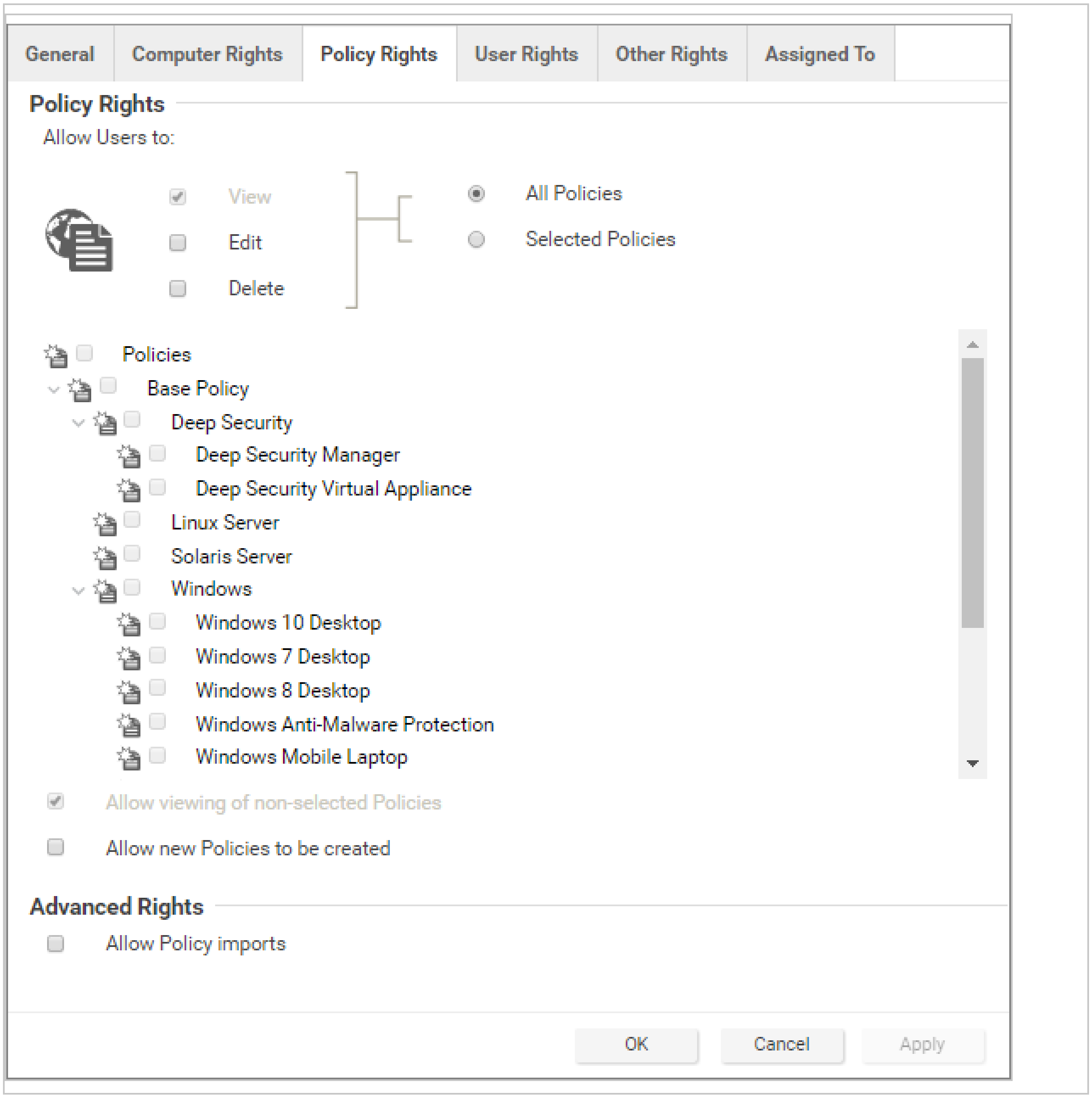
  > **Note:** The previous two settings affect the data that users have access to. Although the ability of a user to make changes to computers have been restricted, these two settings control whether they can see information relating to computers they don't otherwise have access to. This includes receiving email notifications related to those computers.

- **Allow new computers to be created in selected Groups:** Set this option to allow users in this role to create new computers in the computer groups they have access to.
- **Allow sub-groups to be added/removed in selected Groups:** Set this option to allow users in this role to create and delete subgroups within the computer groups to which they have access.

You can also enable these in the **Advanced Rights** section:

- **Allow computer file imports:** Allow Users in this Role to import computers using files created using the Deep Security Manager's **Computer Export** option.
- **Allow Directories to be added, removed and synchronized:** Allow Users in this Role to add, remove, and synchronize computers that are being managed using an LDAP-based directory like MS Active Directory.
- **Allow VMware vCenters to be added, removed and synchronized:** Allow Users in this Role to add, remove and synchronize VMware vCenters.
- **Allow Cloud Providers to be added, removed, and synchronized:** Allow Users in this Role to add, remove, and synchronize Cloud Providers.

5. Use the **Policy Rights** tab to confer viewing, editing, and deleting rights to users in a role. These rights can apply to all policies or they can be restricted to only certain policies. If you wish to restrict access, click **Selected Policies** and put select the policies to which users in this role will have access.



Policy Rights

Allow Users to:

☑ View
□ Edit
□ Delete

● All Policies
○ Selected Policies

□ Policies
- □ Base Policy
  - □ Deep Security
    - □ Deep Security Manager
    - □ Deep Security Virtual Appliance
  - □ Linux Server
  - □ Solaris Server
  - □ Windows
    - □ Windows 10 Desktop
    - □ Windows 7 Desktop
    - □ Windows 8 Desktop
    - □ Windows Anti-Malware Protection
    - □ Windows Mobile Laptop

☑ Allow viewing of non-selected Policies

□ Allow new Policies to be created

Advanced Rights

□ Allow Policy imports

When you allow rights to a policy that has child policies, users automatically get rights to the child policies.

Two basic options are available:

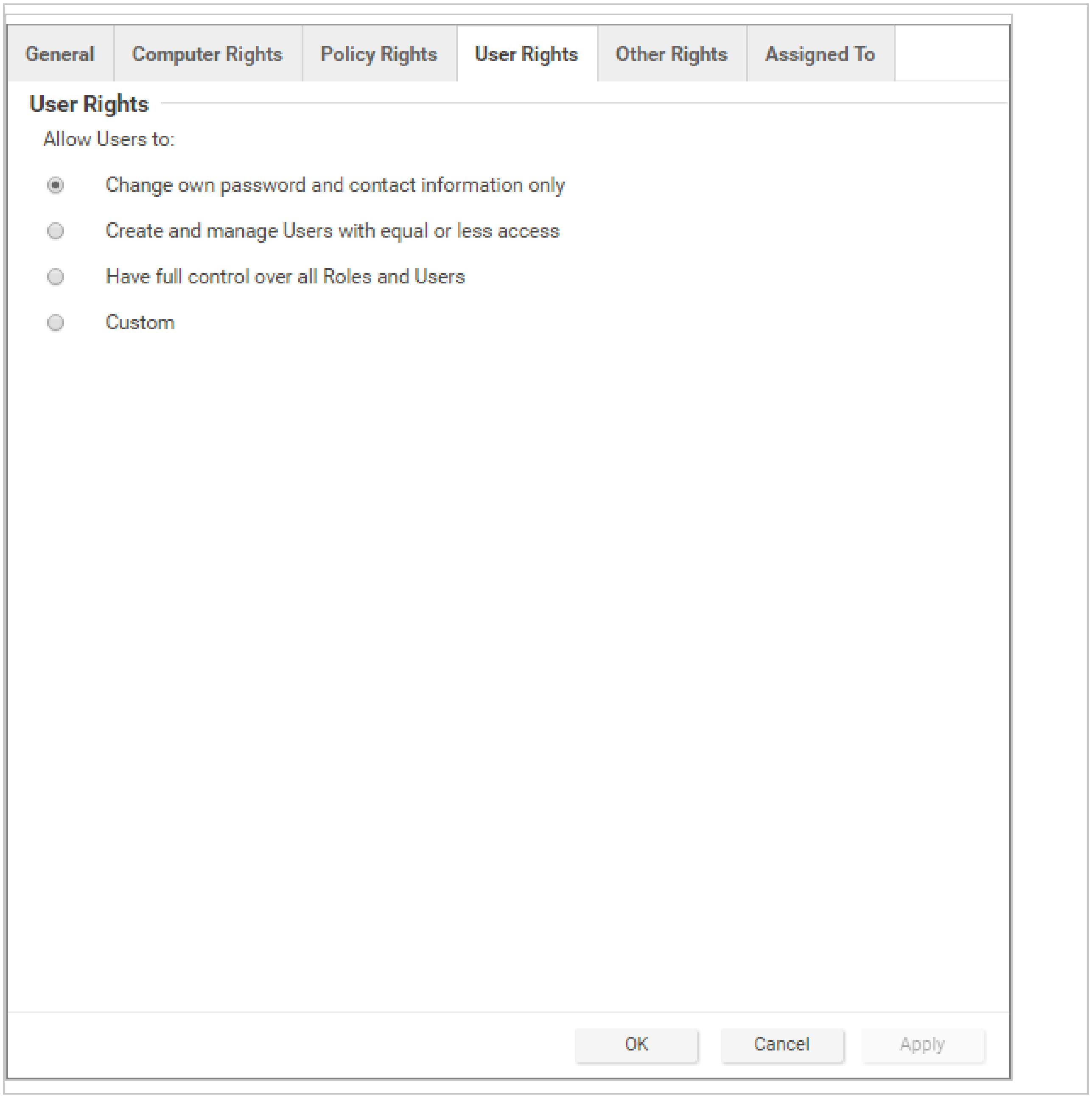
- **Allow viewing of non-selected Policies:** If users in this role have restricted edit or delete rights, you can still allow them to view, but not modify information about other policies.

- **Allow new Policies to be created:** Lets users in this role create new policies.

You can also enable the following in the **Advanced Rights** section:

- **Allow Policy imports:** Allow users in this role to import policies using files created with the Deep Security Manager **Export** option on the **Policies** tab.

6. The options on the **User Rights** tab allow you to define permissions for administrator accounts.



User Rights

Allow Users to:

● Change own password and contact information only

○ Create and manage Users with equal or less access

○ Have full control over all Roles and Users

○ Custom

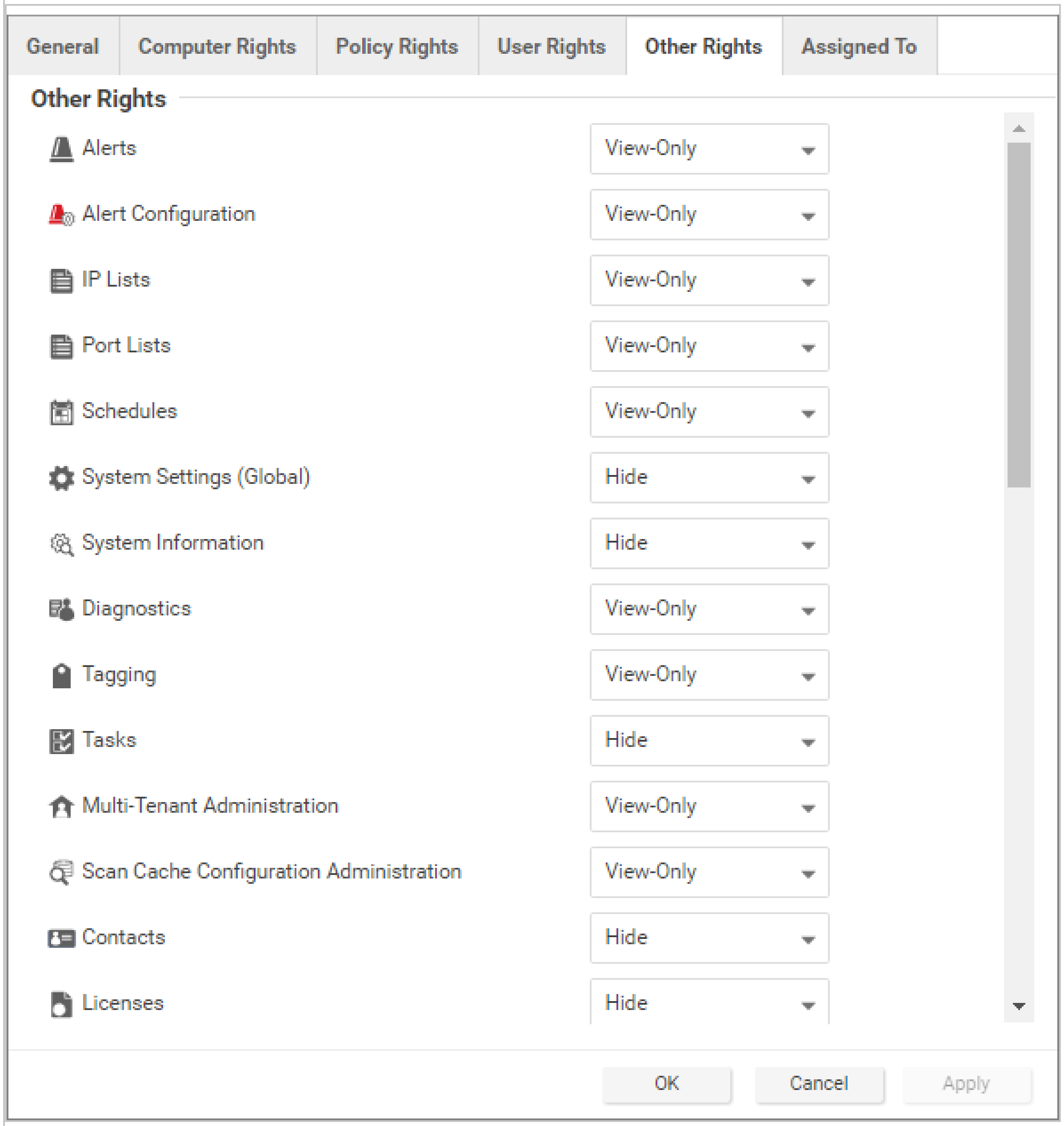
- **Change own password and contact information only:** Users in this role can change their own password and contact information only.
- **Create and manage Users with equal or less access:** Users in this role can create and manage any users who do not have any privileges greater than theirs. If there is even a single privilege that exceeds those of the users with this role, the users with this role will not be able to create or manage them.
- **Have full control over all Roles and Users:** Gives users in this role the ability to create and edit and users or roles without restrictions. Be careful when using this option. If you assign it to a role, you may give a user with otherwise restricted privileges the ability to create and then sign in as a user with full unrestricted access to all aspects of the Deep Security Manager.
- **Custom:** You can further restrict the ability of a user to view, create, edit, or delete users and roles by selecting **Custom** and using the options in the **Custom Rights** section. Some options may be restricted for certain users if the **Can only manipulate Users with equal or lesser rights** option is selected.

  The **Can only manipulate Users with equal or lesser rights** option limits the authority of users in this role. They will only be able to effect changes to users that have equal or lesser rights than themselves. Users in this Role will not be able to create, edit, or delete roles. Selecting this option also places restrictions on some of the options in the **Custom Rights** section:

  - **Can Create New Users:** Can only create users with equal or lesser rights.
  - **Can Edit User Properties:** Can only edit a user (or set or reset password) with equal or lesser rights.
  - **Can Delete Users:** Can only delete users with equal or lesser rights.

7. The **Other Rights** tab enables you to restrict roles' permissions so that they can only access specific Deep Security features, and sometimes specific actions with those features. This can be useful if, for example, you have a team of administrators, and you want to make sure that they don't accidentally overwrite each others' work. By default, roles are **View Only** or **Hide** for each feature. To allow to full control or customized access, select **Custom** from the

list.



Other Rights

| | |
|---|---|
| Alerts | View-Only |
| Alert Configuration | View-Only |
| IP Lists | View-Only |
| Port Lists | View-Only |
| Schedules | View-Only |
| System Settings (Global) | Hide |
| System Information | Hide |
| Diagnostics | View-Only |
| Tagging | View-Only |
| Tasks | Hide |
| Multi-Tenant Administration | View-Only |
| Scan Cache Configuration Administration | View-Only |
| Contacts | Hide |
| Licenses | Hide |

8. The **Assigned To** tab displays a list of the users who have been assigned this role. If you want to test that roles are working correctly, sign in as a newly created user and verify the functionality.

## Default settings for full access, auditor, and new roles

The following table identifies the default rights settings for the full access role and the auditor role. Also listed are the rights settings that are in place when creating a new role by clicking **New** in the toolbar on the **Roles** page.

| RIGHTS | SETTINGS BY ROLE | | |
|---|---|---|---|
| **General** | **Full Access Role** | **Auditor Role** | **New Role Defaults** |
| **Access to DSM User Interface** | Allowed | Allowed | Allowed |
| **Access to Web Service API** | Allowed | Allowed | Not allowed |
| **Computer Rights** | Full Access Role | Auditor Role | New Role Defaults |
| **View** | Allowed, All Computers | Allowed, All Computers | Allowed, All Computers |
| **Clear Warnings/Errors for** | Allowed, All Computers, | Not allowed, All Computers | Not allowed, All Computers |
| **Edit** | Allowed, All Computers | Not allowed, All Computers | Not allowed, All Computers |
| **Delete** | Allowed, All Computers | Not allowed, All Computers | Not allowed, All Computers |
| **Dismiss Alerts for** | Allowed, All Computers | Not allowed, All Computers | Not allowed, All Computers |
| **Tag Items for** | Allowed, All Computers | Not allowed, All Computers | Not allowed, All Computers |
| **Allow viewing of non-selected computers and data (e.g. events, reports)** | Allowed | Allowed | Allowed, All Computers |
| **Allow viewing of events and alerts not related to computers** | Allowed | Allowed | Allowed, All Computers |

| RIGHTS | SETTINGS BY ROLE | | |
|---|---|---|---|
| **Allow new computers to be created in selected Groups** | Allowed | Not allowed | Not allowed |
| **Allow sub-groups to be added or removed in selected Groups** | Allowed | Not allowed | Not allowed |
| **Allow computer file imports** | Allowed | Not allowed | Not allowed |
| **Allow Cloud Accounts to be added, removed and synchronized** | Allowed | Not allowed | Not allowed |
| **Policy Rights** | Full Access Role | Auditor Role | New Role Defaults |
| **View** | Allowed, All Policies | Allowed, All Policies | Allowed, All Policies |
| **Edit** | Allowed, All Policies | Not allowed, All Policies | Not allowed, All Policies |
| **Delete** | Allowed, All Policies | Not allowed, All Policies | Not allowed, All Policies |
| **View non-selected Policies** | Allowed | Allowed | Allowed |
| **Create new Policies** | Allowed | Not allowed | Not allowed |
| **Import Policies** | Allowed | Not allowed | Not allowed |
| **User Rights (See note on User rights below)** | Full Access Role | Auditor Role | New Role Defaults |

| RIGHTS | SETTINGS BY ROLE | | |
|---|---|---|---|
| **View Users** | Allowed | Allowed | Not allowed |
| **Create Users** | Allowed | Not allowed | Not allowed |
| **Edit User Properties** | Allowed | Not allowed | Not allowed |
| **Delete Users** | Allowed | Not allowed | Not allowed |
| **View Roles** | Allowed | Allowed | Not allowed |
| **Create Roles** | Allowed | Not allowed | Not allowed |
| **Edit Role Properties** | Allowed | Not allowed | Not allowed |
| **Delete Roles** | Allowed | Not allowed | Not allowed |
| **Delegate Authority** | Allowed | Not allowed | Not allowed |
| **Other Rights** | Full Access Role | Auditor Role | New Role Defaults |
| **Alerts** | Full (Can Dismiss Global Alerts) | View-Only | View-Only |
| **Alert Configuration** | Full (Can Edit Alert Configurations) | View-Only | View-Only |
| **IP Lists** | Full (Can Create, Edit, Delete) | View-Only | View-Only |
| **Port Lists** | Full (Can Create, Edit, Delete) | View-Only | View-Only |
| **Schedules** | Full (Can Create, Edit, Delete) | View-Only | View-Only |
| **System Settings (Global)** | Full (Can View, Edit System Settings (Global)) | Hide | Hide |
| **Diagnostics** | Full (Can Create Diagnostic Packages) | View-Only | View-Only |

| RIGHTS | SETTINGS BY ROLE | | |
|---|---|---|---|
| **Tagging** | Full (Can Tag (Items not belonging to Computers), Can Delete Tags, Can Update Non-Owned Auto-Tag Rules, Can Run Non-Owned Auto-Tag Rules, Can Delete Non-Owned Auto-Tag Rules) | View-Only | View-Only |
| **Tasks** | Full (Can View, Add, Edit, Delete Tasks, Execute Tasks) | Hide | Hide |
| **Multi-Tenant Administration** | Full | Hide | Hide |
| **Scan Cache Configuration Administration** | Full | View-Only | View-Only |
| **Contacts** | Full (Can View, Create, Edit, Delete Contacts) | Hide | Hide |
| **Licenses** | Full (Can View, Change License) | Hide | Hide |
| **Updates** | Full (Can Add, Edit, Delete Software; Can View Update For Components; Can Download, Import, Apply Update Components; Can Delete Deep Security Rule Updates) | Hide | Hide |
| **Asset Values** | Full (Can Create, Edit, Delete Asset Values) | View-Only | View-Only |
| **Certificates** | Full (Can Create, Delete SSL Certificates) | View-Only | View-Only |
| **Relay Groups** | Full | View-Only | View-Only |
| **Proxy** | Full | View-Only | View-Only |
| **SAML Identity Providers** | Full | Hide | Hide |

| RIGHTS | SETTINGS BY ROLE | | |
|---|---|---|---|
| **Malware Scan Configuration** | Full (Can Create, Edit, Delete Malware Scan Configuration) | View-Only | View-Only |
| **Quarantined File** | Full (Can Delete, Download Quarantined File) | View-Only | View-Only |
| **Web Reputation Configuration** | Full | View-Only | View-Only |
| **Directory Lists** | Full (Can Create, Edit, Delete) | View-Only | View-Only |
| **File Lists** | Full (Can Create, Edit, Delete) | View-Only | View-Only |
| **File Extension Lists** | Full (Can Create, Edit, Delete) | View-Only | View-Only |
| **Firewall Rules** | Full (Can Create, Edit, Delete Firewall Rules) | View-Only | View-Only |
| **Firewall Stateful Configurations** | Full (Can Create, Edit, Delete Firewall Stateful Configurations) | View-Only | View-Only |
| **Intrusion Prevention Rules** | Full (Can Create, Edit, Delete) | View-Only | View-Only |
| **Application Types** | Full (Can Create, Edit, Delete) | View-Only | View-Only |
| **MAC Lists** | Full (Can Create, Edit, Delete) | View-Only | View-Only |
| **Contexts** | Full (Can Create, Edit, Delete) | View-Only | View-Only |
| **Integrity Monitoring Rules** | Full (Can Create, Edit, Delete) | View-Only | View-Only |
| **Log Inspection Rules** | Full (Can Create, Edit, Delete) | View-Only | View-Only |
| **Log Inspection Decoders** | Full (Can Create, Edit, Delete) | View-Only | View-Only |
| **Application Control** | Full (Can Create, View, Edit, or | Hide | Hide |

| RIGHTS | SETTINGS BY ROLE | | |
|---|---|---|---|
| **Rulesets** | Delete Application Control rulesets) | | |
| **Application Control Rule** | Full (Can Create, View, Edit, or Delete Application Control rules) | Hide | Hide |
| **Application Control Unrecognized Software** | Full (Can View or Allow/Block unrecognized software) | Hide | Hide |
| **Application Control Software Inventory** | Full (Can Create, View, or Delete software inventory) | Hide | Hide |

The custom settings corresponding to the **Change own password and contact information only** option are listed in the following table.

| Custom settings for Change own password and contact information only option | |
|---|---|
| Users | |
| **Can View Users** | Not allowed |
| **Can Create New Users** | Not allowed |
| **Can Edit User Properties (User can always edit select properties of own account)** | Not allowed |
| **Can Delete Users** | Not allowed |
| Roles | |
| **Can View Roles** | Not allowed |
| **Can Create New Roles** | Not allowed |
| **Can Edit Role Properties (Warning: conferring this right will let Users with this Role edit their own rights)** | Not allowed |
| **Can Delete Roles** | Not allowed |
| Delegate Authority | |

| Custom settings for Change own password and contact information only option | |
|---|---|
| **Can only manipulate Users with equal or lesser rights** | Not allowed |

The custom settings corresponding to the **Create and manage Users with equal or less access** option are listed in the following table.

| Custom settings for Create and manage users with equal or less access option | |
|---|---|
| Users | |
| **Can View Users** | Allowed |
| **Can Create New Users** | Allowed |
| **Can Edit User Properties (User can always edit select properties of own account)** | Allowed |
| **Can Delete Users** | Allowed |
| Roles | |
| **Can View Roles** | Not allowed |
| **Can Create New Roles** | Not allowed |
| **Can Edit Role Properties (Warning: conferring this right will let Users with this Role edit their own rights)** | Not allowed |
| **Can Delete Roles** | Not allowed |
| Delegate Authority | |
| **Can only manipulate Users with equal or lesser rights** | Allowed |

The custom settings corresponding to the **Have full control over all Roles and Users** option are listed in the following table.

| Custom settings for Have full control over all Roles and Users option | |
|---|---|
| Users | |
| **Can View Users** | Allowed |
| **Can Create New Users** | Allowed |
| **Can Edit User Properties (User can always edit select properties of own account)** | Allowed |
| **Can Delete Users** | Allowed |
| Roles | |
| **Can View Roles** | Allowed |
| **Can Create New Roles** | Allowed |
| **Can Edit Role Properties (Warning: conferring this right will let Users with this Role edit their own rights)** | Allowed |
| **Can Delete Roles** | Allowed |
| Delegate Authority | |
| **Can only manipulate Users with equal or lesser rights** | Not applicable |

## Add users who can only receive reports

"Contacts" are users who cannot sign in to the Deep Security Manager but can periodically be sent reports (using scheduled tasks). Contacts can be assigned a "clearance" level that maps to existing roles. When a contact is sent a report, the report will not contain any information not accessible to a user of the same level. For example, three contacts may each be listed as the recipients of a weekly summary report but the contents of the three reports could be entirely different for each contact depending on their computer rights.

### Add or edit a contact

1. In Deep Security Manager go to **Administration > User Management > Contacts**.
2. Click **New** to add a new contact or double-click an existing contact to edit its settings.

3. In the **General Information** section, specify the name, description, and preferred language of this contact.
4. In the **Contact Information** section, enter the email address to which reports will be sent if this contact is included in a report distribution list. (See the **Reports** page for more information.)
5. In the **Clearance** section, specify the role that determines the information this contact will be allowed to see. For example, if a computer report has been scheduled to be sent to this contact, only information on the computers that his role permits him access to will be included in the report.
6. In the **Password Protected Reports** section, select **Reports generated by this user are password protected** to password-protect exported PDF reports with the **Report Password**.

## Delete a contact

To remove a contact from Deep Security Manager, click **Administration > User Management > Contacts**, click the contact, and then click **Delete**.

# Create an API key for a user

To use the Deep Security Manager API, you will need an API key.

**Note:** API keys can only be used with the new"Use the Deep Security API to automate tasks" on page 1598 available in Deep Security Manager 11.1 and later.

**Note:** Trend Micro recommends creating one API key for every user needing API access to the Deep Security Manager.

**Tip:** You can automate API key creation using the Deep Security API. For examples, see the Create and Manage API Keys guide in the Deep Security Automation Center.

To create a new API key:

1. Go to **Administration > User Management > API Keys**.
2. Click **New**.
3. In the Properties window, enter a **Name** and **Description** for the API key.
4. Click on the **Role** list and select a role. **Auditor** grants read-only access to the Deep Security Manager through the API, while **Full Access** grants both read and write access. If you need more specific roles for API key users, you can select **New** and define one. See "Define roles for users" on page 1415 for more information on doing so.

5. Select a **Language**.
6. Select a **Time Zone**.
7. Optionally select **Expires on** and select an expiry date for the API key.
8. Click **OK**.
9. Copy the **Secret key value**.

> **Note:** Make sure to copy the secret key value now, this is the only time it will be shown.

## Lock out an existing API key

If an existing API key has been compromised you can lock it out:

1. Double click on the API key you want to lock out.
2. Optionally select **Locked Out (Denied permission to authenticate)** to block usage of the API key.
3. Click **OK**.

# Unlock a locked out user name

If you have attempted to sign in multiple times to Deep Security Manager with an incorrect password, your user account will be locked out. The number of sign-in attempts allowed before lock out is configured in **Administration > System Settings > Security > Number of incorrect sign-in attempts allowed (before lock out)**.

You can unlock users in different ways, depending on the following situations:

- If an administrator user is available, see "Unlock users as an administrator" below.
- If all the administrative users are locked out, see "Unlock administrative users from a command line" on the next page.

## Unlock users as an administrator

1. Log in to Deep Security Manager with a working administrator user name and password.
2. Go to **Administration > User Management > Users**. Select the user you want to unlock, right-click, and click **Properties**.
3. In the wizard, go to **General > Sign-In Credentials**. Deselect the **Locked Out (Denied permission to sign in)** check box.
4. Click **Save**.

## Unlock administrative users from a command line

1. Go to your local command line interface.

   If your Deep Security Manager is Windows, go to the `..\Program Files\Trend Micro\Deep security Manager` directory.

   If your Deep Security Manager is Linux, go to the `/opt/dsm` directory.

2. Enter the following command:

   ```
   dsm_c -action unlockout -username <username>
   ```

# Implement SAML single sign-on (SSO)

## About SAML single sign-on (SSO)

To implement SAML single sign-on, see "Configure SAML single sign-on" on page 1435 or "Configure SAML single sign-on with Microsoft Entra ID" on page 1442.

### What are SAML and single sign-on?

Security Assertion Markup Language (or SAML) is an open authentication standard that allows for the secure exchange of user identity information from one party to another. SAML supports single sign-on, a technology that allows for a single user login to work across multiple applications and services. For Deep Security, implementing SAML single sign-on means that users signing in to your organization's portal would be able to seamlessly sign in to Deep Security without an existing Deep Security account.

### How SAML single sign-on works in Deep Security

**Establishing a trust relationship**

In SAML single sign-on, a trust relationship is established between two parties: the identity provider and the service provider. The identity provider has the user identity information stored on a directory server. The service provider (which in this case is Deep Security) uses the identity provider's user identities for its own authentication and account creation.

The identity provider and the service provider establish trust by exchanging a SAML metadata document.

> **Note:** Currently, Deep Security supports only the HTTP POST binding of the SAML 2.0 identity provider (IdP)-initiated login flow, and not the service provider (SP)-initiated login flow.

### Creating Deep Security accounts from user identities

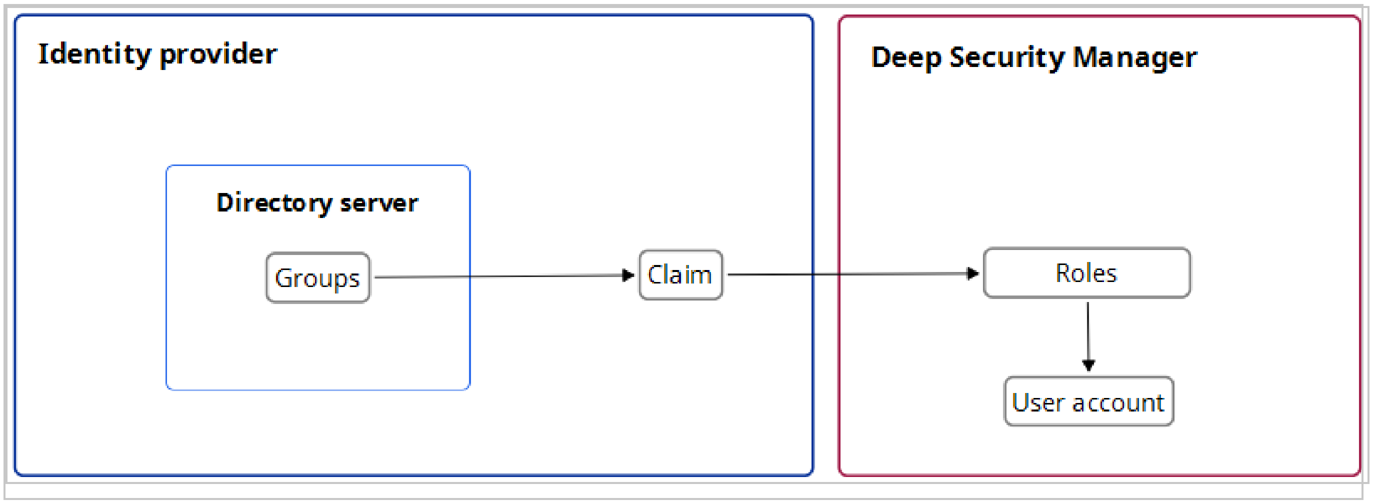
Once Deep Security and the identity provider have exchanged SAML metadata documents and established a trust relationship, Deep Security can access the user identities on the identity provider's directory server. However, before Deep Security can actually create accounts from the user identities, account types need to be defined and instructions for transforming the data format need to be put in place. This is done using groups, roles, and claims.

Groups and roles specify the tenant and access permissions for a Deep Security user account. Groups are created on the identity provider's directory server. The identity provider assigns user identities to one or more of the groups. Roles are created in the Deep Security Manager. There must be both a group and a role for each Deep Security account type, and their access permissions and tenant assignment must match.

Once there are matching groups and roles for each user type, the group data format needs to be transformed into a format Deep Security can understand. This is done by the identity provider with a claim. The claim contains instructions for transforming the group data format into the matching Deep Security role.

See also "SAML claims structure" on page 1438.

The following diagram depicts this process:



#### Implement SAML single sign-on in Deep Security

Once trust has been established between Deep Security and an identity provider with a SAML metadata document exchange, matching groups and roles have been created, and a claim put in place to translate the group data into roles, Deep Security can use SAML single sign-on to automatically make Deep Security accounts for users signing in through your organization's portal.

For more information on implementing SAML single sign-on, see "Configure SAML single sign-on" below.

## Configure SAML single sign-on

When you configure Deep Security to use SAML single sign-on (SSO), users signing in to your organization's portal can seamlessly sign in to Deep Security without an existing Deep Security account. SAML single sign-on also makes it possible to implement user authentication access control features such as:

- Password strength or change enforcement.
- One-Time Password (OTP).
- Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA).

For a more information on the Deep Security's implementation of the SAML standard, see "About SAML single sign-on (SSO)" on page 1433. If you are using Microsoft Entra ID as your identity provider, see "Configure SAML single sign-on with Microsoft Entra ID" on page 1442.

> **Note:** Currently, Deep Security supports only the HTTP POST binding of the SAML 2.0 identity provider (IdP)-initiated login flow, and not the service provider (SP)-initiated login flow

To use SAML single sign-on with Deep Security, you need to do the following:

1. "Configure pre-setup requirements" on the next page
2. "Configure Deep Security as a SAML service provider" on the next page
3. "Configure SAML in Deep Security" on page 1437
4. "Provide information for your identity provider administrator" on page 1437
5. "SAML claims structure" on page 1438
6. "Test SAML single sign-on" on page 1441
7. "Service and identity provider settings" on page 1441

## Configure pre-setup requirements

1. Ensure your Deep Security Manager is functioning properly.
2. Contact the identity provider administrator to:
   - Establish a naming convention for mapping directory server groups to Deep Security roles.
   - Obtain their identity provider SAML metadata document.
   - Ask them to add any required user authentication access control features to their policy.

Support is available to assist with the following identity providers that have been tested in Deep Security with SAML single sign-on:

- Active Directory Federation Services (ADFS)
- Okta
- PingOne
- Shibboleth
- Microsoft Entra ID

## Configure Deep Security as a SAML service provider

First, set up Deep Security as a service provider.

> **Note:** In multi-tenant Deep Security installations, only the primary tenant administrator can configure Deep Security as a SAML service provider.

1. In Deep Security Manager, go to **Administration > User Management > Identity Providers > SAML**.
2. Click **Get Started**.
3. Enter an **Entity ID** and a **Service Name**, and then click **Next.**

   > **Note:** The **Entity ID** is a unique identifier for the SAML service provider. The SAML specification recommends that the entity ID is a URL that contains the domain name of the entity, and industry practices use the SAML metadata URL as the entity ID. The SAML metadata is served from the /saml endpoint on the Deep Security Manager, so an example value might be `https://<DSMServerIP:4119>/saml`.

4. Select a certificate option, and click **Next**. The SAML service provider certificate is not used at this time, but would be used in the future to support service-provider-initiated login or single sign-out features. You can import a certificate by providing a PKCS #12 keystore file and password, or create a new self-signed certificate.

5. Follow the steps until you are shown a summary of your certificate details and then click **Finish**.

## Configure SAML in Deep Security

### Import your identity provider's SAML metadata document

> **Note:** Your Deep Security account must have both administrator and "Create SAML identity provider" permissions.

1. On the Administration page, go to **User Management > Identity Providers > SAML**.
2. Click **Get Started**.
3. Click **Choose File**, select the SAML metadata document provided by your identity provider, and click **Next**.

4. Enter a **Name** for the identity provider, and then click **Finish**.

   You will be brought to the Roles page.

### Create Deep Security roles for SAML users

You need to create a role for each of your expected user types. Each role must have a corresponding group in your identity provider's directory server, and match the group's access permissions and tenant assignment.

Your identity provider's SAML integration will have a mechanism to transform group membership into SAML claims. Consult the documentation that came with your identity provider to learn more about claim rules.

For information on how to create roles, see "Define roles for users" on page 1415.

## Provide information for your identity provider administrator

### Download the Deep Security Manager service provider SAML metadata document

1. On the Administration page, go to **User Management > Identity Providers > SAML**.
2. Under SAML Service Provider, click **Download**.
   Your browser will download the Deep Security service provider SAML metadata document (`ServiceProviderMetadata.xml`).

#### Send URNs and the Deep Security SAML metadata document to the identity provider administrator

You need to give the identity provider administrator Deep Security's service provider SAML metadata document, the identity provider URN and the URN of each Deep Security role you created.

> Tip:
> To view role URNs, go to **Administration > User Management > Roles** and look under the URN column.
>
> To view identity provider URNs, go to **Administration > User Management > Identity Providers > SAML > Identity Providers** and look under the URN column.

Once the identity provider administrator confirms they have created groups corresponding to the Deep Security roles and any required rules for transforming group membership into SAML claims, you are done with configuring SAML single sign-on.

> **Note:** If necessary, you can inform the identity provider administrator about the "SAML claims structure" below required by Deep Security.

### SAML claims structure

The following SAML claims are supported by Deep Security:

- "Deep Security user name (required)" below
- "Deep Security user role (required)" on the next page
- "Maximum session duration (optional)" on page 1440
- "Preferred language (optional)" on page 1440

#### Deep Security user name (required)

The claim must have a SAML assertion that contains an `Attribute` element with a `Name` attribute of `https://deepsecurity.trendmicro.com/SAML/Attributes/RoleSessionName` and a single `AttributeValue` element. The Deep Security Manager will use the `AttributeValue` as the Deep Security user name.

## Sample SAML data (abbreviated)

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
```

```
    <AttributeStatement>
      <Attribute
Name="https://deepsecurity.trendmicro.com/SAML/Attributes/RoleSessionName">
        <AttributeValue>alice</AttributeValue>
      </Attribute>
    </AttributeStatement>
  </Assertion>
</samlp:Response>
```

### Deep Security user role (required)

The claim must have a SAML assertion that contains an `Attribute` element with a `Name` attribute of `https://deepsecurity.trendmicro.com/SAML/Attributes/Role` and between one and ten `AttributeValue` elements. The Deep Security Manager uses the attribute value(s) to determine the tenant, identity provider, and role of the user. A single assertion may contain roles from multiple tenants.

> **Note:** The AttributeValue contains **two** URNs, separated by a comma. The URNs are case sensitive.

## Sample SAML data (abbreviated)

> **Note:** The line break in the `AttributeValue` element is present for readability; in the claim it must be on a single line.

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    <AttributeStatement>
      <Attribute
Name="https://deepsecurity.trendmicro.com/SAML/Attributes/Role">
        <AttributeValue>urn:tmds:identity:[pod ID]:[tenant ID]:saml-
provider/[IDP name],
            urn:tmds:identity:[pod ID]:[tenant ID]:role/[role
name]</AttributeValue>
      </Attribute>
    </AttributeStatement>
  </Assertion>
</samlp:Response>
```

### Maximum session duration (optional)

If the claim has a SAML assertion that contains an `Attribute` element with a `Name` attribute of `https://deepsecurity.trendmicro.com/SAML/Attributes/SessionDuration` and an integer-valued `AttributeValue` element, the session will automatically terminate when that amount of time (in seconds) has elapsed.

## Sample SAML data (abbreviated)

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    <AttributeStatement>
      <Attribute
Name="https://deepsecurity.trendmicro.com/SAML/Attributes/SessionDuration">
        <AttributeValue>28800</AttributeValue>
      </Attribute>
    </AttributeStatement>
  </Assertion>
</samlp:Response>
```

### Preferred language (optional)

If the claim has a SAML assertion that contains an `Attribute` element with the `Name` attribute of `https://deepsecurity.trendmicro.com/SAML/attributes/PreferredLanguage` and a string-valued `AttributeValue` element that is equal to one of the supported languages, the Deep Security Manager will use the value to set the user's preferred language.

The following languages are supported:

- `en-US` (US English)
- `ja-JP` (Japanese)

## Sample SAML data (abbreviated)

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    <AttributeStatement>
      <Attribute
Name="https://deepsecurity.trendmicro.com/SAML/Attributes/PreferredLanguag
e">
```

```
        <AttributeValue>en-US</AttributeValue>
      </Attribute>
    </AttributeStatement>
  </Assertion>
</samlp:Response>
```

## Test SAML single sign-on

Navigate to the single sign-on login page on the identity provider server, and log in to the Deep Security Manager from there. You should be redirected to the Deep Security Manager console. If SAML single sign-on is not functioning, follow the steps below:

### Review the set-up

1. Review the "Configure pre-setup requirements" on page 1436 section.
2. Ensure that the user is in the correct directory group.
3. Ensure that the identity provider and role URNs are properly configured in the identity provider federation service.

### Create a Diagnostic Package

1. Go to **Administration > System Information** and click **Diagnostic Logging**.
2. Select **SAML integration Issues** and click **Save**.
3. Generate logs. Replicate the issue by logging in to the Deep Security Manager through your identity provider.
4. After the login fails, generate a diagnostic package by navigating to **Administration > System Information** and clicking on **Create Diagnostic Package**.
5. Once the diagnostic package has been created, navigate to *https://success.trendmicro.com* to open a Technical Support Case, and upload the diagnostic package during the case creation.

## Service and identity provider settings

You can set how far in advance Deep Security will alert you to the expiry date of the server and identity provider certificates, as well as how much time must pass before inactive user accounts added through SAML single sign-on are automatically deleted.

To change these settings, go to **Administration > System Settings > Security > Identity Providers**.

# Configure SAML single sign-on with Microsoft Entra ID

For a detailed explanation of Deep Security's implementation of the SAML standard, see "About SAML single sign-on (SSO)" on page 1433. For instructions on configuring it with other identity providers, see "Configure SAML single sign-on" on page 1435.

**Note:** Currently, Deep Security supports only the HTTP POST binding of the SAML 2.0 identity provider (IdP)-initiated login flow, and not the service provider (SP)-initiated login flow.

## Who is involved in this process?

Typically, there are two people required to configure Deep Security Manager to use Microsoft Entra ID for SAML single sign-on (SSO): a Deep Security administrator and a Microsoft Entra ID administrator.

The Deep Security administrator must be assigned a Deep Security role with the **SAML Identity Providers** right set to either **Full** or to **Custom** with **Can Create New SAML Identity Providers** enabled.

The following table lists steps that must be performed to set up SAML single sign-on with Deep Security using Microsoft Entra ID.

| Step | Performed by |
|---|---|
| "Configure Deep Security as a SAML service provider" below | Deep Security administrator |
| "Download the Deep Security service provider SAML metadata document" on the next page | Deep Security administrator |
| "Configure Microsoft Entra ID" on the next page | Microsoft Entra ID administrator |
| "Configure SAML in Deep Security" on page 1444 | Deep Security administrator |
| "Define a role in Microsoft Entra ID" on page 1445 | Microsoft Entra ID administrator |

## Configure Deep Security as a SAML service provider

First, set up Deep Security as a service provider.

> **Note:** In multi-tenant Deep Security installations, only the primary tenant administrator can configure Deep Security as a SAML service provider.

1. In Deep Security Manager, go to **Administration > User Management > Identity Providers > SAML**.
2. Click **Get Started**.
3. Enter an **Entity ID** and a **Service Name**, and then click **Next.**

   > **Note:** The **Entity ID** is a unique identifier for the SAML service provider. The SAML specification recommends that the entity ID is a URL that contains the domain name of the entity, and industry practices use the SAML metadata URL as the entity ID. The SAML metadata is served from the /saml endpoint on the Deep Security Manager, so an example value might be `https://<DSMServerIP:4119>/saml`.

4. Select a certificate option, and click **Next**. The SAML service provider certificate is not used at this time, but would be used in the future to support service-provider-initiated login or single sign-out features. You can import a certificate by providing a PKCS #12 keystore file and password, or create a new self-signed certificate.
5. Follow the steps until you are shown a summary of your certificate details and then click **Finish**.

## Download the Deep Security service provider SAML metadata document

In Deep Security Manager, go to **Administration > User Management > Identity Providers > SAML** and click **Download**.

The file is downloaded as `ServiceProviderMetadata.xml`. Send it to your Microsoft Entra ID administrator.

## Configure Microsoft Entra ID

The following steps are performed by a Microsoft Entra ID administrator. For more information, see Configure single sign-on to non-gallery applications in Microsoft Entra ID.

1. In the Microsoft Entra ID portal, add a new non-gallery application.
2. Configure single sign-on for the application. You should upload the `ServiceProviderMetadata.xml` metadata file that was downloaded from Deep Security Manager. Alternatively, you can enter a reply URL (the Deep Security Manager URL + `/saml`).

3. Configure SAML claims. Deep Security requires the following two claims:

   - `https://deepsecurity.trendmicro.com/SAML/Attributes/RoleSessionName` This is a unique user ID that will be the username in Deep Security. For example, you could use the User Principal Name (UPN).
   - `https://deepsecurity.trendmicro.com/SAML/Attributes/Role`
     The format is "IDP URN,Role URN". The IDP has not been created in Deep Security Manager yet, so you can configure this SAML claim later, in "Define a role in Microsoft Entra ID" on the next page.

   You can also configure other optional claims, as described in "SAML claims structure" on the next page.

4. Download the **Federation Metadata XML** file and send it to the Deep Security administrator.

If there are multiple roles defined in Deep Security, repeat these steps to create a separate application for each role.

## Configure SAML in Deep Security

### Import the Microsoft Entra ID metadata document

1. In Deep Security Manager, go to **Administration > User Management > Identity Providers > SAML**.
2. Click **Get Started** or **New**.
3. Click **Choose File**, select the Federation Metadata XML file that was downloaded from Microsoft Entra ID and click **Next**.
4. Enter a **Name** for the identity provider, and then click **Finish**.

You will be brought to the **Roles** page.

### Create Deep Security roles for SAML users

Make sure the **Administration > User Management > Roles** page in Deep Security contains appropriate roles for your organization. Users should be assigned a role that limits their activities to only those necessary for the completion of their duties. For information on how to create roles, see "Define roles for users" on page 1415. Each Deep Security role requires a corresponding Microsoft Entra ID application.

### Get URNs

In Deep Security Manager, gather the following information. You will have to provide it to your Microsoft Entra ID administrator.

- The identity provider URN. To view identity provider URNs, go to **Administration > User Management > Identity Providers > SAML > Identity Providers** and check the URN column.
- The URN of the Deep Security role to associate with the Microsoft Entra ID application. To view role URNs, go to **Administration > User Management > Roles** and check the URN column. If you have multiple roles, you will need the URN for each role, because each one requires a separate Microsoft Entra ID enterprise application.

## Define a role in Microsoft Entra ID

This must be performed by a Microsoft Entra ID administrator.

In Microsoft Entra ID, use the identity provider URN and role URN identified in the previous section to define the role attribute in the enterprise application. This must be in the format "IDP URN,Role URN". See "Deep Security user role (required)" in the "SAML claims structure" below section.

Use the Validate button in Microsoft Entra ID to test the setup, or assign the new application to a user and test that it works.

## Service and identity provider settings

You can set how far in advance Deep Security will alert you to the expiry date of the server and identity provider certificates, as well as how much time must pass before inactive user accounts added through SAML single sign-on are automatically deleted.

To change these settings, go to **Administration > System Settings > Security > Identity Providers**.

## SAML claims structure

The following SAML claims are supported by Deep Security:

- "Deep Security user name (required)" on the next page
- "Deep Security user role (required)" on the next page

- "Maximum session duration (optional)" on the next page
- "Preferred language (optional)" on the next page

### Deep Security user name (required)

The claim must have a SAML assertion that contains an `Attribute` element with a `Name` attribute of `https://deepsecurity.trendmicro.com/SAML/Attributes/RoleSessionName` and a single `AttributeValue` element. The Deep Security Manager will use the `AttributeValue` as the Deep Security user name.

## Sample SAML data (abbreviated)

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    <AttributeStatement>
      <Attribute
Name="https://deepsecurity.trendmicro.com/SAML/Attributes/RoleSessionName">
        <AttributeValue>alice</AttributeValue>
      </Attribute>
    </AttributeStatement>
  </Assertion>
</samlp:Response>
```

### Deep Security user role (required)

The claim must have a SAML assertion that contains an `Attribute` element with a `Name` attribute of `https://deepsecurity.trendmicro.com/SAML/Attributes/Role` and between one and ten `AttributeValue` elements. The Deep Security Manager uses the attribute value(s) to determine the tenant, identity provider, and role of the user. A single assertion may contain roles from multiple tenants.

**Note:** The AttributeValue contains **two** URNs, separated by a comma. The URNs are case sensitive.

## Sample SAML data (abbreviated)

**Note:** The line break in the `AttributeValue` element is present for readability; in the claim it must be on a single line.

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    <AttributeStatement>
      <Attribute
Name="https://deepsecurity.trendmicro.com/SAML/Attributes/Role">
        <AttributeValue>urn:tmds:identity:[pod ID]:[tenant ID]:saml-
provider/[IDP name],
            urn:tmds:identity:[pod ID]:[tenant ID]:role/[role
name]</AttributeValue>
      </Attribute>
    </AttributeStatement>
  </Assertion>
</samlp:Response>
```

### Maximum session duration (optional)

If the claim has a SAML assertion that contains an `Attribute` element with a `Name` attribute of `https://deepsecurity.trendmicro.com/SAML/Attributes/SessionDuration` and an integer-valued `AttributeValue` element, the session will automatically terminate when that amount of time (in seconds) has elapsed.

## Sample SAML data (abbreviated)

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    <AttributeStatement>
      <Attribute
Name="https://deepsecurity.trendmicro.com/SAML/Attributes/SessionDuration">
        <AttributeValue>28800</AttributeValue>
      </Attribute>
    </AttributeStatement>
  </Assertion>
</samlp:Response>
```

### Preferred language (optional)

If the claim has a SAML assertion that contains an `Attribute` element with the `Name` attribute of `https://deepsecurity.trendmicro.com/SAML/attributes/PreferredLanguage` and a string-valued `AttributeValue` element that is equal to one of the supported languages, the Deep Security Manager will use the value to set the user's preferred language.

The following languages are supported:

- `en-US` (US English)
- `ja-JP` (Japanese)

### Sample SAML data (abbreviated)

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    <AttributeStatement>
      <Attribute
Name="https://deepsecurity.trendmicro.com/SAML/Attributes/PreferredLanguage">
        <AttributeValue>en-US</AttributeValue>
      </Attribute>
    </AttributeStatement>
  </Assertion>
</samlp:Response>
```

# Manage the database

## General database maintenance

To improve Deep Security Manager performance, we recommend that you perform regular index maintenance on the Deep Security database to keep it from becoming overly fragmented. Follow your organization's best practices for reindexing databases, or refer to your database vendor's documentation for guidance:

- **PostgreSQL:** See https://www.postgresql.org/docs/10/sql-reindex.html for details on the PostgreSQL reindex command.
- **Microsoft SQL:** Refer to documentation from Microsoft for index maintenance best practices: https://docs.microsoft.com/en-us/sql/relational-databases/indexes/reorganize-and-rebuild-indexes?view=sql-server-ver15. See also Options in the Back Up Database Task for Maintenance Plan.
- **Oracle Database:** Follow Oracle’s best practices on managing indexes. For example, see https://docs.oracle.com/cd/B28359_01/server.111/b28310/indexes002.htm#ADMIN11713.

There are also open source websites that provide scripts that can help you with this task.

Tip: Reindexing may block some operations, so it's best to run it offline.

## Maintain PostgreSQL

Follow these database maintenance and tuning recommendations:

1. Configure database log rotation and performance settings.

   For best practices, see "Log rotation" on the next page, "Lock management" on page 1451, "Maximum concurrent connections" on page 1451, "Autovacuum settings" on page 1452, etc.

   Steps vary by distribution and managed hosting:

   - **Self-hosted database:** Defaults are generic values from the PostgreSQL core distribution. **Some defaults are not appropriate** for data center or customized cloud installs, especially in larger deployments.

     To change settings:

     - In a plain text editor, open the `postgresql.conf` file.
     - Edit the parameters.
     - Save the file.
     - Restart the PostgreSQL service.
   - **Amazon RDS:** Defaults vary by instance size. Often, you only need to fine tune autovacuuming, `max_connections` and `effective_cache_size`. To change settings, use database parameter groups and then restart the database instance.
   - **Amazon Aurora:** Defaults vary by instance size. Often, you only need to fine tune autovacuuming, `max_connections` and `effective_cache_size`. To change settings, use database parameter groups and then restart the database instance.

   Tip: When fine tuning performance, verify settings by monitoring your database IOPS with a service such as Amazon CloudWatch.

Tip: If you need additional help, PostgreSQL offers professional support.

# Log rotation

In PostgreSQL core distributions, by default, the database's local log file has no age or file size limit. Logs will gradually consume more disk space.

To prevent that, configure parameters for either remote logging to a Syslog `log_destination`, or local log rotation.

Log files can be rotated based on age limit, file size limit, or both (whichever occurs sooner). When a limit is reached, depending on whether a log file exists that matches the file name pattern at that time, PostgreSQL either creates a new file or reuses an existing one. Reuse can either append or (for age limit) overwrite.

Log rotation parameters are:

- `logging_collector`: Enter "on" to enable database logging.
- `log_filename`: Log file name pattern. Patterns mostly use IEEE standard time and date formatting.
- `log_truncate_on_rotation`: Enter either "off" to append to the existing log file, or "on" to overwrite it. Only applies when time-based log rotation occurs. (File size-based log rotation always appends.)
- `log_rotation_age`: Maximum age in minutes of a log file. Enter "0" to disable time-based log rotation.
- `log_rotation_size`: Maximum size in kilobytes (KB) of a log file. Enter "0" to disable file size-based log rotation.

## Example: Daily Database Log Rotation

These parameters create 7 rotating database log files: one for each day of the week . (File names are "postgresql-Mon.log" for Monday, etc.)

Each day (1440 minutes) either creates a file with that day's name (if none exists) or overwrites that day's log file from the previous weekly cycle.

During heavy load, logging can *temporarily exceed disk space quota* because the file size limit is disabled. However the number and names of files does not change.

```
log_collector = on
```

```
log_filename = 'postgresql-%a.log'
```

```
log_rotation_age = 1440
```

```
log_rotation_size = 0
```

```
log_truncate_on_rotation = on
```

## Lock management

Increase `deadlock_timeout` to exceed your deployment's normal transaction time.

Each time a query waits for a lock for more than `deadlock_timeout`, PostgreSQL checks for a deadlock condition and (if configured) logs an error. On larger deployments during heavy load, however, it's often normal (not an error) to wait for more than 1 second. Logging these normal events decreases performance.

## Maximum concurrent connections

Increase to `max_connections = 500`.

## Effective cache size

Consider increasing `effective_cache_size`. This setting is used to estimate cache effects by a query. It only affects cost estimates during query planning, and doesn't cause more RAM usage.

## Shared buffers

Increase `shared_buffers` to 25% of the RAM. This setting specifies how much memory PostgreSQL can use to cache data, which improves performance.

## Work memory and maintenance work memory

Increase `work_mem`. This setting specifies the amount of RAM that can be used by internal sort operations and hash tables before writing to temporary disk files. More memory is required when running complex queries.

Consider increasing `maintenance_work_mem`. This setting determines the maximum amount of memory used for maintenance operations such as `ALTER TABLE`.

## Checkpoints

Reduce checkpoint frequency. Checkpoints usually cause most writes to data files. To optimize performance, most checkpoints should be "timed" (triggered by `checkpoint_timeout`), not "requested" (triggered by filling all the available WAL segments or by an explicit `CHECKPOINT` command).

| Parameter name | Recommended value |
|---|---|
| `checkpoint_timeout` | 15min |
| `checkpoint_completion_target` | 0.9 |
| `max_wal_size` | 16GB |

## Write-ahead log (WAL)

If you use database replication, consider using `wal_level = replica`.

## Autovacuum settings

PostgreSQL requires periodic maintenance called "vacuuming". Usually, you don't need to change the default value for `autovacuum_max_workers`.

On the `entitys` and `attribute2s` tables, if frequent writes cause many rows to change often (such as in large deployments with short-lived cloud instances), then autovacuum should run more frequently to minimize disk space usage and maintain performance. Parameters must be set on both the overall database and those specific tables.

| Database-level parameter name | Recommended value |
|---|---|
| `autovacuum_work_mem` | 1GB |

| Table-level parameter name | Recommended value |
|---|---|
| `autovacuum_vacuum_cost_delay` | 10 |
| `autovacuum_vacuum_scale_factor` | 0.01 |

| Table-level parameter name | Recommended value |
|---|---|
| `autovacuum_analyze_scale_factor` | 0.005 |

To change the database-level setting, you must edit the configuration file or database parameter group, and then reboot the database server. Commands cannot change that setting while the database is running.

To change the table-level settings, you can either edit the configuration file or database parameter group, or enter these commands:

```
ALTER TABLE public.entitys SET (autovacuum_enabled = true, autovacuum_
vacuum_cost_delay = 10, autovacuum_vacuum_scale_factor = 0.01, autovacuum_
analyze_scale_factor = 0.005);
```

```
ALTER TABLE public.attribute2s SET (autovacuum_enabled = true, autovacuum_
vacuum_cost_delay = 10, autovacuum_vacuum_scale_factor = 0.01, autovacuum_
analyze_scale_factor = 0.005);
```

## PostgreSQL on Linux

### Transparent huge pages

Transparent huge pages (THP) is a Linux memory management system that reduces the overhead of translation lookaside buffer (TLB) lookups on computers with large amounts of RAM by using larger memory pages. By default, THP is enabled, but it isn't recommended for PostgreSQL database servers. To disable it, see your OS vendor's documentation.

### Host-based authentication

Host-based authentication (HBA) can prevent unauthorized access to the database from other computers that aren't in the allowed IP address range. By default, Linux doesn't have HBA restrictions for databases. However it's usually better to use a security group or firewall instead.

# Maintain Microsoft SQL Server Express

Follow these database maintenance recommendations:

- Remove any unneeded agent software packages from the Deep Security Manager to save disk space in the database.

- Security updates and events require additional space in the database. Monitor your deployment to ensure that you stay within the Express database size limit. For information on database pruning, see "Log and event storage best practices" on page 1050. You may also choose to use the SQL Server settings described in Considerations for the "autogrow" and "autoshrink" settings in SQL Server.

## Migrate Microsoft SQL Server Express to Enterprise

Microsoft SQL Server Express is supported in very limited deployments (see "Microsoft SQL Server Express considerations" on page 503 for details). If you are using a Microsoft SQL Server Express database but find its limitations too constricting, you can migrate it to Microsoft SQL Server Enterprise edition, or another supported database.

To migrate to Enterprise:

1. Stop the Deep Security Manager service so that it stops writing to the database.

   Deep Security Agents will continue to apply their current protection policies while the manager is stopped. Events will be kept and transmitted when Deep Security Manager returns online.

2. Back up the database(s).

3. Back up the database connection settings file:

   ```
   [Deep Security install directory]/webclient/webapps/ROOT/WEB-INF/dsm.properties
   ```

4. Move the database to the new database engine. Restore the backup.

5. Edit dsm.properties to connect to the migrated database:

   ```
   database.SqlServer.user
   ```

   ```
   database.name
   ```

   ```
   database.SqlServer.instance
   ```

   ```
   database.SqlServer.password
   ```

   ```
   database.type
   ```

   ```
   database.SqlServer.server
   ```

   If using the default instance, you can delete the `database.SqlServer.instance` setting.

You can enter a plain text password for `database.SqlServer.password`; Deep Security Manager will encrypt it when the service starts, like this:

```
database.SqlServer.password=!CRYPT!20DE3D96312D6803A53C0D1C691FE6DEB747
6104C0A
```

6. Restart the Deep Security Manager service.
7. To verify that it has successfully reconnected to the database, log in to Deep Security Manager.

   Existing protected computers and event logs should appear. As new events such as administrator logins or policy changes occur, they should be added. If not, verify that you have granted permissions to the database user account on the new database server.

# Back up and restore your database

Separate from high availability or load balancing, best practices include regular database backups and a disaster recovery plan. Backups can be used to restore the database if there is a serious failure.

## Back up your database

Consult your database vendor's documentation for instructions on how to back up your database.

Tip: For RDS, follow the instructions provided by AWS for backing up your database to an S3 bucket. For example, see Amazon RDS for SQL Server - Support for Native Backup/Restore to Amazon S3.

Tip: For PostgreSQL databases, basic tools like `pg_dump` or `pg_basebackup` are not suitable to back up and restore in an enterprise environment. Consider other tools such as Barman.

## Restore the database only

1. Stop the Deep Security Manager service.
2. Restore the database.
   This must be a database from the same version number of the Deep Security Manager.
3. Start the Deep Security Manager service.

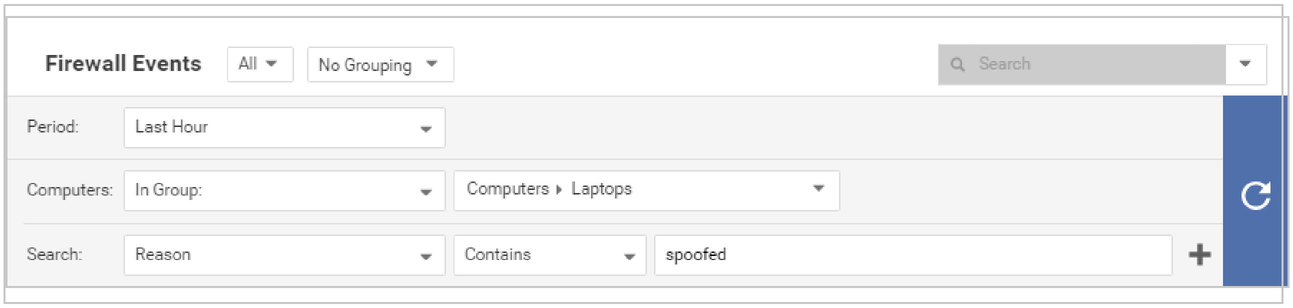
4. Verify contents restored.
5. Update all of the computers to ensure they have the proper configuration.

## Restore both the Deep Security Manager and the database

1. Remove any remnants of the lost or corrupted Deep Security Manager. When uninstalling Deep Security Manager, don't choose to keep configuration files.
2. Restore the database.
3. Find the version of the Deep Security Manager installer that supports your database and install it. During the installation, in the Database options, select the **Add a new Manager node** option.
4. After installing Deep Security Manager successfully, open the Deep Security Manager console, go to **Administration > Manager Nodes**, and decommission the old offline Manager node.

## Export objects in XML or CSV format

- **Events:** Go to one of the Events pages and use the Advanced Search options to filter the event data. For example, you could search for all firewall events for computers in the Computers > Laptops computer group that were logged within the last hour whose reason column contains the word spoofed.

  Firewall Events All No Grouping

  Period: Last Hour

  Computers: In Group: Computers ▸ Laptops

  Search: Reason Contains spoofed

  Click the submit button (with the right-facing arrow) to execute the "query". Then click**Export** to export the filtered data in CSV format. You can export all the displayed entries or just selected data. The exporting of logs in this format is primarily for integration with third-party reporting tools.
- **Computer Lists:** Computers lists can be exported in XML or CSV format from the **Computers** page. You might want to do this if you find you are managing too many computers from a single Deep Security Manager and are planning to set up a second Deep

Security Manager to manage a collection of computers. Exporting a list of selected computers will save you the trouble of rediscovering all of the computers again and arranging them into groups.

> **Note:** Policy, firewall rule, and intrusion prevention rule settings will *not* be included. You will have to export your firewall rules, intrusion prevention rules, firewall stateful configurations, and policies as well and then reapply them to your computers.

- **Policies:** To export these in XML format, go to **Policies**.

  > **Note:** When you export a selected policy to XML, any child policies the policy might have are included in the exported package. The export package contains all of the actual objects associated with the policy except: intrusion prevention rules, log inspection rules, integrity monitoring rules, and application types.

- **Firewall Rules:** Firewall rules can be exported to an XML or CSV file using the same searching and filtering techniques as above.
- **Firewall Stateful Configurations:** Firewall stateful configurations can be exported to an XML or CSV file using the same searching and filtering techniques as above.
- **Intrusion Prevention Rules:** Intrusion prevention rules can be exported to an XML or CSV file using the same searching and filtering techniques as above.
- **Integrity Monitoring Rules:** Integrity monitoring rules can be exported to an XML or CSV file using the same searching and filtering techniques as above.
- **Log Inspection Rules:** Log inspection rules can be exported to an XML or CSV file using the same searching and filtering techniques as above.
- **Other Common Objects :** All the reusable components common objects can be exported to an XML or CSV file the same way.

When exporting to CSV, only displayed column data is included. Use the Columns tool to change which data is displayed. Grouping is ignored so the data might not be in same order as on the screen.

## Import objects

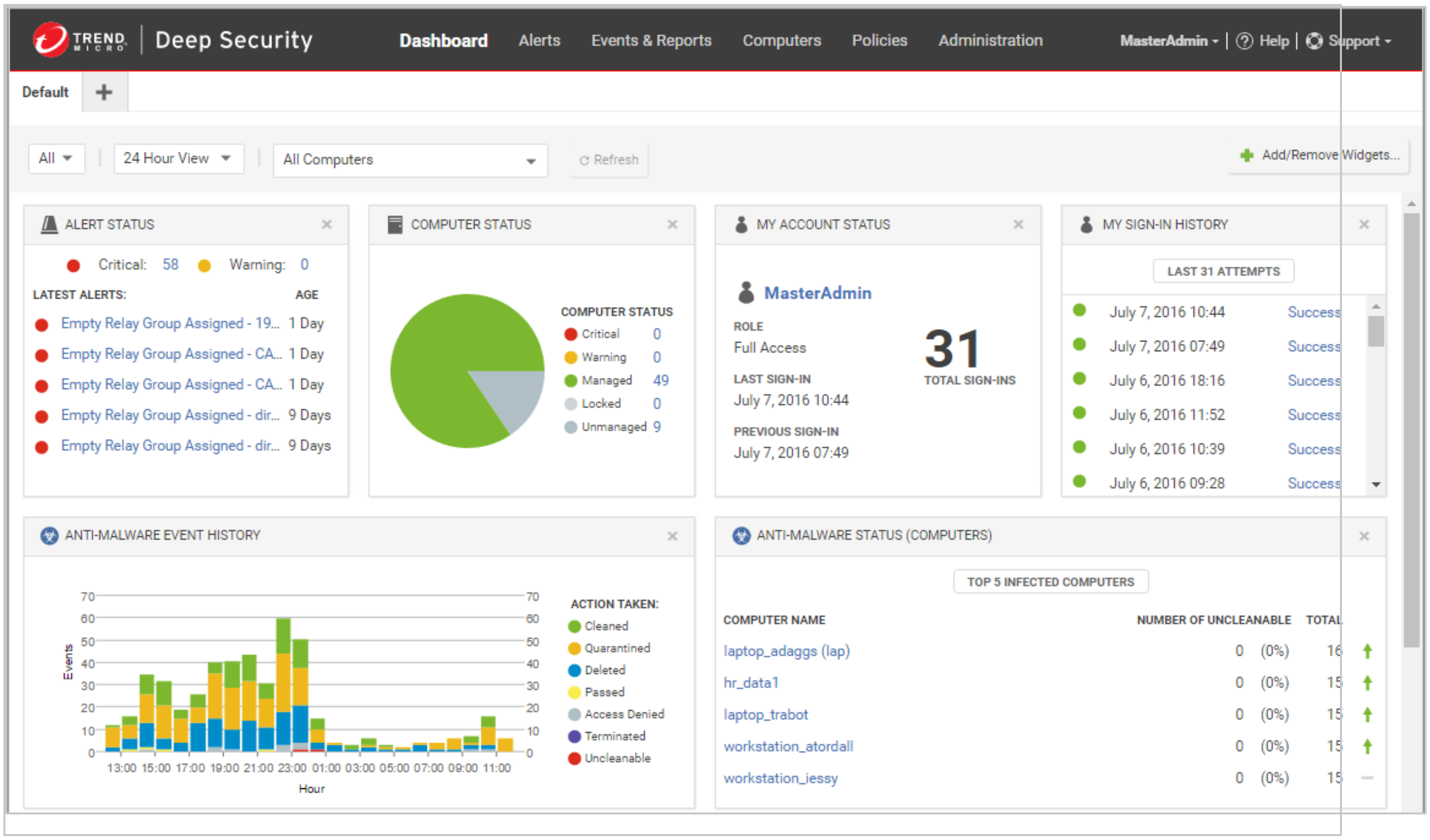
To import each of the individual objects into Deep Security, next to **New** in the object page's toolbar, select **Import From File** .

# Navigate and customize Deep Security Manager

## Customize the dashboard

The dashboard is the first page that appears after you log in to Deep Security Manager.

Each user can customize the contents and layout of their dashboard. Deep Security Manager automatically saves your settings, and will remember your dashboard the next time that you log in. You can also configure the data's time period, and which computer's or computer group's data is displayed.



Critical: 58 Warning: 0

| LATEST ALERTS: | AGE |
|---|---|
| Empty Relay Group Assigned - 19... | 1 Day |
| Empty Relay Group Assigned - CA... | 1 Day |
| Empty Relay Group Assigned - CA... | 1 Day |
| Empty Relay Group Assigned - dir... | 9 Days |
| Empty Relay Group Assigned - dir... | 9 Days |

| COMPUTER STATUS | |
|---|---|
| Critical | 0 |
| Warning | 0 |
| Managed | 49 |
| Locked | 0 |
| Unmanaged | 9 |

MasterAdmin

ROLE
Full Access

LAST SIGN-IN
July 7, 2016 10:44

PREVIOUS SIGN-IN
July 7, 2016 07:49

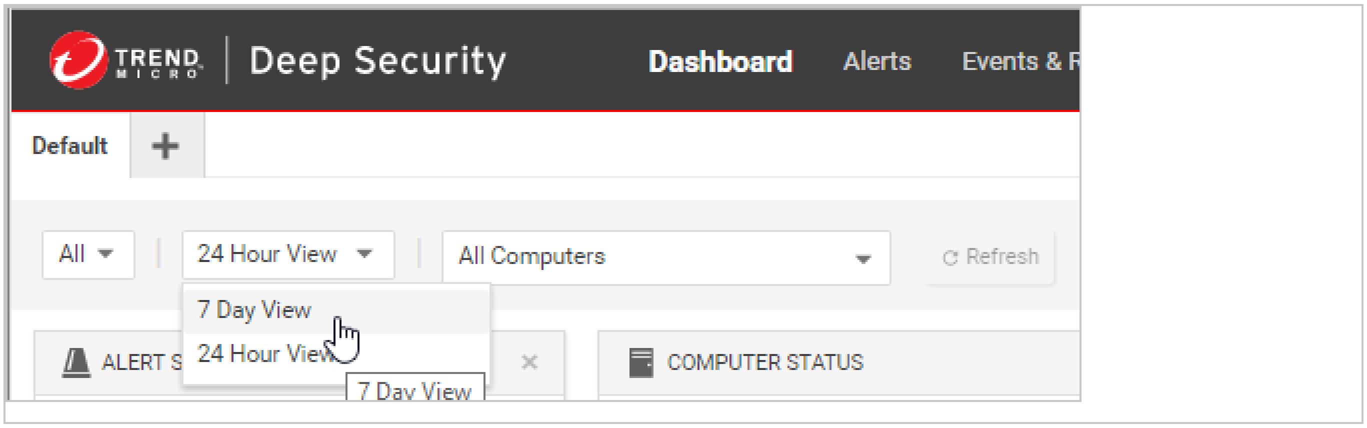
31
TOTAL SIGN-INS

| | |
|---|---|
| July 7, 2016 10:44 | Success |
| July 7, 2016 07:49 | Success |
| July 6, 2016 18:16 | Success |
| July 6, 2016 11:52 | Success |
| July 6, 2016 10:39 | Success |
| July 6, 2016 09:28 | Success |

| COMPUTER NAME | NUMBER OF UNCLEANABLE | | TOTAL |
|---|---|---|---|
| laptop_adaggs (lap) | 0 | (0%) | 16 |
| hr_data1 | 0 | (0%) | 15 |
| laptop_trabot | 0 | (0%) | 15 |
| workstation_atordall | 0 | (0%) | 15 |
| workstation_iessy | 0 | (0%) | 15 |

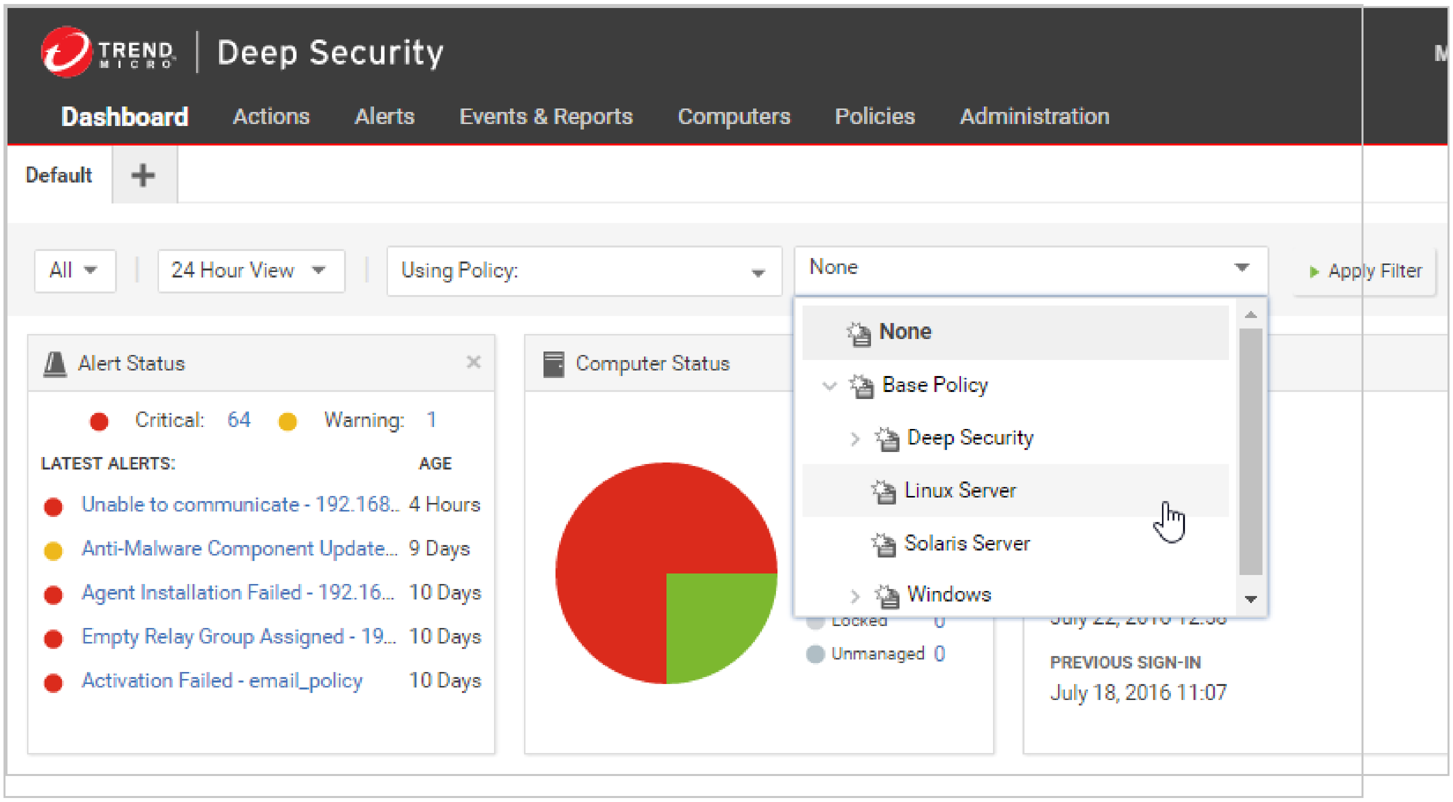
## Specify date and time range

The dashboard can display data from either the last 24 hours or the last seven days, as per the following illustration:



## Specify computers and computer groups

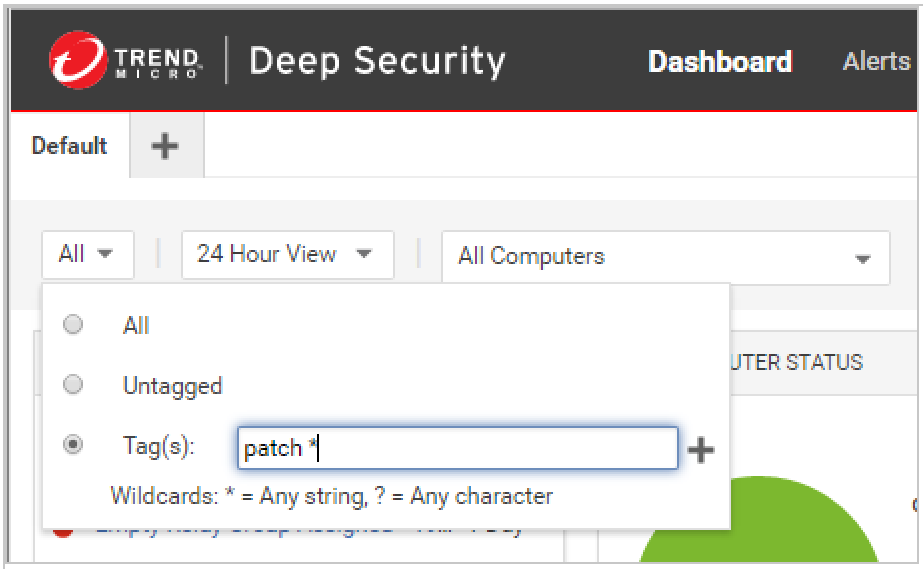
You can use the **Computer** option to filter the displayed data to only data from specific computers. For example, only computers using the **Linux Server** security policy, as per the following illustration:



## Filter by tags

In Deep Security, a tag is a unit of metadata that you can apply to an event in order to create an additional attribute for the event that is not originally contained within the event itself. Tags can be used to filter events to simplify the task of event monitoring and management. A typical use of tagging is to distinguish between events that require action and those that have been investigated and found to be benign.

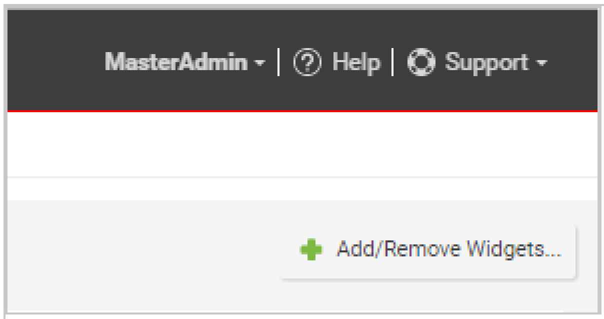
Data displayed in the **Dashboard** can be filtered by tags, as per the following illustration:



For more information, see "Apply tags to identify and group events" on page 1057.

## Select dashboard widgets

Click **Add/Remove Widgets** to display the widget selection window and choose which widgets to display, as per the following illustration:



If widgets take up extra space on the dashboard (more than 1x1), their dimensions are listed next to their names.

The following widgets are available:

## Monitoring:

- **Activity Overview**: Overview of activity, including the number of protected hours and size of database.
- **Alert History [2x1]**: Recent alert history, including the severity of alerts.
- **Alert Status**: Summary of alerts, including their age and severity.
- **Computer Status**: Summary of computers, including whether they are managed or unmanaged, and if there are any warnings or critical alerts.
- **Manager Node Status [3x1]**: The name, CPU usage, memory, jobs, and system events on the manager node.
- **Security Update Status**: The update status of computers, including the number of computers that are up-to-date, out-of-date, and unknown.
- **Tenant Database Usage**: The top five tenants ranked by their database size.
- **Tenant Job Activity**: The top five tenants ranked by their total number of jobs.
- **Tenant Protection Activity**: The top five tenants ranked by the hours they've been protected.
- **Tenant Security Event Activity**: The top five tenants ranked by their total number of security events.
- **Tenant Sign-In Activity**: The top five tenants ranked by their sign-in activity.
- **Tenant System Event Activity**: The top five tenants ranked by their total number of system events.
- **Tenants**: Tenant information, including the number of tenants and the amount of hours they have been protected.

Note that the out-of-date category does not include computers with the status Anti-malware Configuration Off, Anti-malware Engineer Offline, and Agent Offline. These statuses have been separated from the general out-of-date classification and categorized individually as **Out of Date (Anti-Malware Configuration Off)**, **Out of Date (Anti-Malware Offline)**, and **Out of Date (Agent Offline)**. Computers with these statuses are not counted in the total displayed on the **Security Update Status** widget under **Out-of-Date**.

### System:

- **My Sign-in History**: The last 50 sign-in attempts and whether or not they were successful.
- **My User Summary [2x1]**: A summary of the user, including name, role, and sign-in information.
- **Software Updates**: Out-of-date computers.
- **System Event History [2x1]**: Recent system event history, including the number of events that are categorized as info, warning, or error.

### Ransomware:

- **Ransomware Event History [3x1]**: Recent ransomware event history, including the event type.
- **Ransomware Status**: The status of ransomware, including the number of ransomware events that occurred in the last 24 hours, the last 7 days, or the last 13 weeks.

### Anti-Malware:

- **Anti-Malware Event History [2x1]**: Recent anti-malware event history, including the action taken for the events.
- **Anti-Malware Protection Status**: A summary of Anti-Malware Protection status on computers, including whether they are protected, unprotected, or not capable of being protected.
- **Anti-Malware Status (Computers) [2x1]**: The top five infected computers, including the amount of uncleanable files and the total number of files affected.
- **Anti-Malware Status (Malware) [2x1]**: The top five detected malware, including their name, amount of uncleanable files, and number of times it was triggered.
- **Malware scan Status [2x1]**: The top five appliances with incomplete scheduled malware scans.

### Web Reputation:

- **Web Reputation Computer Activity**: The top five computers with Web Reputation events, including the number of events.
- **Web Reputation Event History [2x1]**: Recent Web Reputation event history, including the events severity.

- **Web Reputation URL Activity**: The top five URLs that triggered Web Reputation events, including the number of times they were accessed.

## Firewall:

- **Firewall Activity (Detected)**: The top five reasons packets were detected, including the number of times.
- **Firewall Activity (Prevented)**: The top five reasons packets were prevented, including the number of times.
- **Firewall Computer Activity (Detected)**: The top five computers that generated detected Firewall events and the number of times they occurred.
- **Firewall Computer Activity (Prevented)**: The top five computers that generated prevented Firewall events and the number of times they occurred.
- **Firewall Event History [2x1]**: Recent Firewall event history, including if the events were detected or prevented.
- **Firewall IP Activity (Detected)**: The top five source IPs that generated detected Firewall events and the number of times they occurred.
- **Firewall IP Activity (Prevented)**: The top five source IPs that generated prevented Firewall events and the number of times they occurred.
- **Firewall Port Activity (Detected)**: The top five destination ports for detected Firewall events and the number of times they occurred.
- **Firewall Port Activity (Prevented)**: The top five computers that generated prevented Firewall events and the number of times they occurred.
- **Reconnaissance Scan Activity**: The top five detected reconnaissance scans, including the number of times they occurred.
- **Reconnaissance Scan Computers**: The top five computers where reconnaissance scans occurred and the number of times they occurred.
- **Reconnaissance Scan History [2x1]**: Recent reconnaissance scan history, including the type of scan that occurred.

## Intrusion Prevention:

- **Application Type Activity (Detected)**: The top five detected application types, including the number of times they were triggered.
- **Application Type Activity (Prevented)**: The top five prevented application types, including the number of times they were triggered.

- **Application Type Treemap (Detected) [2x2]**: A map of detected application types. Hover over the boxes to display the severity of the events, the number of times it was triggered, and the percentage for each severity level.
- **Application Type Treemap (Prevented) [2x2]**: A map of prevented application types. Hover over the boxes to display the severity of the events, the number of times it was triggered, and the percentage for each severity level.
- **IPS Activity (Detected):** The top five reasons Intrusion Prevention events were detected, including the number of times it was triggered.
- **IPS Activity (Prevented)**: The top five reasons Intrusion Prevention events were prevented, including the number of times it was triggered.
- **IPS Computer Activity (Detected)**: The top five computers with detected Intrusion Prevention events.
- **IPS Computer Activity (Prevented)**: The top five computers with prevented Intrusion Prevention events.
- **IPS Event History [2x1]**: Recent Intrusion Prevention event history, including if the events were detected or prevented.
- **IPS IP Activity (Detected)**: The top five source IPs that generated detected Intrusion Prevention events.
- **IPS IP Activity (Prevented)**: The top five source IPs that generated prevented Intrusion Prevention events.
- **Latest IPS Activity (Detected)**: The top five reasons Intrusion Prevention events were detected since the latest update.
- **Latest IPS Activity (Prevented)**: The top five reasons Intrusion Prevention events were prevented since the latest update.

## Integrity Monitoring:

- **Integrity Monitoring Activity**: The top five reasons Integrity Monitoring events occurred, including the number of times. In this case, the reason refers to the rule that was triggered.
- **Integrity Monitoring Computer Activity**: The top five computers where Integrity Monitoring events occurred, including the number of events.
- **Integrity Monitoring Event History [2x1]**: Recent Integrity Monitoring event history, including the severity of events.

- **Integrity Monitoring Key Activity**: The top five keys for Integrity Monitoring events. The source of the key varies by Entity Set - for files and directories, it is their path, whereas for ports, it is their unique protocol, IP, port number, or tuple.

### Log Inspection:

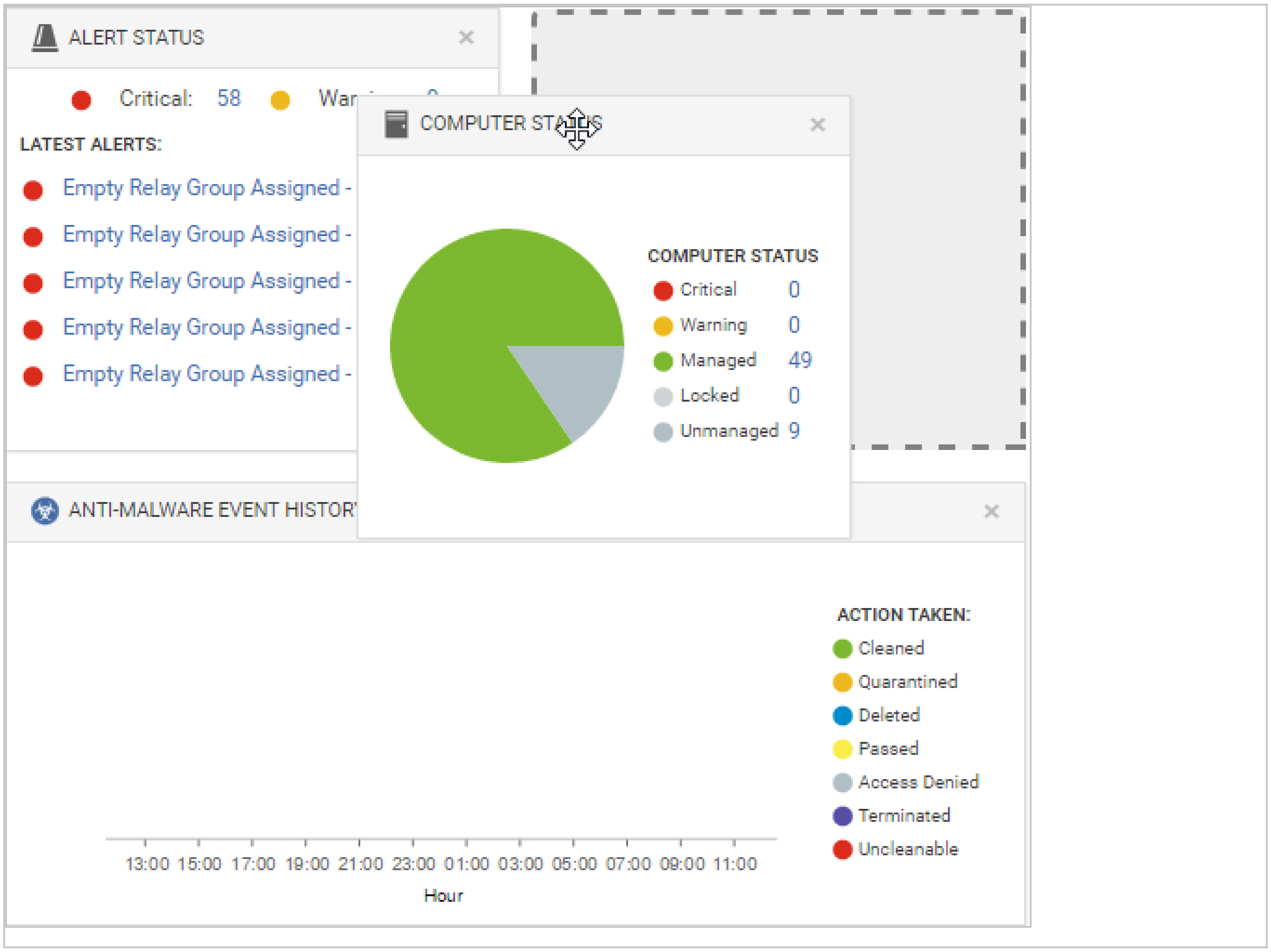
- **Log Inspection Activity**: The top five reasons Integrity Monitoring events occurred, including the number. In this case, the reason refers to the rule that was triggered.
- **Log Inspection Computer Activity**: The top five computers where Log Inspection events occurred, including the number of events.
- **Log Inspection Description Activity**: The top five descriptions for Log Inspection events, including the number of times they occurred. The description refers to the event that was triggered.
- **Log Inspection Event History [2x1]**: Recent Log Inspection event history, including the severity of events.

### Application Control:

- **Application Control Maintenance Mode Status [2x1]**: The computers in maintenance mode, including their start and end time.

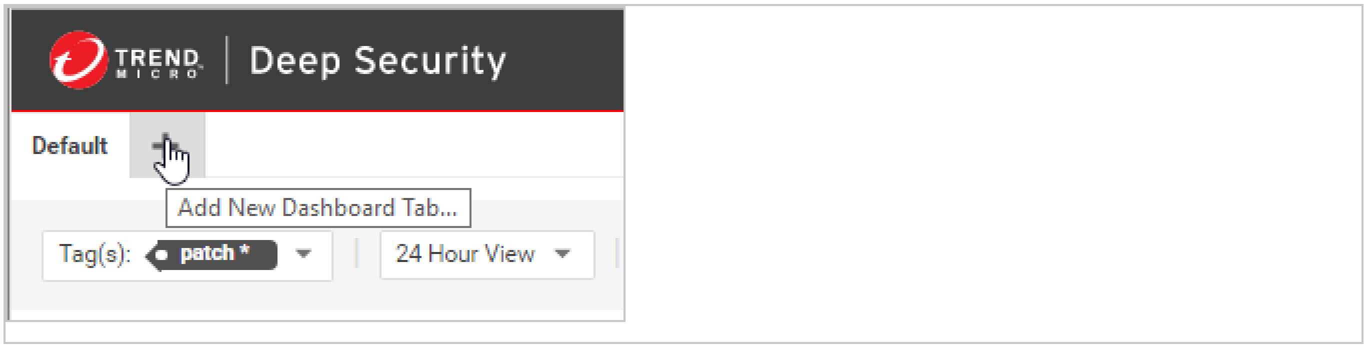
## Change the layout

You can move the selected widgets around the dashboard by dragging them by their title bar. That is, if you move a widget over an existing one, they will exchange places. The widget that is about to be displaced will temporarily gray out.



## Save and manage dashboard layouts

You can create multiple dashboard layouts and save them as separate tabs. Your Dashboard settings and layouts are not visible to other users after you sign out. To create a new Dashboard tab, click the plus symbol to the right of the last tab on the Dashboard, as per the following illustration:



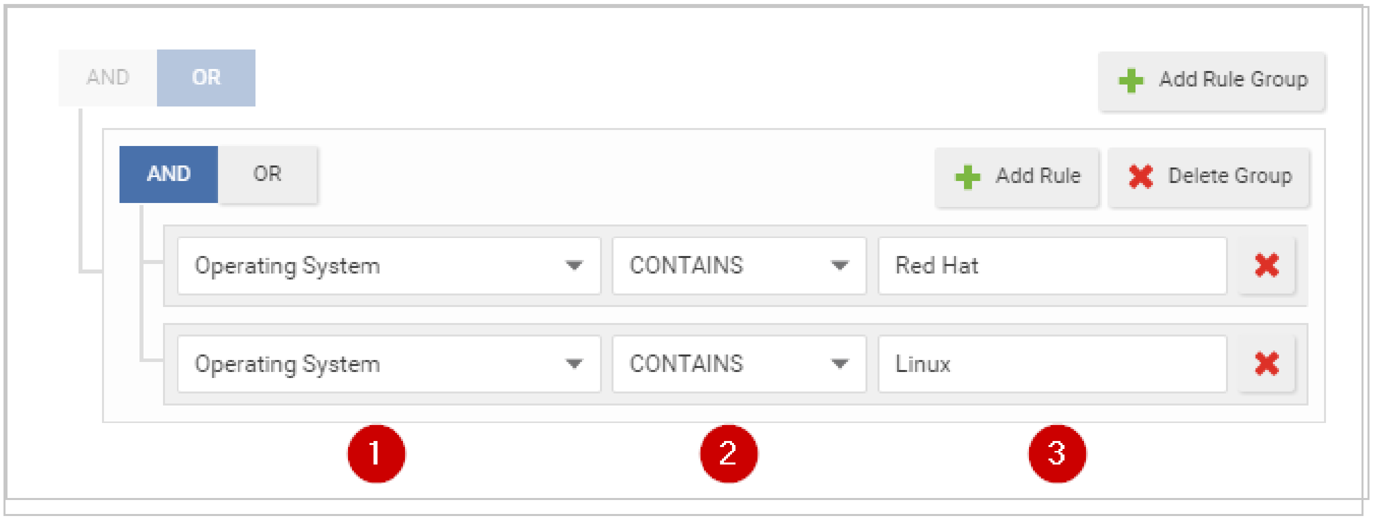
# Group computers dynamically with smart folders

A smart folder is a dynamic group of computers that you define with a saved search query. It finds matching computers each time you click the group. For example, if you want to view your computers grouped by attributes such as operating system or AWS project tags, you can do this using smart folders.

Tip: If you prefer to search for resources programmatically, you can automate resource searches using the Deep Security API. For examples, see the Search for Resources guide in the Deep Security Automation Center.

You create smart folders by defining:

1. What to search (1 - computer properties)
2. How to determine a match (2 - operator)
3. What to search for (3 - value)



Operating System CONTAINS Red Hat

Operating System CONTAINS Linux

## Create a smart folder

1. Go to **Computers > Smart Folders**.
2. Click **Create a Smart Folder**.

   A default, empty search criteria group ("rule group") appears. You must configure this first. If you need to define more or alternative possible matches, you can add more rule groups later.
3. Type a name for your smart folder.

4. In the first drop-down list, select a property that all matching computers have, such as **Operating System**. (See "Searchable Properties" on page 1471.)

   If you selected AWS **Tag** , Azure **Tag**, or GCP **Label**, also type the tag's name or label key.

5. Select the operator: whether to match identical, similar, or opposite computers, such as **CONTAINS**.

   **Note:** Some operators are not available for all properties.

6. Type all or part of the search term.

   **Note:** Wild card characters are not supported.

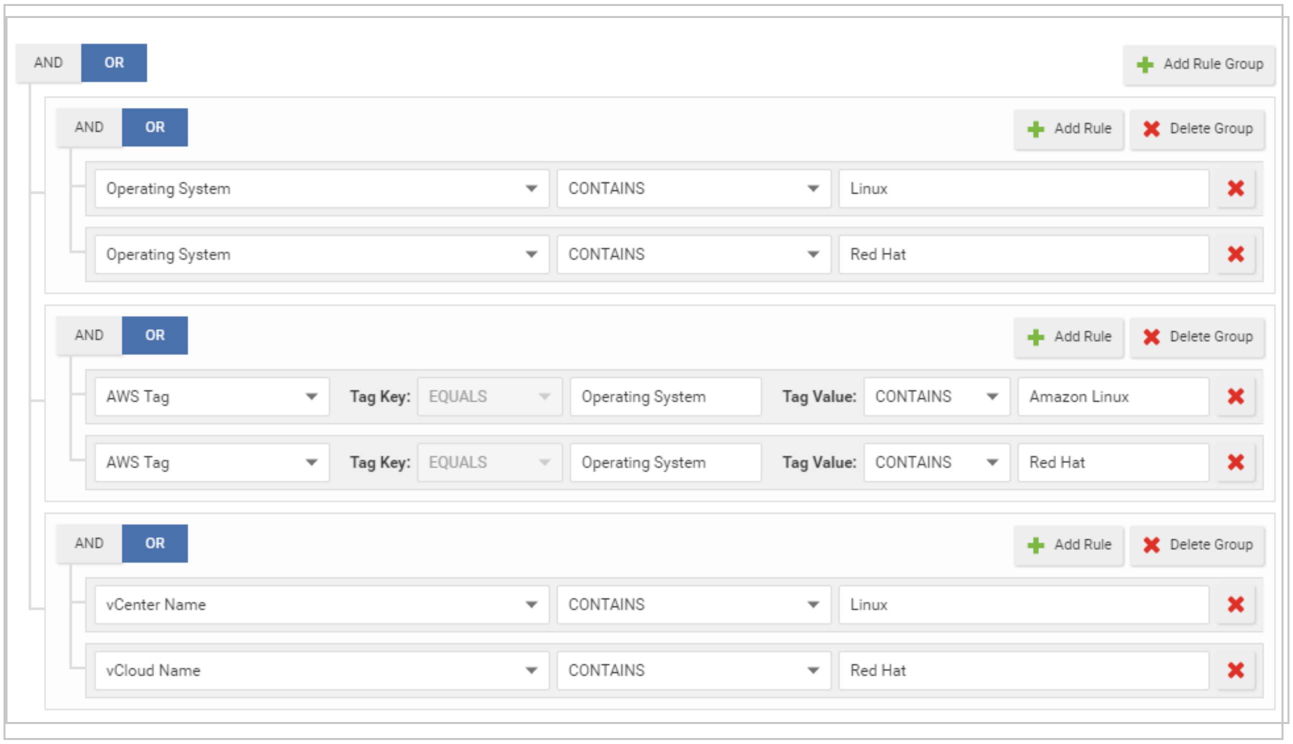
   **Tip:** If you enter multiple words, it compares the *entire phrase* - not each word separately. No match occurs if the property's value has words in a different order, or only some of the words.
   To match *any* of the words, instead click **Add Rule** and **OR**, and then add another value: one word per rule.

7. If computers must match multiple properties, click **Add Rule** and **AND**. Repeat steps 4-6.

   For more complex smart folders, you can chain multiple search criteria. Click **Add Group**, then click **AND** or **OR**. Repeat steps 4-7.

   For example, you might have Linux computers deployed both on-premises and in clouds such as AWS or vCloud. You could create a smart folder that contains all of them by using 3 rule groups based on:

   a. local physical computers' operating system
   b. AWS tag
   c. vCenter or vCloud name



Operating System CONTAINS Linux

Operating System CONTAINS Red Hat

AWS Tag Tag Key: EQUALS Operating System Tag Value: CONTAINS Amazon Linux

AWS Tag Tag Key: EQUALS Operating System Tag Value: CONTAINS Red Hat

vCenter Name CONTAINS Linux

vCloud Name CONTAINS Red Hat

Tip: To test the results of your query before saving your smart folder, click **Preview**.

8. Click **Save**.
9. To verify, click your new smart folder. Verify that it contains all expected computers.

Tip: For faster smart folders, remove unnecessary AND operations, and reduce sub-folder depths. They increase query complexity, which reduces performance.

Also verify that it omits computers that shouldn't match the query. If you need to edit your smart folder's query, double-click the smart folder.

Note: If your account's role doesn't have the permissions, some computers won't appear, or you won't be able to edit their properties. For more information, see "Define roles for users" on page 1415.

## Edit a smart folder

If you need to edit your smart folder's query, double-click the smart folder.

To reorder search criteria rules or rule groups, move your cursor onto a rule or group until it changes to a ✥ , then drag it to its destination.

## Clone a smart folder

To duplicate and modify an existing smart folder as a template for a new smart folder, right-click the original smart folder, then select **Copy Smart Folder**.

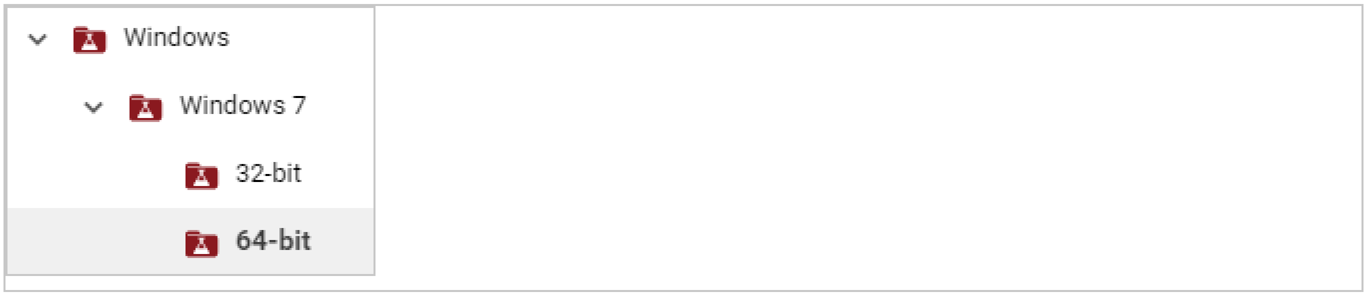
## Focus your search using sub-folders

You can use sub-folders to filter a smart folder's search results.

Smart folders can be nested up to 10 levels deep.

- Smart folder 1
  - Sub-folder 2
    - Sub-folder 3 ...

For example, you might have a smart folder for all your Windows computers, but want to focus on computers that are specifically Windows 7, and maybe specifically either 32-bit or 64-bit. To do this, under the "Windows" parent folder, you could create a child smart folder for Windows 7. Then, under the "Windows 7" folder, you would create two child smart folders: 32-bit and 64-bit.



1. Right-click a smart folder and select **Create Child Smart Folder**.
2. Edit your child smart folder's query groups or rules. Click **Save**.
3. Click your new smart folder. Verify that it contains all expected computers. Also verify that it omits computers that shouldn't match the query.

## Automatically create sub-folders

**Note:** Applies to AWS, Azure, and GCP computers only.

Instead of manually creating child folders, you can automatically create sub-folders for each value of an AWS tag, Azure tag, or GCP label that's assigned to an Amazon EC2 instance, Amazon Workspace, Azure VM, or GCP VM instance. For information on how to apply tags/labels to your computers, refer to the documentation from your cloud provider:

- Amazon: Tag your Amazon EC2 resources, Tag WorkSpaces Resources
- Azure: Use tags to organize your Azure resources and management hierarchy
- GCP: Labeling resources.

**Note:** Tag/label-based sub-folders will replace any existing manually created child folders under the parent folder.

1. In Deep Security Manager, right-click a smart folder and select **Smart Folder Properties**.
2. In the main pane, near the bottom, select the **Automatically create sub-folders for each value of a specific tag or label key** check box.
3. Select either the AWS, Azure, or GCP cloud vendor.
4. Type the name of the AWS tag, Azure tag, or GCP label key. Sub-folders are automatically created for each of the tag or label values.
5. Click **Save**.

**Tip:** Empty sub-folders can appear if tag or label value is not being used anymore. To remove them, right-click the smart folder and select **Synchronize Smart Folder**.

## Searchable Properties

Properties are an attribute that some or all computers you want to find have. Smart folders show computers that have the selected property, and its value matches.

**Note:** Type your search *exactly as that property appears in Deep Security Manager*- not, for example, vCenter/AWS/Azure/GCP. Otherwise your smart folder query won't match.
To find the exact matching text, (unless otherwise noted) go to **Computers** and look in the navigation pane on the left.

### General

| Property | Description | Data type | Examples |
|---|---|---|---|
| Hostname | The computer's host name, as seen on **Computers > Details** in Hostname. | string | ca-staging-web1 |

| Property | Description | Data type | Examples |
|---|---|---|---|
| Computer Display Name | The computer's display name in Deep Security (if any), as seen on **Computers > Details** in Display Name. | string | nginxTest |
| Folder Name | The computer's assigned group. | string | US-East |
| Operating System | The computer's operating system, as seen on **Computers > Details** in Platform. | string | Microsoft Windows 7 (64 bit) Service Pack 1 Build 7601 |
| IP Address | The computer's IP address.<br>You can find the IP address in Deep Security Manager. To find the IP of:<br>- an AWS instance, GCP VM or Azure VM, that was added to Deep Security through **Add > Add AWS\|Azure\|GCP Account**, go the computer's details page, and under the **General** tab, scroll to the **Virtual machine Summary** section. The AWS IP addresses are listed in these fields:<br>  - **Private IP Address**<br>  - **Public IP (PIP) Address**<br>**Note:** If you added the AWS, GCP, or Azure | IPv4 or IPv6 address, or an IPv4 range | 172.20.1.5-172.20.1.55<br>2001:db8:face::5 |

| Property | Description | Data type | Examples |
|---|---|---|---|
| | computer through **Add > Add Computers**, its IP address is located in the same place as a physical computer's.<br>- a physical computer, go to the computer's details page and on the left, click **Interfaces**<br>**Note:** If "DHCP" is displayed instead of a static IP address, it won't match the smart folder query.<br>- a vCenter or vCloud VM, go to the vCenter computer's details page, and under the **General** tab, scroll to the **Virtual machine Summary** section. The vCenter or vCloud IP address is listed in the **IP Address** field. | | |
| Policy | The computer's assigned Deep Security policy, as seen on **Computers > Details**. | string<br>(option in drop-down list) | Base Policy |
| Activated | Whether or not the computer has been activated with Deep | Boolean | Yes |

| Property | Description | Data type | Examples |
|---|---|---|---|
| | Security Manager, as seen on **Computers > Details**. | | |
| Docker Host | Whether or not Docker is installed on the computer, as seen on **Computers > Details**. | Boolean | No |
| Computer Type | The type of computer. Options are: Physical Computer, Amazon EC2 Instance, Amazon WorkSpace, vCenter VM, Azure Instance, Azure ARM Instance, GCP VM Instance. | string (option in drop-down list) | Examples: Physical Computer, Amazon EC2 Instance |
| Last Successful Recommendation Scan | Whether or not the computer has had a successful recommendation scan within a specified time period. The last recommendation scan date and results can be seen on **Computers > Details > General > Intrusion Prevention** or **Integrity Monitoring** or **Log Inspection > Recommendations**. | Date operator drop-down list, String, Date unit drop-down list | **OLDER THAN**, 7, **DAYS** |
| Last Agent Communication | Whether or not the agent has communicated with Deep Security Manager within a specified time period. The Last Communication date can be seen on **Computers > Details > General > Last Communication**. | Date operator drop-down list, String, Date unit drop-down list | **OLDER THAN**, 3, **DAYS** |
| Agent Offline | Whether or not the agent is offline. This is displayed as **Managed (Offline)** or **Offline** on **Computers > Details > General > Last Communication**. | Boolean | Yes |

| Property | Description | Data type | Examples |
|---|---|---|---|
| Task(s) | State of the computer's tasks, as displayed in the **Task(s)** column on the **Computers** page. For a list of all possible tasks, see "Computer and agent statuses" on page 1353. | string | Activating |
| Host Created Date | Date when the computer was added to Deep Security Manager. | string (date) | 2019-03-15 |
| Version | Deep Security Agent version. | string | 12.0.0.1 |

## AWS

| Property | Description | Data type | Examples |
|---|---|---|---|
| Tag | The computer's AWS tag key:value pair, as seen on **Computers > Details > Overview > General** under Virtual machine Summary, in Cloud Instance Metadata.<br>Type the tag name, then its value. Case-sensitive. | string | Tag Key: env<br>Tag Value: staging |
| Security Group Name | The computer's associated AWS security group name, as seen on **Computers > Details > Overview > General** under Virtual machine Summary, in Security Group(s). | string | SecGrp1 |
| Security Group ID | The computer's AWS security group ID, as seen on **Computers > Details > Overview > General** under Virtual machine Summary, in Security Group(s). | string | sg-12345678 |
| AMI ID | The computer's Amazon Machine AMI ID, as seen on **Computers > Details > Overview > General** under Virtual machine Summary, in AMI ID. | string | ami-23c44a56 |
| Account ID | The computer's associated 12-digit AWS | string | 123456789012 |

| Property | Description | Data type | Examples |
|---|---|---|---|
| | Account ID, as seen on **Computers** when you right-click **Amazon Account** and select **Properties**.<br>Results include computers in sub-folders. | | |
| Account Name | The computer's associated AWS Account Alias, as seen on **Computers** when you right-click the AWS Cloud Connector and select **Properties**.<br>Results include computers in sub-folders. | string | MyAccount-123 |
| Region ID | The computer's AWS region suffix.<br>Results include computers in sub-folders. | string | us-east-1 |
| Region Name | The computer's associated AWS region name.<br>Results include computers in sub-folders. | string | US East (Ohio) |
| VPC ID | The computer's Virtual Private Cloud (VPC) ID.<br>If an alias exists, the folder name is the alias, followed by the VPC ID in parentheses. Otherwise the folder's name is the VPC ID.<br>Results include computers in sub-folders. | string | vpc-3005e48a |
| Subnet ID | The computer's associated Virtual Private Cloud (VPC) subnet ID.<br>If an alias exists, the folder name is the alias, followed by the VPC subnet ID in parentheses. Otherwise the folder's name is the VPC subnet ID. | string | subnet-b1c2e468 |

| Property | Description | Data type | Examples |
|---|---|---|---|
| | Results include computers in sub-folders. | | |
| Directory ID | The ID of the AWS directory where the user entry associated with an Amazon WorkSpace resides. The directory ID is seen on the **Computers > Details > Virtual machine Summary**, in the **WorkSpace Directory** field. That field takes the format <directory_alias>(<directory_ID>), for example, myworkspacedir(d-9367232d89). | string | d-9367232d89 |

## Azure

| Property | Description | Data type | Examples |
|---|---|---|---|
| Subscription Name | **Note:** As of Deep Security Manager 12.0, the Subscription Name is no longer collected. It remains visible in the drop-down list of properties in case the information was obtained through a previous version of the manager.<br>The computer's associated Azure subscription account ID, as seen on **Computers** when you right-click **Azure** and select **Properties**.<br>Results include computers in sub-folders. | string | MyAzureAccount |
| Resource Group | The computer's associated resource group. | string | MyResourceGroup |
| Location | The computer’s location name | string | East US |
| Tag | The computer's Azure tag key:value pair, as seen on **Computers > Details > Overview > General** under | string | Tag Key: env<br>Tag Value: staging |

| Property | Description | Data type | Examples |
|---|---|---|---|
| | under **Virtual machine Summary**, in **Cloud Instance Metadata**.<br>Type the tag name, then its value. Case-sensitive. | | |

## GCP

| Property | Description | Data type | Examples |
|---|---|---|---|
| Label | The computer's GCP label key:value pair, as seen on **Computers > Details > Overview > General** under **Virtual machine Summary**, in **Cloud Instance Metadata**.<br>Type the label key, and then its value. Case-sensitive. | string | Label Key: env<br>Label Value: staging |
| Network Tag | The computer's network tag, as seen on **Computers > Details > Overview > General** under **Virtual machine Summary**, in **Cloud Instance Metadata**. | string | production |

## vCenter

| Property | Description | Data type | Examples |
|---|---|---|---|
| Name | The computer's associated vCenter.<br>Results include computers in sub-folders. | string | vCenter - lab13-vc.example.com |
| Datacenter | The computer's associated vCenter data center.<br>Results include computers in sub-folders. | string | lab13-datacenter |
| Folder | The computer's vCenter folder. | string | db_dev |

| Property | Description | Data type | Examples |
|---|---|---|---|
| | Results include computers in sub-folders. | | |
| Parent ESX Hostname | The hostname of the ESXi hypervisor where the computer's guest VM is running, as seen on **Computers**. | string | lab13-esx2.example.com |
| Custom Attribute | The computer's assigned vCenter custom attribute, as seen on **Computers > Details** in Virtual machine Summary. | string<br>(comma-separated attribute name and value) | env, production |
| Power State | The computer's vCenter state, as seen on **Computers > Details** in VMware Virtual machine Summary. | string<br>(option in list) | Powered On |

## vCloud

| Property | Description | Data type | Examples |
|---|---|---|---|
| Name | The computer's associated vCloud.<br>Results include computers in sub-folders. | string | vCloud-lab23 |
| Datacenter | The computer's associated vCloud data center.<br>Results include computers in sub-folders. | string | lab13-datacenter |
| vApp | The computer's associated vCloud data center folder.<br>Results include computers in sub-folders. | string | db_dev |

### Active Directory

| Property | Description | Data type | Examples |
|---|---|---|---|
| Name | The hostname of the Microsoft Active Directory or LDAP directory.<br>Results include computers in sub-folders. | string | ad01.example.com |
| Folder | The computer's Microsoft Active Directory or LDAP folder name.<br>Results include computers in sub-folders. | string | Computers |

## Operators

Smart folder operators indicate whether matching computers should have a property value that is identical, similar, or dissimilar to your search term. Not all operators are available for every property.

| Operator | Description | Example usage |
|---|---|---|
| EQUALS | The search query only finds computers that are an exact match. | A search query for 'Windows' in the Operating System property does not find computers with 'Windows 7' or 'Microsoft Windows'. |
| DOES NOT EQUAL | The search query finds any computers that are not an exact match. | A search query for 'Amazon Linux (64 bit)' in the Operating System property finds all computers other than Amazon Linux 64-bit machines. |
| CONTAINS | The search query finds any computers that contain the search term. | A search query for '203.0.113.' in the IP Address property finds any computers on the 203.0.113.xxx subnet. |
| DOES NOT CONTAIN | The search query finds any computers that do not contain the search term. | A search query for 'Windows' in the Operating System property finds any computers that do not have 'Windows' in their operating system name. |
| ANY VALUE | The search query finds all computers | A search query in the Group Name property finds all computers in that group. |

| Operator | Description | Example usage |
|---|---|---|
| | with the selected property. | |
| IN RANGE | The search query finds all computers between the specified start and end range. | A search query in the IP Address property with Start Range 10.0.0.0 and End Range 10.255.255.255 would find all computers with IP addresses between 10.0.0.0 and 10.255.255.255. |
| NOT IN RANGE | The search query finds all computers that are not between the specified start and end range. | A search query in the IP Address property with Start Range 10.0.0.0 and End Range 10.255.255.255 finds all computers that have IP addresses outside the range of 10.0.0.0 and 10.255.255.255. |
| Yes | The search query finds all computers with the selected property. | A search query with 'Yes' selected for the Docker property finds any computers with the Docker service running. |
| No | The search query finds all computers that do not have the selected property. | A search query with 'No' selected for the Docker property would find any computers that do not have the Docker service running. |
| OLDER THAN | The search query finds all computers prior to the specified date for the property.<br>Used with an accompanying DAYS, WEEKS, HOURS, or MINUTES operator. | A search query with 'OLDER THAN', '7', 'DAYS' for the 'Last Successful Recommendation Scan' property finds computers that have had a successful recommendation scan 8 days or longer ago. |
| MORE RECENTLY THAN | The search query finds all computers more recent than the specified date for the property. | A search query with 'MORE RECENTLY THAN', '1', 'MONTH' for the 'Last Successful Recommendation Scan' property finds computers that have had a successful recommendation scan earlier than 1 month ago. |

| Operator | Description | Example usage |
|---|---|---|
| | Used with an accompanying DAYS, WEEKS, HOURS, or MINUTES operator. | |
| NEVER | The search query finds all computers that do not match the property. | A search query with 'NEVER' for the 'Last Successful Recommendation Scan' property finds computers that have never had a successful recommendation scan. |

## Customize advanced system settings

Several features for advanced users are located on **Administration > System Settings > Advanced**.

**Tip:** You can automate system setting changes using the Deep Security API. For examples, see the Configure Policy, Computer, and System Settings guide in the Deep Security Automation Center.

### Primary Tenant Access

By default, the primary tenant can access your Deep Security environment.

If the primary tenant enabled the "Primary Tenant Access" settings in your environment, however, you can prevent the primary tenant from accessing your Deep Security environment, or grant access for a limited amount of time.

### Load Balancers

**Note:** The load balancer settings are not available when FIPS mode is enabled. See "FIPS 140 support" on page 1639.

Agents are configured with a list of Deep Security Manager and Deep Security Relays. When multiple managers and relays are deployed *without* a load balancer, agents will automatically contact the managers and relays using a round robin sequence.

To better scale your network, you can put a load balancer in front of the managers or relays. When you configure the load balancer hostname and port numbers, it will override the IP address or hostname and port numbers currently used by the agents.

The script generator uses the address of the Deep Security Manager that you are connected to. This ensures that the scripts continue to function even if one of the Deep Security Manager nodes fails or is down for maintenance or upgrades.

**Note:** The load balancer must be non-terminating for the SSL or TLS session with the agent's heartbeat port number because its uses mutual authentication. SSL inspection that terminates (for example, if you try to use SSL offloading) will break the session.

## Multi-tenant Mode

1. Select **Enable Multi-Tenant Mode**.
2. In the wizard that appears, enter your **Multi-Tenant Activation Code** and click **Next**.
3. Select the license mode, either:
   - **Inherit Licensing from Primary Tenant:** All tenants use the same licenses as the primary tenant.
   - **Per Tenant Licensing:** Tenants themselves enter a license when they log in for the first time.
4. Click **Next**.

## Deep Security Manager Plug-ins

Plug-ins are modules, reports and other add-ons for the Deep Security Manager. Trend Micro occasionally produces new or additional versions of these which are distributed as self-installing packages.

## SOAP Web Service API

Enable or disable the legacy SOAP API Web services. The WSDL (Web Services Description Language) can be found at the URL displayed in the panel on the page. For more information about APIs, see "Use the Deep Security API to automate tasks" on page 1598.

**Note:** To access the Web Services APIs, a user must be assigned a role with the appropriate access rights. To configure the role, go to **Administration > User Management > Roles**, open the role properties, and select **Allow Access to web services API**.

## Status Monitoring API

Enable or disable the Status Monitoring API of the legacy REST API. This API lets you query the Deep Security Manager (including individual Manager Nodes) for status information such as CPU and memory usage, number of queued jobs, total and Tenant-specific database size. For more information about APIs, see "Use the Deep Security API to automate tasks" on page 1598.

## Export

**Export file character encoding:** The character encoding used when you export data files from the Deep Security Manager. The encoding must support characters in your chosen language.

**Exported Diagnostics Package Language:** Your support provider may ask you generate and send them a Deep Security diagnostics package. This setting specifies the language the package will be in. The diagnostic package is generated on **Administration > System Information**.

## Whois

Whois can be used to look up which domain name is associated with an IP address when you review logged intrusion prevention and firewall events. Enter the search URL using "[IP]" as a placeholder for the IP address to look up.
(For example, "http://reports.internic.net/cgi/whois?whois_nic=[IP]&type=nameserver".)

## Licenses

**Hide unlicensed Protection Modules for new Users** determines whether unlicensed modules are hidden rather than simply grayed out for subsequently created Users. (This setting can be overridden on a per-user basis on **Administration > User Management > Users > Properties**).

## Scan Cache Configurations

## CPU Usage During Recommendation Scans

This setting controls the amount of CPU resources dedicated to performing Recommendation Scans. If you notice that CPU usage is reaching unreasonably high levels, try changing to a lower setting to remedy the situation. For other performance controls, see **Administration > Manager Nodes > Properties > Performance Profiles**.

## Logo

You can replace the Deep Security logo that appears on the login page, at the top right of the Deep Security Manager GUI, and at the top of reports. Your replacement image must be in PNG format, be 320 px wide and 35 px high, and have a file size smaller than 1 MB. A template is available in the `installfiles` directory of the Deep Security Manager.

Click **Import Logo** to import your own logo, or click **Reset Logo** to reset the logo to its default image.

## Manager AWS Identity

You can configure cross-account access. Select either:

- **Use Manager Instance Role:** The more secure option to configure cross-account access. Attach a policy with the sts:AssumeRole permission to the Deep Security Manager's instance role, then select this option. Does not appear if the Deep Security Manager does not have an instance role, or if you're using an Azure Marketplace or on-premise installation of Deep Security Manager.
- **Use AWS Access Keys:** Create the keys and attach a policy with the sts:AssumeRole permission before you select this option, and then type the **Access Key** and **Secret Key**. Does not appear if you're using an Azure Marketplace or on-premise installation of Deep Security Manager.

## Application control

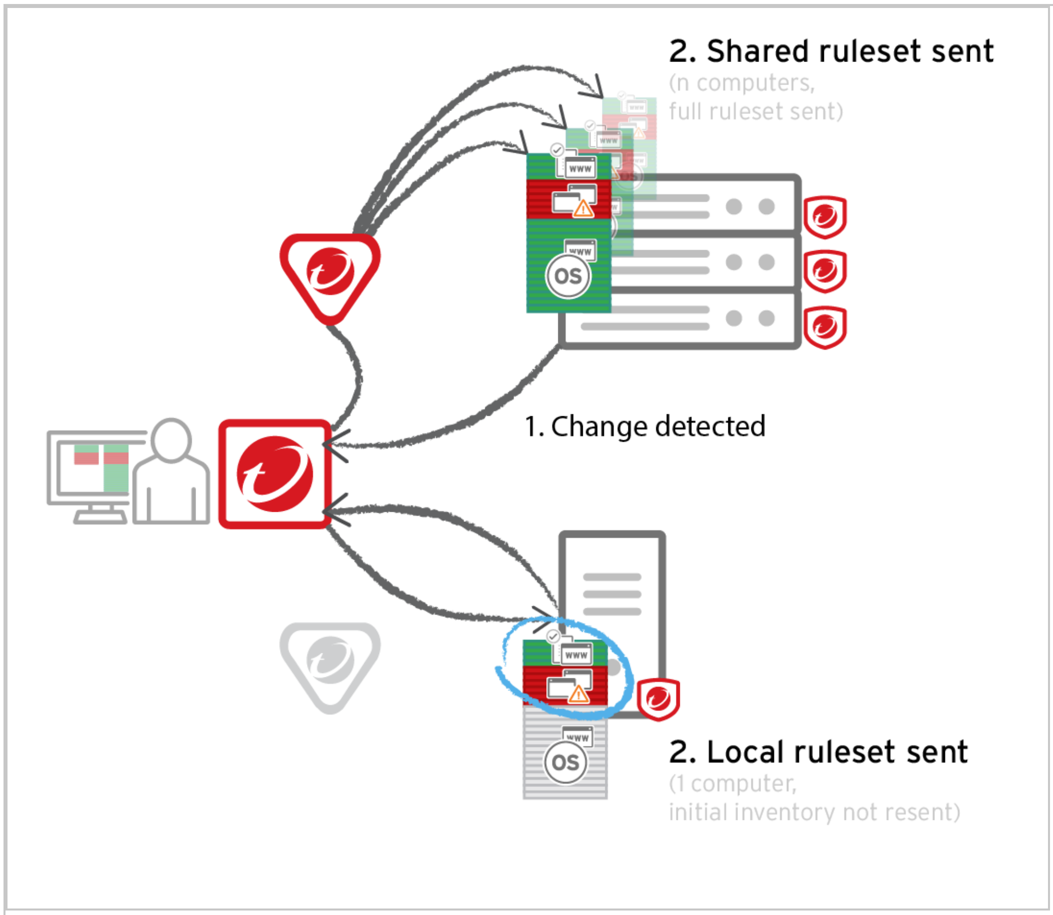
Each time you create an Application Control ruleset or change it, it must be distributed to all computers that use it. Shared rulesets are bigger than local rulesets. Shared rulesets are also often applied to many servers. If they all downloaded the ruleset directly from the manager at the same time, high load could cause slower performance. Global rulesets have the same considerations.

Using Deep Security Relays can solve this problem. (For information on configuring relays, see "Deploy additional relays" on page 1345.)

Steps vary by whether or not you have a multi-tenant deployment.

### Single tenant deployments

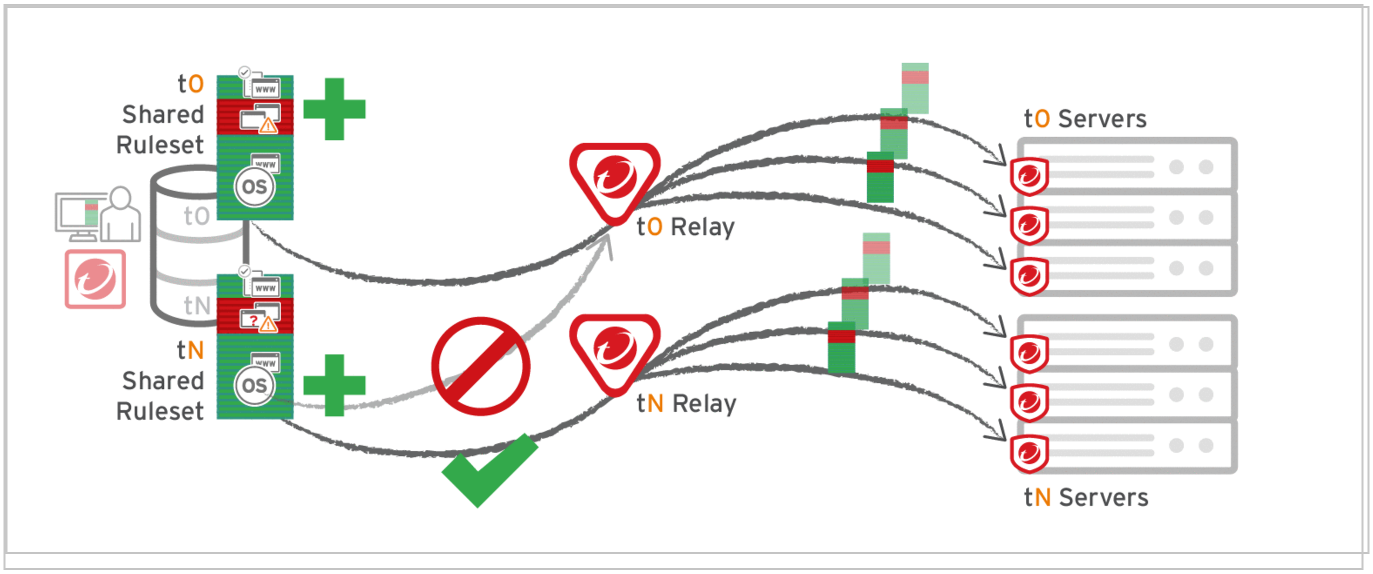
Go to **Administration > System Settings > Advanced** and then select **Serve Application Control rulesets from relays**.



### Multi-tenant deployments

The primary tenant (t0) can't access other tenants' (tN) configurations, so t0 relays don't have tN Application Control rulesets. (Other features like IPS don't have this consideration, because their rules come from Trend Micro, not a tenant.)

Other tenants (Tn) must create their own relay group, then select **Serve Application Control rulesets from relays**.



Warning:

Verify compatibility with your deployment before using relays. If the agent doesn't have any previously downloaded rulesets currently in effect, and **if it doesn't receive new Application Control rules, then the computer won't be protected by Application Control.** If an Application Control ruleset fails to download, a ruleset download failure event will be recorded on the manager and on the agent.

Relays might either change performance, break Application Control ruleset downloads, or be required; it varies by proxy location, multi-tenancy, and global/shared vs. local rulesets.

| Required for... | Faster performance for... | Slower performance for... | Don't enable for... |
|---|---|---|---|
| Agent > Proxy > Manager | Shared rulesets<br>Global ruleset | Local rulesets | Multi-tenant configurations when non-primary tenants (tN) use the default, primary (t0) relay group:<br>• Agent (tN) > DSR (t0) > DSM (tN) |

| Required for... | Faster performance for... | Slower performance for... | Don't enable for... |
|---|---|---|---|
| **Note:** In Deep Security Agent 10.0 GM and earlier, agents didn't have support for connections through a proxy to relays. If a ruleset download fails due to a proxy, and if your agents require a proxy to access the relay or manager, then you must either: | | | - Agent (tN) > Proxy > DSR (t0) > DSM (tN) |

| Required for... | Faster performance for... | Slower performance for... | Don't enable for... |
|---|---|---|---|
| - update agents' software, then configure the proxy<br>- bypass the proxy<br>- add a relay and then select **Serve Application Control rule** | | | |

| Required for... | Faster performance for... | Slower performance for... | Don't enable for... |
|---|---|---|---|
| sets from relays | | | |

# Harden Deep Security

## About Deep Security hardening

There are several measures you can take to increase the security of your Deep Security deployment.

- "Protect Deep Security Manager with an agent" below
- "Protect Deep Security Agent" on page 1492
- "Replace the Deep Security Manager TLS certificate" on page 1494
- "Update the load balancer's certificate" on page 1504
- "Encrypt communication between the Deep Security Manager and the database" on page 1506
- "Change the Deep Security Manager database password" on page 1511
- "Configure HTTP security headers" on page 1514
- "Enforce user password rules" on page 1519
- "Set up multi-factor authentication" on page 1521
- "Manage trusted certificates" on page 1525
- "SSL implementation and credential provisioning" on page 1528

## Protect Deep Security Manager with an agent

To protect the server where Deep Security Manager is installed, install an agent on it and apply the Deep Security Manager policy.

1. Install an agent on the same computer as the manager.
2. Go to **Computers**.
3. Add the manager's computer. Do not choose to apply a policy yet.
4. Turn on the **Intrusion Prevention** with no rule. Double-click the new computer to display its **Details** window and go to **Intrusion Prevention > General > Configuration > On**.
5. Wait for the **Intrusion Prevention** to turn on.
6. Go to **Intrusion Prevention > Advanced > SSL Configurations**.
7. Click **View SSL Configurations > New** to start the wizard to create a new SSL Configuration.
8. Specify the interface used by the manager. Click **Next**.
9. On the **Port** page, select whether to protect the Deep Security Manager GUI's port number. Click **Next**.
10. Specify whether SSL Intrusion Prevention analysis should take place on all IP addresses for this computer, or just one. (This feature can be used to set up multiple virtual computers on a single computer.)
11. Select **Use the SSL Credentials built into the Deep Security Manager**. (This option only appears when creating an SSL Configuration for the Manager's computer.) Click **Next**.
12. Finish the wizard and close the **SSL Configuration** page.
13. Return to the computer's **Details** window. Apply the **Deep Security Manager Policy**, which includes the Firewall Rules and Intrusion Prevention Rules required to protect the Deep Security Manager's GUI port number.

You have now protected the Manager's computer and are now filtering the traffic (including SSL) to the Manager.

**Note:** After configuring the Agent to filter SSL traffic, you may notice that the Deep Security Agent will return several **Renewal Error** events. These are certificate renewal errors caused by the new SSL certificate issued by the Manager computer. To fix this, refresh the web page and reconnect to the Deep Security Manager's GUI.

The **Deep Security Manager** Policy has the basic Firewall Rules assigned to enable remote use of the Manager. Additional Firewall Rules may need to be assigned if the Manager's computer is being used for other purposes. The Policy also includes the Intrusion Prevention Rules in the **Web Server Common** Application Type. Additional Intrusion Prevention Rules can be assigned as desired.

Because the **Web Server Common** Application Type typically filters on the **HTTP** Port List and does not include the Deep Security Manager GUI's port number, it is added as an override to the ports setting in the **Intrusion Prevention Rules** page of the Policy's **Details** window.

For more information on SSL data inspection, see "Inspect TLS traffic" on page 832.

# Protect Deep Security Agent

To improve security, you can bind Deep Security Agent to a specific Deep Security Manager. The procedure vary depending on if you are using manager-initiated activation or agent-initiated activation:

Manager-initiated activation

During agent-manager communications, Deep Security Agent can authenticate the identity of its manager. It does this by comparing your trusted manager's certificate to the connecting manager's certificate. If they do not match, the manager authentication fails and the agent does not connect.

This prevents agents from activating with or connecting to a malicious server pretending to be your Deep Security Manager. This is recommended especially if agents connect through an untrusted network such as the Internet.

To protect your agents, you must configure each agent so it can recognize its authorized manager before the agent tries to activate:

> **Note:** If you reset or deactivate an agent, it deletes the Deep Security Manager certificate. Repeat these steps if you want to reactivate the agent.

1. On Deep Security Manager, run the command to export its server certificate:

   ```
   dsm_c -action exportdsmcert -output ds_agent_dsm.crt
   ```

   where

   - `ds_agent_dsm.crt` is the name of the manager's server certificate. You must use this exact file name.

2. On each agent's computer, put the `ds_agent_dsm.crt` file in the following location:

   - On Windows: *`%ProgramData%\Trend Micro\ Deep Security Agent\dsa_core`*
   - On Linux or Unix: *`/var/opt/ds_agent/dsa_core`*

Initially, after completing these steps, the agent enters a preactivated state. Until the agent is fully activated, operations initiated by other Deep Security Managers or by entering commands to the agent via `dsa_control` do not work. This is intentional, and the regular operation resumes upon activation.

---

Agent-initiated activation

During agent activation, Deep Security Agent can authenticate the identity of its Deep Security Manager by pinning the manager's certificate to the agent. It does this by validating the connecting manager’s certificate path and ensuring it is signed by a trusted Certificate Authority (CA). If the certificate path is validated, the manager authentication passes and activates the agents. This prevents agents from activating with a malicious server that is pretending to be your Deep Security Manager.

To protect your agents, you must configure each agent so it can recognize its authorized manager before the agent tries to activate.

## Import a Deep Security Manager certificate chain issued by a public CA

1. Prepare a `chain.pem` file based on the following specifications:
   - A private key in PKCS #8 format.
   - The X509 certificate that corresponds to the private key.
   - Any other intermediate X509 certificates to build a chain of trust to a certificate to a trusted certificate authority (CA) root. Each certificate must sign the certificate that directly precedes it, so the order is important. See `certificate_list` in the RFC.
2. On Deep Security Manager, run the following command to import the certificate chain:

   ```
   /opt/dsm/dsm_c -action agentHBPublicServerCertificate -set
   ${path_to_pem_file}
   ```

   `${path_to_pem_file}` must be an absolute path.

---

3. Copy the public CA certificate and rename it to `ds_agent_dsm_public_ca.crt`.
4. On the agent computer, place the `ds_agent_dsm_public_ca.crt` file in one of these locations:
   - On Windows: `%ProgramData%\Trend Micro\Deep Security Agent\dsa_core`
   - On Linux or Unix: `/var/opt/ds_agent/dsa_core`

**Note:** If you have installed Deep Security Manager 20.0.262 and are activating Deep Security Agent 20.0.1540 or later, the following error message appears upon activation, which indicates you have not pinned the manager's certificate to the agent:

"[Warning/2] | SSLVerifyCallback() - verify error 20: unable to get local issuer certificate"

Pinning a trusted certificate is optional, so you can ignore this error if it does not apply to you. However, if you want to use a trusted certificate, follow the preceding steps before activating Deep Security Agent.

To confirm that the certificate chain has been imported, enter the following command:

```
/opt/dsm/dsm_c -action agentHBPublicServerCertificate -isSet
```

### Delete the imported certificate chain

To stop using a Deep Security Manager certificate chain issued by a public CA, enter the following command:

```
/opt/dsm/dsm_c -action agentHBPublicServerCertificate -delete
```

By default, Deep Security Manager reverts to using a self-signed certificate.

## Replace the Deep Security Manager TLS certificate

During installation, Deep Security Manager automatically generates a self-signed X.509 certificate so that you can use TLS during your first connection to the console. Because web browsers do not know this self-signing certificate authority (CA), they cannot validate the certificate's signature, and therefore do not automatically trust it. The browser displays a security alert and asks you to manually validate the certificate in order to connect. To avoid this every time an administrator connects, you can replace this default certificate with a certificate from a trusted CA.

> **Warning:** If you replace the default certificate with an invalid certificate or with the one that has an incomplete certificate signing chain, then you cannot connect to the Deep Security Manager console until you correct it. Before replacing the certificate, carefully read the instructions.

> **Note:** The certificates are kept when you upgrade Deep Security Manager. You do not need to upload them again.

To replace the certificate, do one of the following:

- **Request a new certificate for the Deep Security Manager domain name**

  a. If FIPS mode is enabled (see "FIPS 140 support" on page 1639), then disable FIPS mode before you begin to replace the certificate.
  b. "Generate the private key and Java keystore" on the next page.
  c. "Request a signed certificate (CSR)" on page 1498.
  d. "Import the signed certificate into the keystore" on page 1499.
  e. "Configure Deep Security Manager to use the keystore" on page 1501.
  f. If you disabled FIPS mode in the first step, re-enable FIPS mode now.

- **Use an existing Java keystore file or certificate**

  If you have a certificate file backup from a previous installation, or if you already have a certificate because you use the same certificate for multiple domain names (a wildcard certificate such as `*.example.com`, or a multiple-domain/Subject Alternative Name (SAN) field certificate), then you can use it instead.

  a. If FIPS mode is enabled (see "FIPS 140 support" on page 1639), then disable FIPS mode before you begin to replace the certificate.
  b. Verify that you have the complete certificate signing chain. If necessary, ask the CA that issued your certificate.
  c. "Configure Deep Security Manager to use the keystore" on page 1501.
  d. If you disabled FIPS mode in the first step, re-enable FIPS mode now.

## Generate the private key and Java keystore

Many public and private CAs have a website that can generate a public and private key pair and certificate signing request (CSR) at the same time. For example, you can generate the key pair and CSR at the same time in Microsoft Active Directory or an `openssl` CA, and then download and import the PKCS #12 file with both the signed certificate and private key into the Java keystore.

If you want to do that, then skip the next steps and "Request a signed certificate (CSR)" on page 1498, and then continue with "Import the signed certificate into the keystore" on page 1499. Otherwise, use these steps to locally generate the files.

1. On the computer where Deep Security Manager is running, open a command prompt as an administrator.
2. Enter the commands to generate a new private key and keystore file.

   In the following command example, the keystore entry (alias) for the new private key is named `tomcat`.

   > **Note:**
   > **A certificate's Common Name (CN) or Subject Alternative Name (SAN) field often must be different from the domain name that appears in your browser's location bar.**
   >
   > For example, the URL in your browser's location bar might show `https://dsm2.infosec.example.com`, but you want to use the same certificate for all of your Deep Security Manager nodes, so you make a wild card certificate with the common name (CN) `*.infosec.example.com`.

   - **Linux:**

     ```
     cd /opt/dsm/jre/bin
     keytool -genkey \
     -alias tomcat \
     -keystore ~/.keystore \
     -keyalg RSA \
     -validity 365 \
     -keysize 2048 \
     -dname "cn=dsm.example.com, ou=IT, o=Trend Micro, l=Ottawa,
     s=Ontario, c=CA"
     ```

- **Windows:**

  ```
  cd "C:\Program Files\Trend Micro\Deep Security
  Manager\jre\bin"
  keytool -genkey ^
  -alias tomcat ^
  -keystore C:\Users\Administrator\.keystore ^
  -keyalg RSA ^
  -validity 365 ^
  -keysize 2048 ^
  -dname "cn=dsm.example.com, ou=IT, o=Trend Micro, l=Ottawa,
  s=Ontario, c=CA"
  ```

  > **Note:** The example command uses Command Prompt (cmd.exe) syntax. If you use PowerShell instead, then replace the carrets (^) with backticks (`).

  For more information about the `keytool` command, see the Java keytool documentation.

3. Enter a password that Deep Security Manager will use to access the keystore. In the example commands, this is shown as `YOUR_PASSWORD`.

4. Enter the command to export the keystore in PKCS #12 format.

   In this command example, the name of the exported file is `.YOUR_PKCS12_EXPORTED_KEYSTORE`.

   - **Linux:**

     ```
     keytool -importkeystore \
     -srckeystore ~/.keystore \
     -destkeystore ~/.YOUR_PKCS12_EXPORTED_KEYSTORE \
     -deststoretype pkcs12
     ```

   - **Windows:**

     ```
     keytool -importkeystore ^
     -srckeystore C:\Users\Administrator\.keystore ^
     -destkeystore "C:\Users\Administrator\.YOUR_PKCS12_EXPORTED_
     ```

```
KEYSTORE" ^
-deststoretype pkcs12
```

When prompted, enter a new password for the exported (destination) keystore, and then the password for the original (source) keystore.

5. Continue with "Request a signed certificate (CSR)" below.

## Request a signed certificate (CSR)

Certificate signing request (CSR) files contain your unsigned certificate and public key. Ask a CA that your web browser trusts to sign it. The CA that signs your certificate can be either a root CA that is directly trusted by web browsers, or any intermediary CA that is directly or indirectly trusted by a root CA.

1. Enter the command to use the PKCS #12 file to generate a CSR file.

   You can create a multiple-domain/Subject Alternative Name (SAN) certificate by specifying matching domain names and/or IP addresses in the `san=` field of the `-ext` extension parameter. If you don't need a SAN certificate, then omit the `-ext` parameter.

   For a multiple-domain/SAN certificate, browsers should ignore the CN field when validating the connection. Instead they use the SAN field that contains the comma-separated list of matching domain names and IP addresses. Required syntax is shown in the example command.

   - **Linux:**

     ```
     keytool -certreq \
     -alias tomcat \
     -keystore ~/.YOUR_PKCS12_EXPORTED_KEYSTORE  \
     -file YOUR_CSR.csr \
     -keyalg RSA \
     -ext san=dns:dsm.example.com,dns:*.example.org,ip:10.10.10.5
     ```

   - **Windows:**

     ```
     keytool -certreq ^
     -alias tomcat ^
     -keystore C:\Users\Administrator\.YOUR_PKCS12_EXPORTED_
     ```

```
KEYSTORE ^
-file YOUR_CSR.csr ^
-keyalg RSA ^
-ext san=dns:dsm.example.com,dns:*.example.org,ip:10.10.10.5
```

2. Upload the CSR file to your CA. When the request has been processed, download the signed certificate file.
3. If you used an intermediary CA, and if your certificate is **not** in PKCS #7 format (it does not contain the signing chain), then also download the CA certificate and the certificates of all other CAs (if any) between it and the root CA.
4. Continue with "Import the signed certificate into the keystore" below.

## Import the signed certificate into the keystore

**Note:**
Browsers use the list of CA signatures that is added to the certificate (signing chain/chain of trust), to validate the certificate and determine if it is safe for you to connect. It evaluates each CA certificate in order. **You must import all of the CA certificates in the correct order, as shown in the following instructions.**

If the list of signatures is not in order, then web browsers cannot validate your certificate, and will block the connections to the console until you correct it.

1. If the root CA is already in the keystore, skip this step. Otherwise enter the command to import it.

   **Tip:**
   If you don't know what is in the keystore, you can view the contents:

   ```
   keytool -list -v
   ```

   In this command example, the certificates are in .crt format and the keystore entry (alias) for the root CA is named `rootCA`.

   - **Linux:**

     ```
     keytool -import \
     -alias rootCA \
     -file ~/YOUR_ROOT_CA.crt \
     ```

```
-keystore ~/.YOUR_PKCS12_EXPORTED_KEYSTORE \
-storepass YOUR_PASSWORD
```

- **Windows:**

```
keytool -import ^
-alias rootCA ^
-file c:\Users\Administrator\YOUR_ROOT_CA.crt ^
-keystore c:\Users\Administrator\.YOUR_PKCS12_EXPORTED_
KEYSTORE ^
-storepass YOUR_PASSWORD
```

2. If your intermediary CAs (if any) are already in the keystore, skip this step. Otherwise enter the commands to import them. Start with the one that was signed by the root CA, and end with the one that signed your certificate.

- **Linux:**

```
keytool -import \
-alias intermediateCA \
-trustcacerts \
-file ~/YOUR_INTERMEDIARY_CA.crt \
-keystore ~/.YOUR_PKCS12_EXPORTED_KEYSTORE \
-storepass YOUR_PASSWORD
```

- **Windows:**

```
keytool -import ^
-alias intermediateCA ^
-trustcacerts ^
-file c:\Users\Administrator\YOUR_INTERMEDIARY_CA.crt ^
-keystore c:\Users\Administrator\.YOUR_PKCS12_EXPORTED_
KEYSTORE ^
-storepass YOUR_PASSWORD
```

3. Enter the command to import your signed certificate.

- **Linux:**

  ```
  keytool -import \
  -alias tomcat \
  -trustcacerts \
  -file ~/YOUR_SIGNED_CERTIFICATE.crt \
  -keystore ~/.YOUR_PKCS12_EXPORTED_KEYSTORE \
  -storepass YOUR_PASSWORD
  ```

- **Windows:**

  ```
  keytool -import ^
  -alias tomcat ^
  -trustcacerts ^
  -file c:\Users\Administrator\YOUR_SIGNED_CERTIFICATE.crt ^
  -keystore c:\Users\Administrator\.YOUR_PKCS12_EXPORTED_
  KEYSTORE ^
  -storepass YOUR_PASSWORD
  ```

If the import is successful, then this message appears:
`Certificate reply was installed in keystore`

4. Continue with "Configure Deep Security Manager to use the keystore" below.

## Configure Deep Security Manager to use the keystore

1. Enter the commands to back up the configuration and old keystore files, replace the keystore file, and then update the keystore password:

   - **Linux:**

     ```
     cp /opt/dsm/configuration.properties
     /opt/dsm/configuration.properties.bak
     ```

     ```
     cp /opt/dsm/.keystore /opt/dsm/.keystore.bak
     ```

     ```
     cp ~/.YOUR_PKCS12_EXPORTED_KEYSTORE /opt/dsm/.keystore
     ```

   - **Windows:**

```
copy "C:\Program Files\Trend Micro\Deep Security
Manager\configuration.properties" "C:\Program Files\Trend
Micro\Deep Security Manager\configuration.properties.bak"
```

```
copy "C:\Program Files\Trend Micro\Deep Security
Manager\.keystore" "C:\Program Files\Trend Micro\Deep
Security Manager\.keystore.bak"
```

```
copy "c:\Users\Administrator\.YOUR_PKCS12_EXPORTED_KEYSTORE"
"C:\Program Files\Trend Micro\Deep Security
Manager\.keystore"
```

> **Note:** You **must** overwrite the default keystore file in its original location. Don't configure the path to point to a new filename or different location instead. Deep Security Manager upgrades do not keep keystore path changes, and this will undo the change.

2. In a plaintext editor, open the `configuration.properties` file and update the keystore password setting:

   ```
   keystorePass=YOUR_PASSWORD
   ```
3. Restart the Deep Security Manager service.
4. To verify that the manager now uses the new certificate, open a web browser and connect to the Deep Security Manager console. Click the padlock icon in the location bar and examine the certificate details such as its fingerprint (SHA-256 signature).

## Regenerate self-signed certificates in Deep Security Manager (summary)

Before regenerating a self-signed certificate, you need to backup the old `.keystore` by executing the following commands:

**Linux:**

```
cp /opt/dsm/configuration.properties /opt/dsm/configuration.properties.bak
```

```
cp /opt/dsm/.keystore /opt/dsm/.keystore.bak
```

**Windows:**

```
copy "C:\Program Files\Trend Micro\Deep Security
Manager\configuration.properties" "C:\Program Files\Trend Micro\Deep
Security Manager\configuration.properties.bak"
```

```
copy "C:\Program Files\Trend Micro\Deep Security Manager\.keystore"
"C:\Program Files\Trend Micro\Deep Security Manager\.keystore.bak"
```

Create a new `.keystore`, as follows:

- **Linux:**
  a. On the computer where Deep Security Manager is installed, open the command prompt as an administrator and navigate to the `/opt/dsm/jre/bin` directory.
  b. Execute the following command, replacing the `cn` value to match your Deep Security Manager:

     ```
     keytool -genkey -alias tomcat -keystore ~/.keystore -keyalg
     RSA -validity 365 -keysize 2048 -dname "cn=dsm.example.com,
     ou=IT, o=Trend Micro, l=Ottawa, s=Ontario, c=CA"
     ```

  c. When prompted, enter a password that you will later set in the `/opt/dsm/configuration.properties` file for the `keystorePass` value.
  d. When prompted, enter a key password for tomcat or press Enter to have the same key as the keystore file.
  e. Copy the new keystore to the correct location by executing the following command:

     ```
     cp ~/.keystore /opt/dsm/.keystore
     ```

  f. In the `/opt/dsm/configuration.properties` file, set the keystore password for the `keystorePass` value, and then save the file.
  g. Restart Deep Security Manager.
  h. Verify that the browser can validate the certificate.
- **Windows:**
  a. On the computer where Deep Security Manager is installed, open the command prompt as an administrator and navigate to the `C:\Program Files\Trend Micro\Deep Security Manager\jre\bin` directory.
  b. Execute the following command, replacing the `cn` value to match your Deep Security Manager:

```
keytool -genkey -alias tomcat -keystore
C:\Users\Administrator\.keystore -keyalg RSA -validity 365 -
keysize 2048 -dname "cn=dsm.example.com, ou=IT, o=Trend
Micro, l=Ottawa, s=Ontario, c=CA"
```

c. When prompted, enter a password that you will later set in the `C:\Program Files\Trend Micro\Deep Security Manager\configuration.properties` file for the `keystorePass` value.
d. When prompted, enter a key password for tomcat or press Enter to have the same key as the keystore file.
e. Copy the new keystore to the correct location by executing the following command:

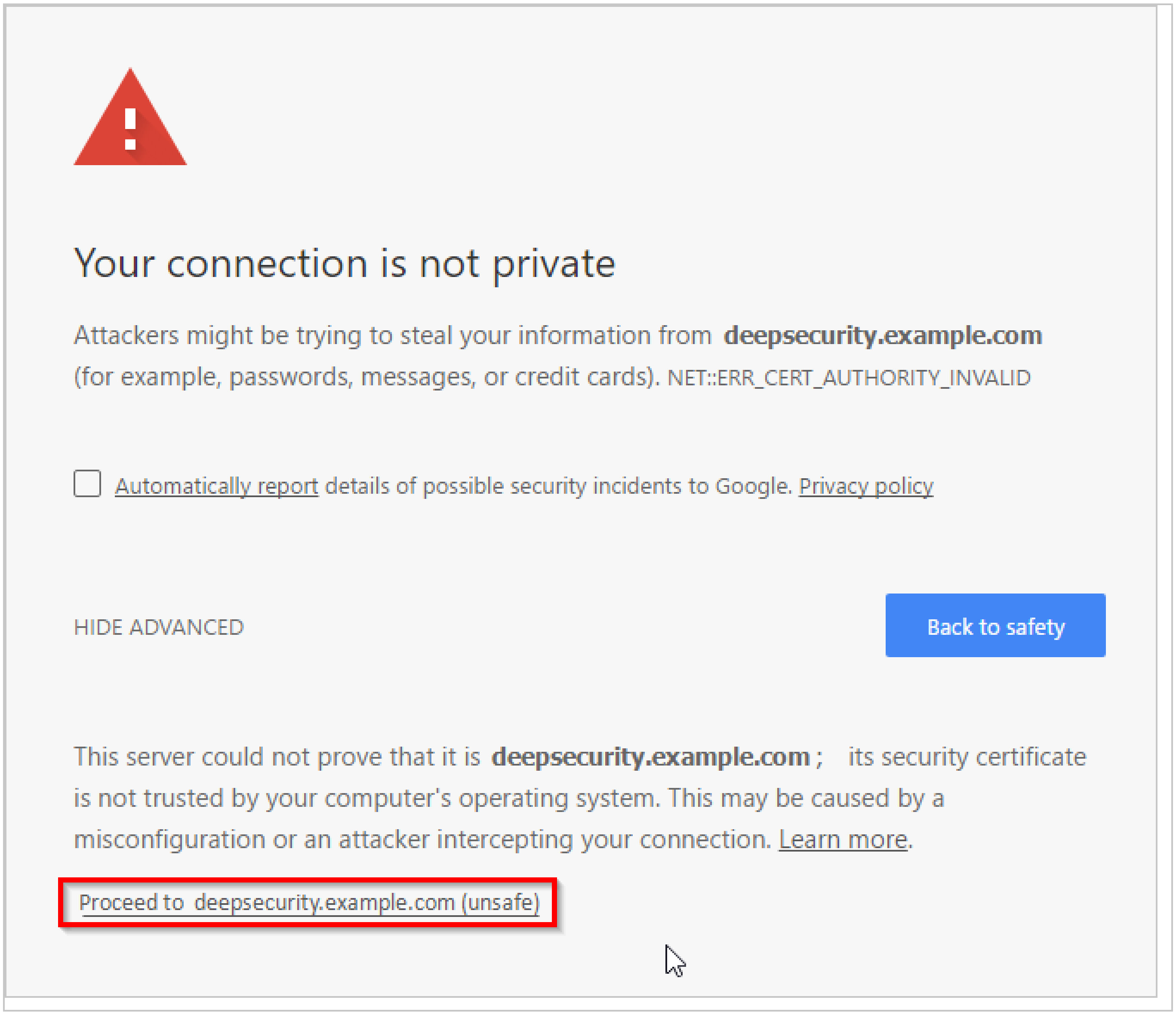
```
copy "c:\Users\Administrator\.keystore" "C:\Program
Files\Trend Micro\Deep Security Manager\.keystore"
```

f. In the `C:\Program Files\Trend Micro\Deep Security Manager\configuration.properties` file, set the keystore password for the `keystorePass` value, and then save the file.
g. Restart Deep Security Manager.
h. Verify that the browser can validate the certificate.

## Update the load balancer's certificate

Usually, your browser should warn you with a certificate validation error whenever you try to connect to a server with a self-signed certificate. This is because with any *self*-signed certificate, the browser cannot automatically validate the certificate's signature with a trusted *third party* certificate authority (CA), and therefore the browser doesn't know if the certificate was sent by an attacker or not. When installed, Deep Security Manager is initially configured to use a self-signed certificate for HTTPS connections (SSL or TLS), so you must manually verify that the server certificate fingerprint used to secure the connection belongs to your Deep Security server. This is normal until you replace the self-signed certificate with a CA-signed certificate.

The same error will occur if you have an AWS Elastic Load Balancer (ELB) or other load balancer, and it presents a self-signed certificate to the browser.



Your connection is not private

Attackers might be trying to steal your information from **deepsecurity.example.com** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically report details of possible security incidents to Google. Privacy policy

This server could not prove that it is **deepsecurity.example.com** ; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection. Learn more.

You can still access Deep Security Manager if you ignore the warning and proceed (method varies by browser). However, this error will occur again each time you connect, unless you either:

- add the certificate to your computer's store of trusted certificates (not recommended) or
- replace the load balancer's certificate with one signed by a trusted CA (strongly recommended)

1. With a CA that is trusted by all HTTPS clients, register the fully qualified domain name (*not IP address*) that administrators, relays, and agents will use to connect to Deep Security Manager.

   Specify the sub-domain (for example, deepsecurity.example.com) that will uniquely identify Deep Security Manager. For nodes behind an SSL terminator load balancer, this certificate will be presented to browsers and other HTTPS clients by the load balancer, not by each Deep Security Manager node.

   When the CA signs the certificate, download both the certificate (with public key) and the private key.

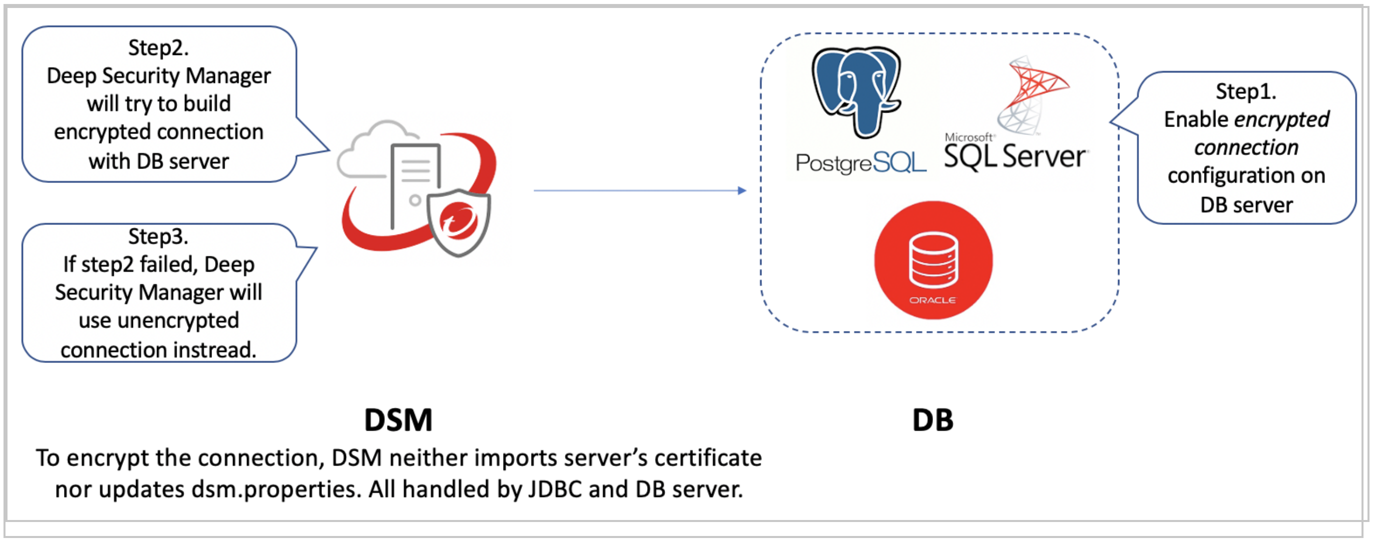
   > **Warning:** Store and transmit the private key securely. If file permissions or unencrypted connections allow a third party to access your private key, then all connections secured by that certificate and key are compromised. You must revoke that certificate, remove the key, and get a new certificate and key.

2. Add the certificate to your certificate store (optional if your computer trusts the CA that signed the certificate).
3. Update the DNS settings of the load balancer to use the new domain name.
4. Replace the SSL certificate of the load balancer.

## Encrypt communication between the Deep Security Manager and the database

If the communication channel between the Deep Security Manager and the database is not secure, you may wish to encrypt the communications between them. In the current design, Deep Security Manager first attempts to build an encrypted connection with the database server. If it fails, Deep Security Manager uses an unencrypted connection with the database server instead.

The related mechanisms are built into the database library that Deep Security Manager is based on, therefore the server certificate doesn't need to be imported and the configuration file doesn't need to be updated. You should consult with the database vendor and their supporting documentation to determine if there will be any significant performance impact when enabling encrypted sessions.


Step2.
Deep Security Manager will try to build encrypted connection with DB server
Step3.
If step2 failed, Deep Security Manager will use unencrypted connection instread.
PostgreSQL
Microsoft SQL Server
ORACLE
Step1.
Enable *encrypted connection* configuration on DB server
DSM
DB
To encrypt the connection, DSM neither imports server's certificate nor updates dsm.properties. All handled by JDBC and DB server.

The instructions vary depending on the database you are using:

- "Microsoft SQL Server database" below
- "Oracle database" on the next page
- "PostgreSQL" on the next page

**Note:** If you are running the Deep Security Manager in multi-node mode, these changes must be made on each node.

This section also provides information on "Running an agent on the database server" on page 1509how to "Disable encryption between the manager and database" on page 1509, and how to "Upgrade from an old Deep Security Manager version" on page 1511.

## Encrypt communication between the manager and database

### Microsoft SQL Server database

If you have **not** already installed Deep Security Manager 20:

1. Follow the instructions in Enable encrypted connections to the Database Engine on the Microsoft MSDN site and enable encrypted connection options on Microsoft SQL Server.

By default, the communication between Deep Security Manager 20 and Microsoft SQL Server is encrypted.

If you have **already** installed Deep Security Manager 20 and you haven't enabled encryption options on your Microsoft SQL Server:

1. Stop Deep Security Manager 20.
2. Follow the instructions in Enable encrypted connections to the Database Engine on the Microsoft MSDN site and enable encrypted connection options on Microsoft SQL Server.
3. "Restart the Deep Security Manager" on page 1560.

By default, the communication between Deep Security Manager 20 and Microsoft SQL Server is encrypted.

> **Note:** You can use SQL Server Manager Studio to connect your Microsoft SQL Server. Use the command `select client_net_address,connect_time,net_transport,protocol_type,encrypt_option from sys.dm_exec_connections` to see if your Deep Security Manager encrypted connection is working or not.

## Oracle database

If you have **not** already installed Deep Security Manager 20:

1. Follow the instructions How To Configure Data Encryption and Integrity on the Oracle Help Center, and enable encrypted connection options on Oracle Database Server side.

By default, the communication between Deep Security Manager 20 and Oracle Database Server is encrypted.

If you have **already** installed Deep Security Manager 20 and you haven't enabled encryption options on your Oracle Database Server:

1. Stop Deep Security Manager 20.
2. Follow the instructions How To Configure Data Encryption and Integrity  on the Oracle Help Center, and enable encrypted connection options on Oracle Database Server side.
3. "Restart the Deep Security Manager" on page 1560.

By default, the communication between Deep Security Manager 20 and Oracle Database Server is encrypted.

> **Note:** Follow the Oracle blog article Verifying the use of Native Encryption and Integrity to see if the encrypted connection is working or not.

## PostgreSQL

If you have not already installed Deep Security Manager 20:

1. Turn on SSL in PostgreSQL. For on-premises PostgreSQL database, see Secure TCP/IP Connections with SSL for more information. For an Amazon RDS for PostgreSQL, see Using SSL with a PostgreSQL DB Instance for more information.

By default, the communication between Deep Security Manager 20 and PostgreSQL Database Server is encrypted.

If you have already installed Deep Security Manager 20 and you haven't enabled encryption options on your PostgreSQL Database Server:

1. Stop Deep Security Manager 20.
2. Turn on SSL in PostgreSQL. For on-premises PostgreSQL database, see Secure TCP/IP Connections with SSL for more information. For an Amazon RDS for PostgreSQL, see Using SSL with a PostgreSQL DB Instance for more information.
3. "Restart the Deep Security Manager" on page 1560.

By default, the communication between Deep Security Manager 20 and PostgreSQL Database Server is encrypted.

**Note:** To check that the manager is connected using TLS, use the following query and check the SSL column: `select a.client_addr, a.application_name, a.usename, s.* from pg_stat_ssl s join pg_stat_activity a using (pid) where a.datname='<Deep Security database name>';`

## Running an agent on the database server

Encryption should be enabled if you are using an agent to protect the database. When you perform a security update, the Deep Security Manager stores new Intrusion Prevention rules in the database. The rule names themselves will almost certainly generate false positives as they get parsed by the agent if the data is not encrypted.

## Disable encryption between the manager and database

In rare cases, you may need to disable encryption between Deep Security Manager and the database. For example, if you're using an older version of SQL Server, you may need to disable encryption to avoid connection errors. For details, see Error: The installer could not establish a secure connection to the database server.

Follow the instructions for your database type to disable encryption.

## Microsoft SQL Server

1. Stop the Deep Security Manager service.
2. In the SQL Server, disable the "Force Encryption" option that was enabled in Enable encrypted connections to the Database Engine.
3. (Optional) If your Deep Security Manager 20 was upgraded from Deep Security Manager 12.5 or older, remove all encryption related configurations in `dsm.properties`:

   ```
   database.SqlServer.encrypt=true
   ```

   ```
   database.SqlServer.trustServerCertificate=true
   ```

   > **Note:** If you upgraded from Deep Security 10.1 or a previous version, and your connection to the database uses named pipes as the transport, remove the following line instead: `database.SqlServer.ssl=require`

4. Restart Microsoft SQL Server if necessary.
5. Start Deep Security Manager.

### Oracle Database

1. Stop the Deep Security Manager service.
2. Follow How To Configure Data Encryption and Integrity to disable the connection encryption in the Oracle server.
3. (Optional) If your Deep Security Manager 20 was upgraded from Deep Security Manager 12.5 or older, remove all encryption related configurations in `dsm.properties`:

   ```
   database.Oracle.oracle.net.encryption_types_client=(AES256)
   ```

   ```
   database.Oracle.oracle.net.encryption_client=REQUIRED
   ```

   ```
   database.Oracle.oracle.net.crypto_checksum_types_client=(SHA1)
   ```

   ```
   database.Oracle.oracle.net.crypto_checksum_client=REQUIRED
   ```

4. Restart the Oracle listener.
5. Start the Deep Security Manager service.

### PostgreSQL

1. Stop the Deep Security Manager service.
2. Follow Secure TCP/IP Connections with SSL to remove `ssl=on in postgresql.conf` and disable the connection encryption in the PostgrSQL database.
3. (Optional) If your Deep Security Manager 20 was upgraded from Deep Security Manager 12.5 or older, remove all encryption related configurations in `dsm.properties`:

```
database.PostgreSQL.connectionParameters=ssl=true
```

4. Restart the PostgreSQL service.
5. Start the Deep Security Manager service.

## Upgrade from an old Deep Security Manager version

If you're currently using Deep Security Manager 12.5 or older and meet the following criteria:

- Encrypted connection is enabled.
- Uses PostgreSQL database server.

Please follow the instructions below before upgrading.

If either of the above criteria is not satisfied, you can ignore the following section and upgrade straight to Deep Security Manager 20.0.

### Upgrade Deep Security Manager

Since PostgreSQL JDBC driver has different behaviors in different versions, you need to complete the following steps before upgrading.

1. Export the certificate from your PostgreSQL database server. (This should already be completed because the old Deep Security Manager requires the certificate to enable connection encryption).
2. Rename the certificate file as `root.crt` .
3. Put it in the predefined Deep Security Manager 20 path:

   In Linux, put `root.crt` in `~/.postgresql/`

   In Windows, put `root.crt` in `c:\Users\{USERNAME}\AppData\Roaming\postgresql\`.
4. Run the upgrade flow. Deep Security Manager 20 will continue to use an encrypted connection with PostgreSQL server after upgrade.

# Change the Deep Security Manager database password

Your organization's security policies may require that you periodically change the password that Deep Security Manager uses to access the database.

- "Change your Microsoft SQL Server password" on the next page
- "Change your Oracle password" on the next page

- "Change your PostgreSQL password" on the next page

## Change your Microsoft SQL Server password

1. On Windows, stop the Trend Micro Deep Security Manager service on each of your Deep Security Manager instances.

   On Linux, the command to stop the service is:

   ```
   # service dsm_s stop
   ```

2. Use SQL Server Management Studio to change the SQL user password.
3. On each Deep Security Manager instance, modify the `/opt/dsm/webclient/webapps/ROOT/WEB-INF/dsm.properties` file to specify the new password. When you open this file, you will see an obfuscated value for the password, similar to this:

   ```
   database.SqlServer.password=$1$4ec04f9550e0bf378fa6b1bc9698d0bbc59ac010bfef7ea1e6e47f30394800b1a9554fe206a3ee9ba5f774d205ba03bb86c91c0664c7f05f8c467e03e0d8ebbe
   ```

   Overwrite that value with your new password (the new password will be obfuscated when the service restarts):

   ```
   Database.SqlServer.password=NEW PASSWORD GOES HERE
   ```

4. On Windows, start the Trend Micro Deep Security Manager service on each of your Deep Security Manager instances.

   On Linux, the command to start the service is:

   ```
   # service dsm_s start
   ```

## Change your Oracle password

1. On Windows, stop the Trend Micro Deep Security Manager service on each of your Deep Security Manager instances.

   On Linux, the command to stop the service is:

   ```
   # service dsm_s stop
   ```

2. Use your Oracle tools to change the password.

3. On each Deep Security Manager instance, modify the `/opt/dsm/webclient/webapps/ROOT/WEB-INF/dsm.properties` file to specify the new password. When you open this file, you will see an obfuscated value for the password, similar to this:

   ```
   database.Oracle.password=$1$4ec04f9550e0bf378fa6b1bc9698d0bbc59ac010bfef7ea1e6e47f30394800b1a9554fe206a3ee9ba5f774d205ba03bb86c91c0664c7f05f8c467e03e0d8ebbe
   ```

   Overwrite that value with your new password (the new password will be obfuscated when the service restarts):

   ```
   Database.Oracle.password=NEW PASSWORD GOES HERE
   ```

4. On Windows, start the Trend Micro Deep Security Manager service on each of your Deep Security Manager instances.

   On Linux, the command to start the service is:

   ```
   # service dsm_s start
   ```

## Change your PostgreSQL password

1. On Windows, stop the Trend Micro Deep Security Manager service on each of your Deep Security Manager instances.

   On Linux, the command to stop the service is:

   ```
   # service dsm_s stop
   ```

2. Follow instructions from your PostgreSQL documentation to change the password.
3. On each Deep Security Manager instance, modify the `/opt/dsm/webclient/webapps/ROOT/WEB-INF/dsm.properties` file to specify the new password. When you open this file, you will see an obfuscated value for the password, similar to this:

   ```
   database.PostgreSQL.password=$1$4ec04f9550e0bf378fa6b1bc9698d0bbc59ac010bfef7ea1e6e47f30394800b1a9554fe206a3ee9ba5f774d205ba03bb86c91c0664c7f05f8c467e03e0d8ebbe
   ```

   Overwrite that value with your new password (the new password will be obfuscated when the service restarts):

   ```
   Database.PostgreSQL.password=NEW PASSWORD GOES HERE
   ```

4. On Windows, start the Trend Micro Deep Security Manager service on each of your Deep Security Manager instances.

   On Linux, the command to start the service is:

   ```
   # service dsm_s start
   ```

# Configure HTTP security headers

Security headers are directives used by web applications to configure security defenses in web browsers. Based on these directives, browsers can make it harder to exploit client-side vulnerabilities such as Cross-Site Scripting or Clickjacking. Headers can also be used to configure the browser to only allow valid TLS communication and enforce valid certificates, or even enforce using a specific server certificate.

The sections below detail the various security headers and support for them in Deep Security:

- "Customizable security headers" below
- "Enforced security headers" on page 1517
- "Unsupported security headers" on page 1518

## Customizable security headers

The following headers can be enabled and configured based on specific environment requirements:

- "HTTP Strict Transport Security (HSTS)" below
- "Content Security Policy (CSP)" on the next page
- "HTTP Public Key Pinning (HPKP)" on page 1516

> **Note:** As the primary tenant, you can "Enable customizable security headers" on page 1516 in the Deep Security Manager or "Reset your configuration" on page 1517.

### HTTP Strict Transport Security (HSTS)

HTTP Strict Transport Security is a header that configures the web browser to always use a valid secure connection with the web application. If the server TLS certificate suddenly becomes expired or untrusted, the browser will no longer connect to the web application. Also, if the user attempts to access the web application using an `http://` url, the browser will automatically change it to `https://`. These countermeasures help prevent Man-in-the-middle attacks as well as other attacks such as Session Hijacking.

On install, the Deep Security Manager console has a self-signed (untrusted) certificate and HSTS is turned off. This is because each organization must configure the Deep Security web application with a specific certificate that matches the manager hostname. This can also be achieved by configuring a Load Balancer with TLS termination such as AWS ELB/ALB.

Once a valid TLS configuration is in place, the HTTP Strict Transport Security Header can be enabled from **Administration > System Settings > Security**.

For instructions on enabling HTTP Strict Transport Security (HSTS), see "Enable customizable security headers" on the next page.

## Content Security Policy (CSP)

Content Security Policy includes a comprehensive set of directives that help prevent client-side attacks, such as Cross-Site Scripting and Clickjacking, by restricting the type of content the browser is allowed to include or execute.

> **Note:** Enabling CSP can have adverse effects. For example, embedded scripts might stop working or certain types of images required by third-party components such as jQuery might not load.

When you enable CSP, it is always a good idea to run it in **Report only** first and observe if any violations are reported to the provided URL for expected application functionality.

The Deep Security CSP can be configured under **Administration > System Settings > Security**.

Deep Security works best with the following settings:

```
object-src 'self'
```

```
default-src 'self'
```

```
script-src 'self' 'unsafe-eval' 'unsafe-inline'
```

```
frame-src 'self'
```

```
frame-ancestors 'self'
```

```
style-src 'self' 'unsafe-inline' blob:
```

```
form-action 'self'
```

```
img-src 'self' data:
```

```
report-uri https://your_report_uri.org/DS_CSP_Violation
```

**Note:** By default, the **Report only** check box is selected. Once you confirm that the CSP does not break the expected application functionality, you can deselect **Report only** to enforce the policy.

**Warning:** Currently, **script-src** does not support 'nonce' or 'harsh-algorithm'. If you have concerns about cross-site scripting (XSS), enable the Intrusion Prevention rule **1000552 - Generic Cross Site Scripting (XSS) Prevention**.

For instructions on enabling Content Security Policy (CSP), see "Enable customizable security headers" below.

## HTTP Public Key Pinning (HPKP)

The HPKP header forces browsers to only trust a specific certificate or certificate authority for secure communications. This prevents attacks that leverage a trusted certificate authority which has been compromised or maliciously installed on the client.

**Note:** Enabling HPKP can leave browsers unable to connect if a certificate is changed without its header also being changed.

For instructions on enabling HTTP Public Key Pinning (HPKP), see "Enable customizable security headers" below.

### Enable customizable security headers

**Note:** In multi-tenant mode, security header settings are only available to the primary tenant.

1. Go to **Administration** > **System Settings** > **Security**.
2. Enter your HTTP Strict Transport Security (HSTS), Content Security Policy (CSP), or HTTP Public Key Pinning (HPKP) directive(s) in the corresponding field(s).

   **Note:** Before you enable settings, you can test them by selecting the **Report Only** option and verifying that the policy violation reports are correct.

   **Tip:** You can enter individual policy directives on separate lines.
3. Click **Save** at the bottom of the page.

#### Reset your configuration

If you experience trouble while configuring your directive and cannot correct it in the Deep Security Manager, SSH into the manager and run the corresponding commands to reset your configuration:

### HTTP Strict Transport Security

```
dsm_c -action changesetting -name
settings.configuration.enableHttpStrictTransportSecurity -value ""
```

```
dsm_c -action changesetting -name
settings.configuration.enableHttpStrictTransportSecurity -value "false"
```

### Content Security Policy

```
dsm_c -action changesetting -name
settings.configuration.contentSecurityPolicy -value ""
```

```
dsm_c -action changesetting -name
settings.configuration.contentSecurityPolicyReportOnly -value "true"
```

### Public Key Pinning Policy

```
dsm_c -action changesetting -name settings.configuration.publicKeyPinPolicy -
value ""
```

```
dsm_c -action changesetting -name
settings.configuration.publicKeyPinPolicyReportOnly -value "true"
```

## Enforced security headers

The following headers are enforced by default and cannot be changed:

- "Cache-Control and Pragma" below
- "X-XSS-Protection" on the next page
- "X-Frame-Options" on the next page

### Cache-Control and Pragma

These headers configure how the browser caches content. Caching sensitive content from an authenticated application can be a security vulnerability if the content is cached on a machine that is used by multiple users or if an attacker gains access to an unlocked machine after the user has logged out of the application. For this reason, Deep Security disables caching on all content that is not static by enforcing the `no-cache` and `no-store` values.

### X-XSS-Protection

This XSS-Protection header forces the browser's Cross-Site Scripting (XSS) heuristics to detect XSS attacks. Deep Security enforces this header in block mode by default. This means that if the browser detects a potential XSS attack it will stop the page from loading altogether–a safer approach than the alternative of trying to sanitize the page by replacing potentially malicious elements.

> **Note:** XSS-Protection does not work for all types of attacks and not all browsers have an XSS filter.

### X-Frame-Options

This header helps to prevent Clickjacking attacks. The Deep Security Manager enforces the `SAMEORIGIN` value for this header, only allowing it to be embedded in web applications that are hosted on the same domain.

> **Note:** This header has the same effect as the frame-ancestors CSP directive. The frame-ancestors directive will override the value of the X-Frame-Options header.

## Unsupported security headers

The following header type is unsupported.

### X-Content-Type-Options

This header with the `nosniff` value helps protect against mime type sniffing. Mime type sniffing attacks are only effective in specific scenarios where they cause the browser to interpret text or binary content as HTML. For example, if a user uploads an avatar file named `xss.html` and the web application does not set a Content-type header when serving the image, the browser will try to determine the content type and will likely treat `xss.html` as an HTML file. The attacker can then direct users to `xss.html` and conduct a Cross-Site Scripting attack.

Deep Security does not currently support enabling this header as it has been observed to cause adverse effects on redirects, however the relevant attack scenarios are not likely to impact the manager web application and its usual functionality.

# Enforce user password rules

You can specify password requirements for Deep Security Manager passwords, and other settings related to user authentication.

## Specify password requirements

> **Note:** For greater security, enforce stringent password requirements: minimum 8 characters, include both numbers and letters, use upper and lower case, include non-alphanumeric characters, and expire regularly.

Go to **Administration > System Settings > Security**. In the **User Security** section, you can change these settings:

- **Session idle timeout:** Specify the period of inactivity after which a user will be required to sign in again.
- **Maximum session duration:** Maximum length of time that a user can be signed into the Deep Security Manager before they'll be required to sign in again.
- **Number of incorrect sign-in attempts allowed (before lock out):** The number of times an individual user (i.e. with a specific username) can attempt to sign in with an incorrect password before they are locked out. Only a user with "Can Edit User Properties" rights can unlock a locked-out user (see "Define roles for users" on page 1415).

  > **Note:** If a user gets locked out for a particular reason (too many failed sign-in attempts, for example), and no user remains with the sufficient rights to unlock that account, please contact Trend Micro for assistance.

- **Number of concurrent sessions allowed per User:** Maximum number of simultaneous sessions allowed per user.

  > **Note:** A note about being signed in as two users at once: Remember that Firefox sets session cookies on a per-process basis, and not on a per-window basis. This means that if for some reason you want to be signed in as two users at the same time, you will either have to use two different browsers (if one of them is Firefox), or sign in from two separate computers.

- **Action when concurrent session limit is exceeded:**Specifies what happens when a user reaches the maximum number of concurrent sessions.

- **User password expires:** Number of days that passwords are valid. You can also set passwords to never expire.
- **User password minimum length:** The minimum number of characters required in a password.
- **User password requires both letters and numbers:** Letters (a-z, A-Z) as well as numbers (0-9) must be used as part of the password.
- **User password requires both upper and lower case characters:** Upper and lower case characters must be used.
- **User password requires non-alphanumeric characters:** Passwords must include non-alphanumeric characters.
- **Send email when a user's password is about the expire:** Before a user's password expires, they will receive an email message. To use this feature, you must "Configure SMTP settings for email notifications" on page 1186.

## Use another identity provider for sign-on

You can also configure Deep Security to use SAML single sign-on. For details, see "Configure SAML single sign-on" on page 1435.

## Add a message to the Deep Security Manager Sign In page

On the **Administration > System Settings > Security** page, use **Sign-In Page Message** to enter text that will be displayed on the Deep Security Manager's sign in page.

## Present users with terms and conditions

You can configure Deep Security Manager so that users must agree to terms and conditions before they can sign in to the Deep Security Manager.

To enable this feature, select **User must agree to the terms and conditions** on the **Administration > System Settings > Security** page. In the two text boxes, enter a title and the list of terms and conditions that will be displayed when a user clicks the **Terms and Conditions** link on the Sign In page.

## Other Security settings

The **Administration > System Settings > Security** page also enables you to:

- "Manage trusted certificates" on page 1525
- "Configure HTTP security headers" on page 1514

# Set up multi-factor authentication

The Deep Security Manager allows you the option to use multi-factor authentication (MFA). MFA is a method of access control requiring more than a user name and password that is recommended as a best practice.

In this article:

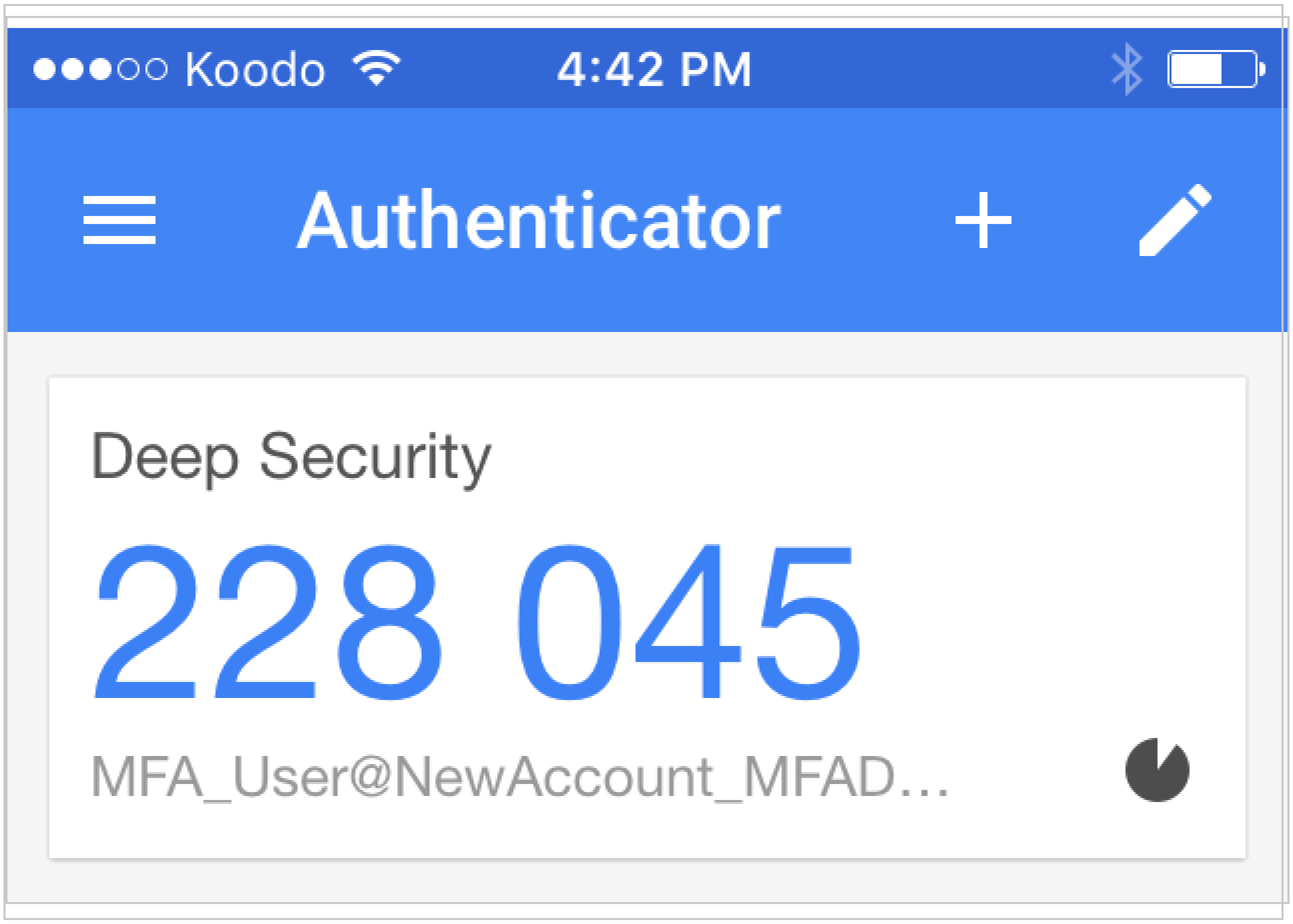
- "Enable multi-factor authentication" below
- "Disable multi-factor authentication" on page 1524
- "Supported multi-factor authentication (MFA) applications" on page 1524
- "Troubleshooting MFA" on page 1525

## Enable multi-factor authentication

1. In Deep Security Manager, select **User Properties** from the menu under your user name in the upper-right corner.
2. On the **General** tab, click the **Enable MFA** button. This will open the **Enable Multi-Factor Authentication** wizard to guide you through the rest of the process.
3. The first screen of the wizard will remind you to install a compatible virtual MFA application, such as Google Authenticator. For more information, see "Supported multi-factor authentication (MFA) applications" on page 1524 at the bottom of this article.
4. If your device supports scanning QR codes, you can use your camera to configure your MFA application and click **Next**.

   Otherwise, you can choose **My device does not support scanning QR codes. Show secret key for manual time-based configuration**.

5. Enter the **Authentication Code** (without the space), for example: 228045.

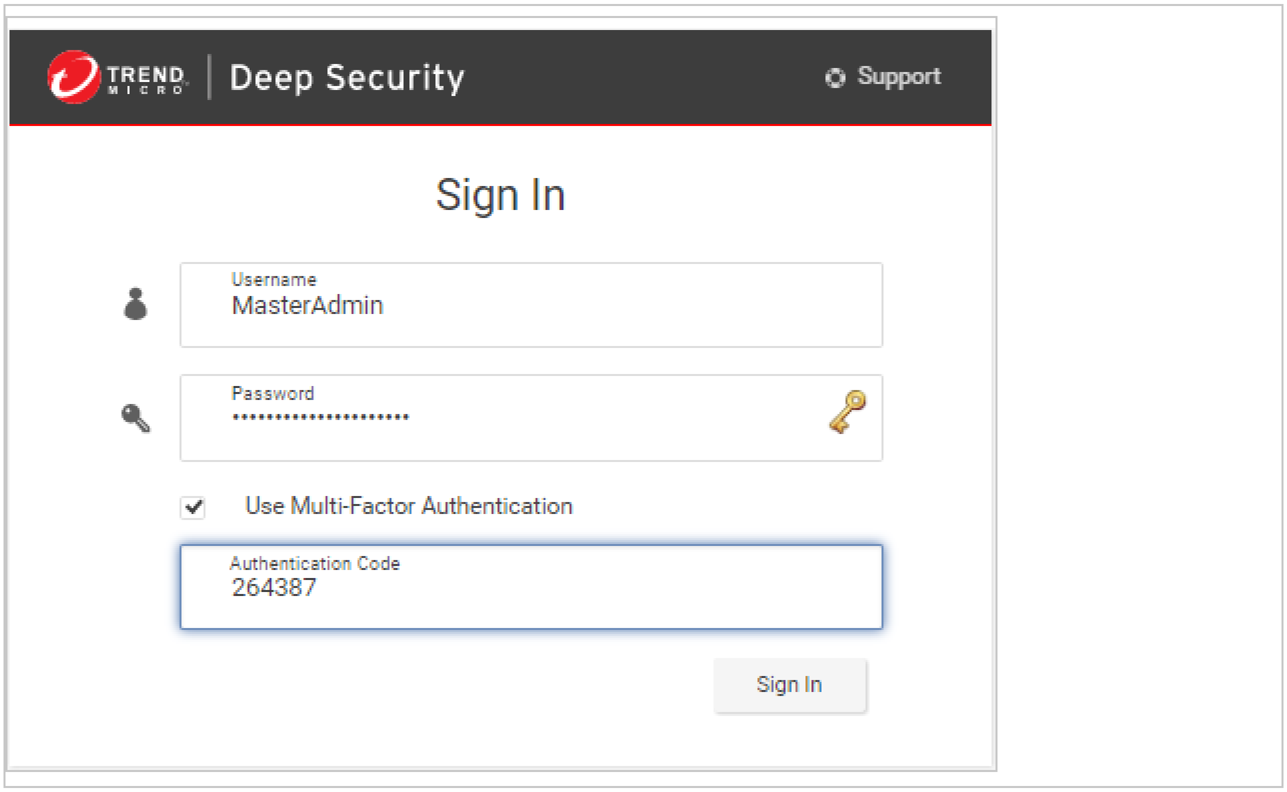


Deep Security

228 045

MFA_User@NewAccount_MFAD…

6. If the authorization code is correct, MFA will be enabled for your account and you will be required to enter a new MFA code each time you sign in.



Username
MasterAdmin

Password
••••••••••••••••••••••

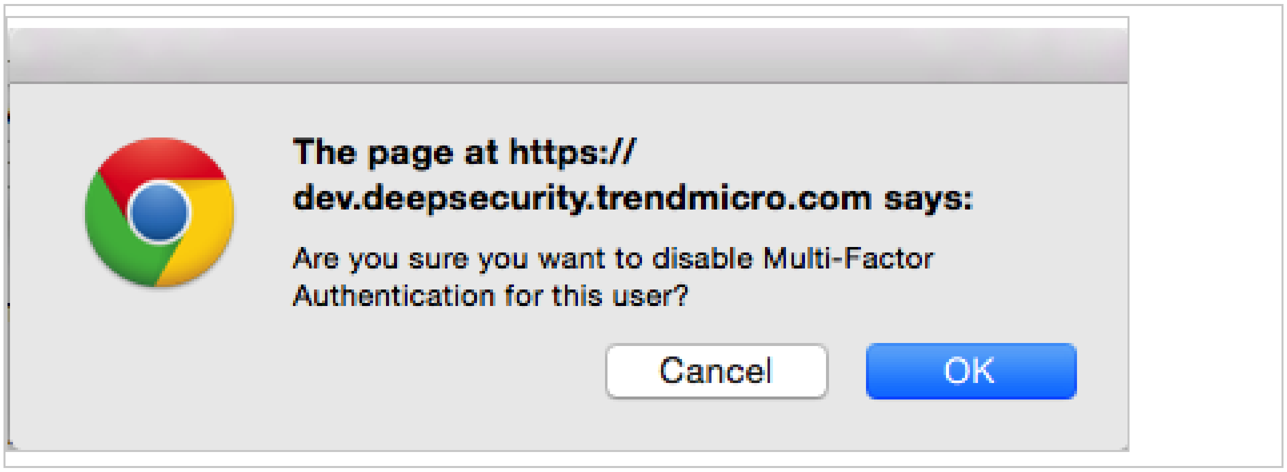
☑ Use Multi-Factor Authentication

Authentication Code
264387

## Disable multi-factor authentication

1. In the Deep Security Manager, select **User Properties** from the menu under your user name in the upper-right corner.

2. On the **General** tab, click the **Disable MFA** button.
3. Click **OK** on the confirmation screen to disable MFA.



The page at https://
dev.deepsecurity.trendmicro.com says:

Are you sure you want to disable Multi-Factor Authentication for this user?

4. Your user properties screen displays with a note to indicate the changes to MFA. Click **OK** to close the screen.

## Supported multi-factor authentication (MFA) applications

The following smartphones and applications are actively supported for MFA. However, any application implementing an RFC 6238 compliant Time-base One-time Password Algorithm should work.

| Smartphone | MFA App |
|---|---|
| Android | Google Authenticator, Duo |
| iPhone | Google Authenticator, Duo |
| Blackberry | Google Authenticator |

## Troubleshooting MFA

### What if my MFA is enabled but not working?

The most common source of MFA login issues is caused by the time on your Deep Security Manager being out of sync with your device.

Follow the instructions below for your chosen operating system to make sure the time is properly synced:

**If your Deep Security Manager is Linux:**

Check that NTP is working correctly by entering `ntpstat` in the command line. To view the current system time and date, enter `date`.

**If your Deep Security Manager is Windows:**

Check that the Windows Time Service is working correctly. To view the current system time and date, enter `time` and `date` in the command line.

### What if my MFA device is lost or stops working?

If your MFA device is lost, destroyed, or stops working, you'll need to have MFA disabled for your account in order to be able to sign in.

1. Get in touch with the person who provided you with your sign in credentials and ask them to follow the instructions in "Disable multi-factor authentication" on the previous page. (You'll then be able to sign in with just your user name and password.)
2. After you've signed in, change your password.
3. Follow the instructions for "Enable multi-factor authentication" on page 1521.

# Manage trusted certificates

Trusted certificates are used for code signing and SSL connections to external services such as a Microsoft Active Directory. They are also used to exclude files from Anti-Malware scanning.

## Import trusted certificates

> **Note:** If you are importing a trusted certificate to establish trust with an Amazon Web Services region, you must use the `dsm_c` command-line tool.

**To import trusted certificates using the Deep Security Manager:**

1. In the Deep Security Manager, go to **Administration** > **System Settings** > **Security**.
2. Under **Trusted Certificates**, click **View Certificate List** to view a list of all security certificates accepted by Deep Security Manager.
3. Click **Import From File** to start the Import Certificate wizard.

**To import a trusted certificate using dsm_c:**

1. On the Deep Security Manager server, run the following command:

```
dsm_c -action addcert -purpose PURPOSE -cert CERTFILE
```

where the parameters are:

| Parameter | Description | Sample value |
|---|---|---|
| PURPOSE | What type of connections the certificate will be used for. This value must be selected from one of the sample values listed on the right. | `AWS` - Amazon Web Services |
| | | `DSA` - code signing |
| | | `EXCEPTION` - scan exclusion |
| | | `SSL` - SSL connections |
| CERTFILE | The (user-defined) name of the file containing the certificate you want to import. | `/path/to/cacert.pem` |

**Note:** If you are running the Deep Security Manager in a Linux environment, you will need to run the `dsm_c` command as the root user.

## View trusted certificates

**Note:** To view trusted certificates for Amazon Web Services connections, you must use the `dsm_c` command-line tool.

**To view trusted certificates using the Deep Security Manager:**

1. In the Deep Security Manager, go to **Administration** > **System Settings** > **Security**.
2. Under **Trusted Certificates**, click **View Certificate List**.

**To view trusted certificates using dsm_c:**

1. On the Deep Security Manager server, run the following command:

   ```
   dsm_c -action listcerts [-purpose PURPOSE]
   ```

   The `-purpose PURPOSE` parameter is optional and can be omitted to see a list of all certificates. If you specify a value for `PURPOSE`, then only the certificates used for that purpose will be shown.

| Parameter | Description | Sample value |
|---|---|---|
| PURPOSE | What type of connections the certificate will be used for. | `AWS` - Amazon Web Services |
| | | `DSA` - code signing |
| | | `EXCEPTION` - scan exclusion |
| | | `SSL` - SSL connections |

**Note:** If you are running the Deep Security Manager in a Linux environment, you will need to run the `dsm_c` command as the root user.

## Remove trusted certificates

**Note:** To remove trusted certificates for Amazon Web Services connections, you must use the `dsm_c` command-line tool.

**To remove a trusted certificate using the Deep Security Manager:**

1. In the Deep Security Manager, go to **Administration** > **System Settings** > **Security**.
2. Under **Trusted Certificates**, click **View Certificate List**.
3. Select the certificate you want to remove and click **Delete**.

**To remove a trusted certificate using dsm_c:**

1. Log in to Deep Security Manager .
2. Run the following command:

   ```
   dsm_c -action listcerts [-purpose PURPOSE]
   ```

   The `-purpose PURPOSE` parameter is optional and can be omitted to see a list of all certificates. If you specify a value for `PURPOSE`, then only the certificates used for that purpose will be shown.

| Parameter | Description | Sample value |
|---|---|---|
| PURPOSE | What type of connections the certificate will be used for. | `AWS` - Amazon Web Services |
| | | `DSA` - code signing |
| | | `EXCEPTION` - scan exclusion |
| | | `SSL` - SSL connections |

3. Find the `ID` value for the certificate you want to remove in the list.
4. Run the following command:

```
dsm_c -action removecert -id ID
```

The `ID` parameter value is required.

| Parameter | Description | Sample value |
|---|---|---|
| ID | The ID value assigned by Deep Security Manager for the certificate you want to delete. | `3` |

**Note:** If you are running the Deep Security Manager in a Linux environment, you will need to run the `dsm_c` commands as the root user.

## SSL implementation and credential provisioning

Deep Security Agent may initiate communication to Deep Security Manager or it may be contacted by the manager if the computer object is set to operate in bi-directional mode. Deep Security Manager treats all connections to agents in a similar way. If the agent has not been activated, a limited set of interactions is possible. If the agent has been activated (either by an administrator or via the agent-initiated activation feature), the full set of interactions is enabled. Deep Security Manager acts as an HTTP client in all cases, regardless of whether or not it was the client when forming the TCP connection. Agents cannot ask for data or initiate operations themselves. The manager requests information such as events and status, invokes operations, or pushes configuration to the agent. This security domain is highly controlled to ensure that agents have no access to Deep Security Manager or the computer on which it is running.

Both agent and manager use two different security contexts to establish the secure channel for HTTP requests:

1. Before activation, the agent accepts the bootstrap certificate to form the SSL or TLS channel.
2. After authentication, mutual authentication is required to initiate the connection. For mutual authentication, the manager's certificate is sent to the agent and the agent's certificate is sent to the manager. The agent validates that the certificates come from the same certificate authority (which is the Deep Security Manager) before privileged access is granted.

Once the secure channel is established, the agent acts as the server for the HTTP communication. It has limited access to the manager and can only respond to requests. The secure channel provides authentication, confidentiality through encryption, and integrity. The use of mutual authentication protects against man-in-the-middle (MiTM) attacks where the SSL communication channel is proxied through a malicious third party. Within the stream, the inner content uses GZIP and the configuration is further encrypted using PKCS #7.

It is not recommended to perform SSL/TLS decryption of communications between Deep Security products. Any device or middleware should be configured for TLS passthrough. For instance, if a firewall performs SSL inspection, it decrypts and then re-encrypts the communication, altering the certificate in the process. This alteration causes the certificate to differ from the original one provided. As a result, when the communication from Deep Security Agent reaches Deep Security Manager, the altered certificate is deemed unauthorized.

## If I have disabled the connection to the Smart Protection Network, is any other information sent to Trend Micro?

When Smart Protection Network is disabled, the Deep Security Agents will not send any threat intelligence information to Trend Micro.

# Upgrade Deep Security

## About upgrades

Types of Deep Security updates from Trend Micro include:

- **Software upgrades:** New software such as the Deep Security Manager, Agent and Relay.
- **Security updates:** Rules and malware patterns that Deep Security Agent software uses to identify potential threats. Types of security updates include:
  - **Pattern updates**: Used by Anti-Malware.
  - **Rule updates**: Used by:
    - Firewall
    - Intrusion Prevention
    - Integrity Monitoring
    - Log Inspection

Application Control rule updates are created locally, based on your computers' software. They are not from Trend Micro.

The Anti-Malware engine in agent software can be updated independently to keep up with the newest threats. See "Enable automatic Anti-Malware engine updates" on page 1537.

Trend Micro releases new rule updates every Tuesday, with additional updates as new threats are discovered. Information about the updates is available in the Trend Micro Threat Encyclopedia.

## How Deep Security Manager checks for software upgrades

Deep Security Manager periodically connects to Trend Micro Update servers to check for updates to software that you have imported into the Deep Security Manager database, such as:

- Deep Security Agent
- Deep Security Manager

This checks based on the local inventory, not the Download Center. (There is a separate alert for new software on the Download Center.)

**Note:**
Deep Security only informs you of **minor** version updates-not major-of software.

For example, if you have Deep Security Agent **9.6.100**, and Trend Micro releases **9.6.200**, an alert tells you that software updates are available. However, if **10.0.nnn** (a major version difference) is released and you do not have any **10.0** agents, the alert does *not* appear (even though **10.0**is later than **9.6.100**).

An alert on the manager notifies you that software updates are available. On **Administration > Updates > Software**, the Trend Micro Download Center section also indicates whether there are updates available. Once you import (download) software into the Deep Security Manager database, you can upgrade the software in your deployment. See "Upgrade Deep Security Agent" on page 1542.

**Tip:** To see *all* software packages that are available for download (even if you have not imported it before), go to **Administration > Updates > Software > Download Center**.

To determine when the last check was performed, whether it was successful, or to manually initiate a check for updates, go to **Administration > Updates > Software** and view the "Deep Security" section. If you have configured a scheduled task to check for updates, the date and time of the next scheduled check is also listed here. See "Schedule Deep Security to perform tasks" on page 1600.

When imported, software is stored in the Deep Security Manager database. Imported software is periodically replicated to relays.

## Best practices for upgrades

When deploying a new release of the Deep Security Agent:

- Deep Security Relays must be the same version or newer than all agents and appliances in your environment.
- Deep Security Relays should be the same version as your Deep Security Manager.
- When performing upgrades of Deep Security software, the order of upgrade is important. Upgrade your Deep Security Manager first, then all relays, then agents.

**Note:** Beginning with Deep Security 20, you cannot activate a Deep Security Agent with a Deep Security Manager that is older than the **Minimum DSM Version** for that agent release. You can find the Minimum DSM Version on the Deep Security Software download page.

Tip: With Workload Security, the manager and relays provided with the service are always up to date. You can ignore the Minimum DSM Version and not think about relay versions unless you choose to deploy extra relays in your environment.

## How Deep Security validates update integrity

Both software updates and security updates are digitally signed. In addition to automatic checks, if you want to manually validate the signatures or checksums, you can use external tools such as:

- sha256sum (Linux)
- Checksum Calculator (Windows)
- jarsigner (Java Development Kit (JDK); see "Check digital signatures on software packages" on page 494)

### Digital signatures

When security updates are viewed, used, or imported into the Deep Security Manager database (either manually or automatically, via scheduled task), the manager validates the signature. A correct digital signature indicates that the software is authentically from Trend Micro and hasn't been corrupted or tampered with. If the digital signature is invalid, the manager does not use the file. A warning is also recorded in log files such as `server0.log`:

```
WARNING: ThID:85|TID:0|TNAME:Primary|UID:1|UNAME:MasterAdmin|Verifying the
signature failed.
```

```
com.thirdbrigade.manager.core.general.exceptions.FileNotSignedValidationExce
ption: "corrupted_rules.zip." has not been digitally signed by Trend Micro
and cannot be imported.
```

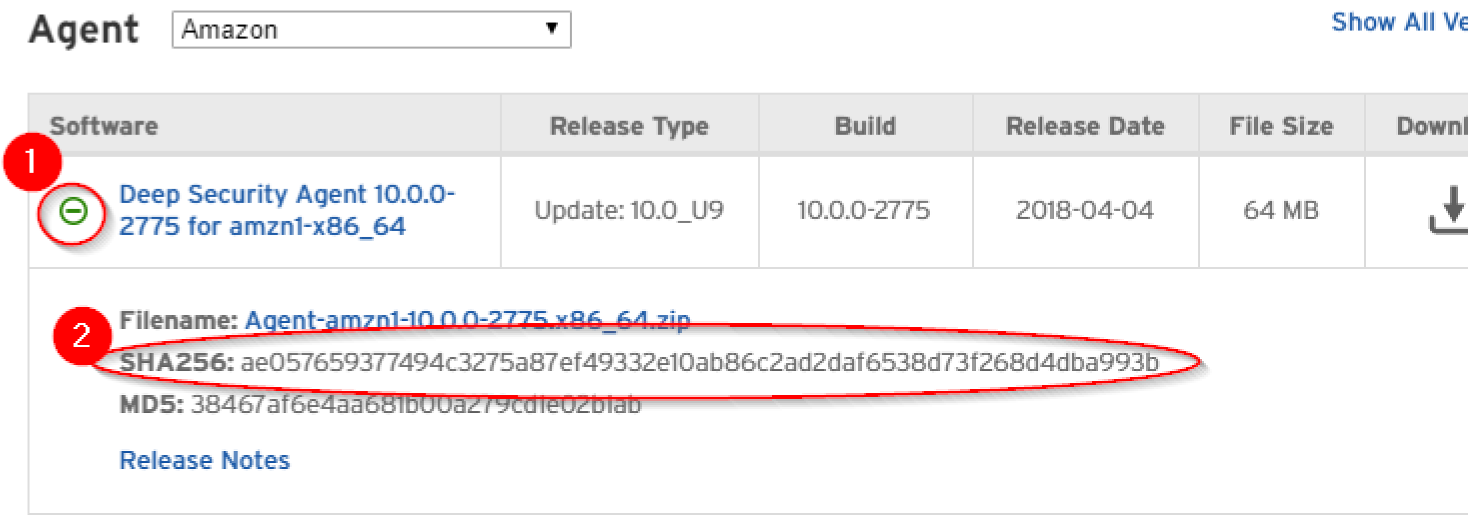
If you manually import a security update package with an invalid digital signature, the manager also displays an error message.

Note: Old security updates that are not signed fail validation if they are used, even if you successfully imported them in a previous version of Deep Security Manager that did not enforce signatures. For better protection, use new security updates instead. However if you still require the old security updates, you can contact your support provider to request a file that is signed, and then manually import the security update.

Deep Security Agent also validates the digital signature, compares checksums (sometimes called hashes or fingerprints) and uses other, non-disclosed integrity methods.

### Checksums

Software checksums (also called hashes or fingerprints) are published on the Download Center. To view the SHA-256 hash, click the **+** button next to the software's name.



Agent: Amazon

| Software | Release Type | Build | Release Date | File Size | Downl |
|---|---|---|---|---|---|
| Deep Security Agent 10.0.0-2775 for amzn1-x86_64 | Update: 10.0_U9 | 10.0.0-2775 | 2018-04-04 | 64 MB | |

**Filename:** Agent-amzn1-10.0.0-2775.x86_64.zip
**SHA256:** ae057659377494c3275a87ef49332e10ab86c2ad2daf6538d73f268d4dba993b
**MD5:** 38467af6e4aa681b00a279cd1e02b1ab

Release Notes

## Apply security updates

To remain effective at identifying new threats, your Deep Security Agents need periodic security updates.

Before your agents and relays can receive security updates, you must define how to distribute them (see "Deploy additional relays" on page 1345 and "Configure the update source" on page 1348). Then you can:

- "Initiate security updates" on the next page
- "Check your security update status" on the next page
- "View details about pattern updates" on the next page
- "Revert, import, or view details about rule updates" on page 1535
- "Configure security updates" on page 1536

## Initiate security updates

> Tip: Instead of manually checking for updates, configure Deep Security Manager to automatically check for security updates via a scheduled task. See "Schedule Deep Security to perform tasks" on page 1600.

You can manually initiate security updates at any time, regardless of scheduled tasks.

- To get security updates on *one* agent, go to **Computers**, select the agent, then right-click and select **Actions > Download Security Update**.

## Check your security update status

To view the status of your security updates, go to **Administration > Updates > Security**.

- **Trend Micro Update Server:** Indicates whether relays can connect to Trend Micro ActiveUpdate to check for the latest security updates.
- **Deep Security:** Indicates when the last successful check and download were performed, and when the next scheduled check will be performed. **All Relays are in sync** indicates that all relays are distributing the latest successfully downloaded pattern updates.

  > Tip: Out-of-sync status usually indicates that the relay cannot connect to Trend Micro Update Servers. Usually, this is not normal. You should fix network connectivity problems. In "air-gapped" deployments, however, network isolation is intentional; you must provide updates manually.

- **Computers:** Indicates whether any computers are out-of-date *compared to the pattern updates currently on the relays*. To tell all computers to get the latest pattern updates from their assigned relays, click **Send Patterns to Computers**.

## View details about pattern updates

To view a list of the components in an Anti-Malware pattern update, go to **Administration > Updates > Security > Patterns**. This page is displayed only when Deep Security has an active relay.

- **Component:** The type of update component.
- **For Use By:** The Deep Security product this component is intended for.
- **Platform:** The operating system for which the update is intended.
- **Current Version:** The version of the component currently being distributed by the Deep Security Relays.

  > **Tip:** To check which security update component version is being used on a protected computer, go to **Computers**, double-click the computer, and then select **Updates**.

- **Last Updated:** When the current security update was downloaded from Trend Micro.

## Revert, import, or view details about rule updates

To view a list of the most recent Intrusion Prevention, Integrity Monitoring, and Log Inspection Rules that have been downloaded into the Deep Security Manager database, go to **Administration > Updates > Security > Rules**.

From there you can:

- **View details about a rule update:** Select a rule update and click **View**. Details include a list of the update's specific rules.

  > **Tip:** To check which rule update version a relay is distributing, go to **Computers**, double-click the relay, and then select **Security Updates**. If Anti-Malware is enabled for that computer, it also displays the computer's pattern version.

- **Roll back a rule update:** If a recent rule update has caused problems, you can revert to a previous rule version. Select the rule update that you want to revert to and then click **Rollback**. Deep Security Manager generates a preview change summary so that you can confirm results before finalizing.

  > **Note:** All policies affected by the reverted rules will be immediately updated on *all computers using those policies*.

- **Reapply the current rule set:** ✓ indicates that a rule update has been applied. To reapply that rule update to protected computers, right-click the rule update and click **Reapply**.

- **Import a rule update:** Normally, rule updates are imported either manually or automatically (via scheduled task). However, if your deployment has no connectivity to the Trend Micro Update servers on the Internet (an "air-gapped" deployment), or if you are asked to do so by your support provider, you can click this button to manually upload and import a security update package.
- **Export a rule update:** Normally, you should not need to export a rule update unless your support provider asks you.
- **Delete a rule update:** Removes the selected rule update from the Deep Security Manager database.

  > Tip: To limit the number of rule updates that are kept in the Deep Security Manager database, go to **Administration > System Settings > Storage** .

Security update packages must have a valid digital signature. If you try to view or use an invalid package (including old security updates that don't have a signature), then the manager displays an error message. See "How Deep Security validates update integrity" on page 1532.

## Configure security updates

You can make the following configurations:

- "Enable automatic patches for rules" below
- "Enable automatic Anti-Malware engine updates" on the next page
- "Enable security updates for older agents" on the next page
- "Change the alert threshold for late security updates" on the next page

### Enable automatic patches for rules

Trend Micro sometimes updates an existing Deep Security rule to improve performance or fix a bug. To automatically apply these patches, go to **Computer or Policy editor > Settings > General** and in the **Send Policy Changes Immediately** area, select **Automatically send Policy changes to computers** and set the drop-down to **Yes**. If it's not selected, you must manually apply downloaded rule updates to policies: go to **Administration > System Settings > Updates** and click **Automatically apply Rule Updates to Policies**.

> Note: By default, changes to policies are automatically applied to computers.

## Enable automatic Anti-Malware engine updates

By default, when you update Deep Security Agent software, then its Deep Security Anti-Malware engine is updated together with it. If you don't update software often, then over time, the Anti-Malware engine might become much older than the malware patterns it uses (which should be frequently updated).

For better protection, you can configure agents to automatically keep the Anti-Malware engine part of the software updated — an approach more similar to the security updates that it uses.

1. Go to **Computers or Policies**.
2. Double-click a computer or policy.
3. Go to **Settings > Engine Update**.
4. For **Automatically update anti-malware engine**, select **Yes** .

   If this setting is disabled, then on **Computer Details > Updates > Advanced Threat Scan Engine**, the **Is Latest** section displays "N/A".

**Note:** Regardless of this setting, relays always receive the latest Anti-Malware engine updates. This keeps the relay's local protection and engine update source for the same relay group up-to-date. Therefore, you cannot enable or disable engine updates directly on a relay.

## Enable security updates for older agents

For some platforms, Deep Security Manager20 supports older versions. See "Agent platform compatibility" on page 389.

By default, to conserve disk space, Deep Security Relay will not download and distribute security updates for these older agents. To enable security updates for them, go to **Administration > System Settings > Updates**. Select **Allow supported 8.0 and 9.0 Agents to be updated**.

**Note:** Deep Security Agent 8.0 is no longer supported. This check box only applies to the 9.0 agent.

## Change the alert threshold for late security updates

If an update has been downloaded from Trend Micro and available for some time, but computers are not updated yet, an alert occurs. For rule updates, by default, the limit is 30 minutes. For pattern updates, by default, the limit is 1 hour.

If you want to change the time limit for the alert, go to **Administration > System Settings > Alerts** and configure **Length of time an Update can be pending before raising an Alert**.

## Disable emails for New Pattern Update alerts

The "New Pattern Update is Downloaded and Available" alert is raised when a security update has not been applied to an agent one hour after Deep Security Manager has downloaded it. The one-hour time span is not configurable. The alert is sent via email when the alert is raised by default.

If you are receiving too many of these email alerts because one hour is not long enough to disperse the updates, you can disable email notifications for this alert. Instead, you can receive email messages for the "Computer Not Receiving Updates" alert for which you can configure the time that passes before the alert is raised.

1. To ensure that Deep Security Manager is configured to automatically download security updates, in Deep Security Manager, click **Administration > Scheduled Tasks**.
2. If there is no scheduled task of type Check for Security Updates, create one (see "Schedule Deep Security to perform tasks" on page 1600).
3. Click **Administration > System Settings > Updates**. In the Rules section under Security Updates, make sure **Automatically apply Rule Updates to Policies** is selected.
4. Click **Alerts > Configure Alerts**.
5. In the Alert Configuration window, click the **New Pattern Update is Downloadable and Available** alert and then click **Properties**.
6. On the Alert Information window, deselect **Send Email to notify when this alert is raised** and then click **OK**.
7. Click the **Computer Not Receiving Updates** alert and then click **Properties**.
8. Make sure **Send Email to notify when this alert is raised** is selected, and click **OK**.
   The alert is raised when an update is pending for 7 days.
9. To raise the alert after a different amount of time has passed since the update was pending, click **Administration > System Settings > Alerts**.
10. In the alerts area, use the drop-down to select the period of time, and then click **Save**.

## Use a web server to distribute software updates

Deep Security software updates are normally hosted and distributed by relays. However, if you already have a web server, you can provide software updates via the web server instead of a relay. To do this, you must mirror the software repository of the relay on your web server.

**Note:** Although Deep Security Agents can download their *software* updates from the web server, at least one relay is still required to distribute *security* package updates such as anti-malware and IPS signatures (see "Apply security updates" on page 1533).

**Note:** Even though you are using your own web servers to distribute software, you must still go to **Administration > Updates > Software** and import software into the Deep Security Manager's database. Then you must ensure that your software web server contains the same software that has been imported into Deep Security Manager. Otherwise the alerts and other indicators that tell you about available updates will not function properly.

## Web server requirements

**Disk Space:** 20 GB

**Ports:** Web server port, relay port

## Copy the folder structure

Mirror the folder structure of the software repository folder on a relay-enabled agent. Methods vary by platform and network. For example, you could use `rsync` over SSH for a Linux computer and network that allows SSH.

On Windows, the default location for the relay-enabled agent's software repository folder is:

```
C:\ProgramData\Trend Micro\Deep Security Agent\relay\www\dsa\
```

On Linux, the default location for the Relay's software repository folder is:

```
/var/opt/ds_agent/relay/www/dsa/
```

The structure of the folder is like this:

```
|-- dsa
|    |-- <Platform>.<Architecture>
|         |--  <Filename>
|         |--  <Filename>
|         |--  ...
|
|    |-- <Platform>.<Architecture>
|          |--  <Filename>
|          |--  <Filename>
|          |--  ...
```

For example:

```
|-- dsa
|    |--  CentOS_<version>.x86_64
|          |--   Feature-AM-CentOS_<version>.x86_64.dsp
|          |--   Feature-DPI-CentOS_<version>.x86_64.dsp
|          |--   Feature-FW-CentOS_<version>.x86_64.dsp
|          |--   Feature-IM-CentOS_<version>.x86_64.dsp
|          |--  ...
|
|    |--  RedHat_EL6.x86_64
|          |--   Agent-Core-RedHat_<version>.x86_64.rpm
|          |--   Feature-AM-RedHat_<version>.x86_64.dsp
|          |--   Feature-DPI-RedHat_<version>.x86_64.dsp
|          |--   Feature-FW-RedHat_<version>.x86_64.dsp
|          |--  ...
|          |--   Plugin-Filter_2_6_32_131_0_15_el6_x86_64-RedHat_
<version>.x86_64.dsp
|          |--   Plugin-Filter_2_6_32_131_12_1_el6_x86_64-RedHat_
<version>.x86_64.dsp
|          |--  ...
|
|    |-- Windows.x86_64
|          |--  Agent-Core-Windows-<version>.x86_64.msi
|          |--  Agent-Core-Windows-<version>.x86_64.msi
|          |--  Feature-AM-Windows-<version>.x86_64.dsp
|          |--  Feature-AM-Windows-<version>.x86_64.dsp
|          |--  Feature-DPI-Windows-<version>.x86_64.dsp
|          |--  Feature-DPI-Windows-<version>.x86_64.dsp
|          |--  ...
|          |--  Plugin-Filter-Windows-<version>.x86_64.dsp
```

```
   |          |--  Plugin-Filter-Windows-<version>.x86_64.dsp
   |          |--  ...
```

The example above shows only a few files and folders. Inside a complete `dsa` folder, there are more. If you need to save disk space or bandwidth, you don't need to mirror all of them. You're only required to mirror the files that apply to your computers' platforms.

### Configure agents to use the new software repository

When the mirror on the web server is complete, configure Deep Security Agents to get their software updates from your web server.

1. On Deep Security Manager, go to **Administration > System Settings > Updates**.
2. In the Software Updates section, enter the URL(s) of the mirror folder(s) on your web server (s).
3. Click **Save**.

> **Note:** Verify that connectivity between agents and your web server is reliable. If the connection is blocked, agents will instead use the relay.

## Upgrade Deep Security Relay

Upgrade all your relays before you start to upgrade agents (see "Best practices for upgrades" on page 1531 for details.) There are two ways to upgrade a relay, as described below.

### Upgrade a relay starting from the manager

1. Log in to Deep Security Manager.
2. Identify your Deep Security Relays. Either:
   - Go to **Computers** . In the main pane, look for computers with the relay icon (■).
   - Go to **Administration**. On the left, click **Updates > Relay Management**. In the main pane, expand a **Relay Group**. Your relays are displayed with the relay icon (■).
3. Double-click the relay that you want to upgrade.
4. Click the **Actions** tab.
5. Click **Upgrade Agent**.

Follow the steps in the wizard that appears. Steps are similar to upgrading a Deep Security Agent, since a relay is just an agent with relay functionality enabled. For details, see "Upgrade Deep Security Agent" below.

### Upgrade a relay by running the installer manually

Sometimes you may not be able to upgrade the relay software from the Deep Security Manager. In these cases, you can upgrade a relay manually. For detailed instructions, see "Upgrade the agent manually" on page 1545. The referred-to instructions are for agents, but will work equally for relays.

## Upgrade Deep Security Agent

Software upgrades can be initiated through Deep Security Manager or a third-party deployment system.

In this topic:

### Before you begin an upgrade

Before you begin an agent upgrade:

1. Check that you're upgrading from a supported version. You can upgrade to Deep Security 20 from:
   - Deep Security 11 LTS (GA version or LTS updates)
   - Deep Security 11 Feature Releases
   - Deep Security 12 LTS (GA version or LTS updates)
   - Deep Security 12 Feature Releases

2. Back up the agent computers that you plan to upgrade. Make a system restore point or VM snapshot of each agent.
3. Import the new agent package into the manager. See "Import agent software" on page 522.
4. Upgrade all Deep Security Relays. See "Upgrade Deep Security Relay" on page 1541.

   **Warning:** You must upgrade all relays before you begin upgrading agents, otherwise, upgrades may fail.

   **Note:** When you upgrade the Deep Security Agent, Deep Security verifies your signature on Deep Security Agent to ensure that the software files have not changed since the time of signing. For more information, see "Agent package integrity check" on page 1637.

Next, review the platform-specific notes below and complete any advised tasks.

### Linux agent upgrade notes

Before upgrading the Deep Security Agent on a Linux platform, confirm the OS kernel is supported by the latest version of the agent. See "Linux kernel compatibility" on page 408

### Windows agent upgrade notes

Immediately after upgrading Deep Security Agent 12 or later on Windows with Anti-Malware enabled, be aware that the Anti-Malware engine may appear as 'Offline'. The engine will return to the 'online' state after the first heartbeat following the upgrade.

### Solaris agent upgrade notes

- On Solaris 11, if you are upgrading from Deep Security Agent 9.0, you must first upgrade to Deep Security Agent 9.0.0-5616 or a later 9.0 agent, and from there, upgrade to Deep Security Agent 11.0. If you upgrade from an earlier build, the agent may fail to start. If this problem occurs, see "Fix the upgrade issue on Solaris 11" on page 1701.
- An upgrade on Solaris may take five minutes or longer to complete in some cases.

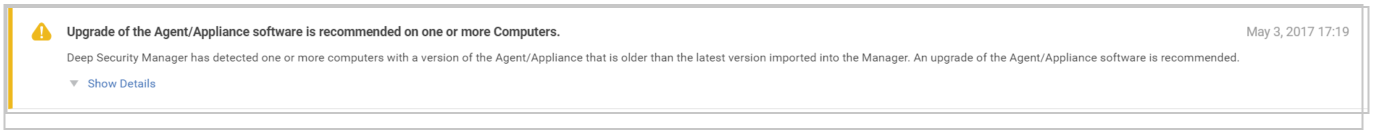
### AIX agent upgrade notes

*There are no upgrade notes for AIX at this time.*

You are now ready to upgrade your agent using any of the methods described in this topic.

## Upgrade the agent starting from an alert

When a new agent software version is available, a message appears on **Alerts**.



**Upgrade of the Agent/Appliance software is recommended on one or more Computers.** May 3, 2017 17:19

Deep Security Manager has detected one or more computers with a version of the Agent/Appliance that is older than the latest version imported into the Manager. An upgrade of the Agent/Appliance software is recommended.

1. In the alert, click **Show Details** and then click **View all out-of-date computers**. **Computers** appears, displaying all computers where **Software Update Status** is **Out-of-Date**. What is considered 'out-of-date' is determined by version control rules you've set up. For details, see "Configure agent version control" on page 1367.
2. Continue with "Upgrade the agent from the Computers page" below or "Upgrade the agent manually" on the next page.

## Upgrade multiple agents at once

1. In Deep Security Manager, go to **Administration > Updates > Software**.
2. In the main pane, look under the **Computers** section to see whether any computers or virtual appliances are running agents for which upgrades are available. The check is only performed against software that has been imported into Deep Security, not against software available from the Download Center.
3. Click **Upgrade Agent / Appliance Software** to upgrade all out-of-date computers. What is considered 'out-of-date' is determined by version control rules you've set up. For details, see "Configure agent version control" on page 1367.

## Upgrade the agent from the Computers page

1. In Deep Security Manager, go to **Computers**, and then:
   - Right-click the computer(s) that you want to upgrade, and select **Actions > Upgrade Agent Software**.

     Or

- Select the computer(s) that you want to upgrade, click the **Actions** button near the top and select **Upgrade Agent Software**.

  Or

- Double-click a computer that you want to upgrade and on the Computer details dialog box, click the **Upgrade Agent** button.

> **Warning:** You must upgrade your relays before your agents to prevent failures. Learn more. To identify a relay, look for the relay icon ( ).

2. In the dialog box that appears, select the **Agent Version**. We recommend that you select the default **Use the latest version for platform (X.Y.Z.NNNN)**. Click **Next**.

## Upgrade the agent on activation

If Deep Security Agent is installed on Linux or Windows, you can choose to automatically upgrade the agent to the newest software version that's compatible with your Deep Security Manager when the agent is activated or reactivated. For details, see "Automatically upgrade agents on activation" on page 1388.

## Upgrade the agent from a scheduled task

You can create a Scheduled Task to upgrade a group of agents on a set schedule. For details, see Scheduled Agent Upgrade Task.

## Upgrade the agent manually

Sometimes you may not be able to upgrade the agent software from the Deep Security Manager. Reasons may include:

- There are connectivity restrictions between the manager and agent computers.
- Your agent software is too old, and the manager doesn't support upgrading it anymore.
- You prefer to deploy upgrades using a third-party system.

If any of the above scenarios describes your situation, you can upgrade the agent by running the installer manually. The method varies by operating system.

## Upgrade the agent on Windows

1. Disable agent self-protection to allow the installer to make modifications to the agent. To disable self-protection:
   a. In the Deep Security Manager, go to Computer editor[1] > **Settings** > **General**.
   b. In **Agent Self Protection**, deselect **Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent** or enter a password for a local override.
2. Export the new agent ZIP from the manager. See "Export the agent installer" on page 524 for instructions. If multiple new agents are available for your platform, choose the latest one.
3. Copy the ZIP to the agent computer and extract it.
4. Double-click the MSI file in the root of the ZIP file. The installer detects the previous agent and performs the upgrade.

## Upgrade the agent on Linux

1. Disable agent self-protection to allow the installer to make modifications to the agent.
2. Export the new agent ZIP file from the manager. See "Export the agent installer" on page 524 for instructions. If multiple new agents are available for your platform, select the latest one.
3. Copy the ZIP file to the agent computer and extract it.
4. If the computer uses the RPM package manager (Red Hat, CentOS, Amazon Linux, Cloud Linux, SUSE), run the following command:

   ```
   rpm -U <new agent installer rpm>
   ```

   The `-U` argument instructs the installer to perform an upgrade.

   If the computer uses the dpkg package manager (Debian or Ubuntu), enter the command:

   ```
   dpkg -i <new agent installer dpkg>
   ```

## Upgrade the agent on Solaris

[1] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

1. Export the new agent ZIP from the manager. See "Export the agent installer" on page 524 for instructions. If multiple new agents are available for your platform, choose the latest one.
2. Copy the ZIP to the agent computer and extract it.
3. Run the installer:

- Solaris 11, one zone (run in the global zone):

  x86: `pkg update -g file:///mnt/Agent-Solaris_5.11-9.x.x-xxxx.x86_64/Agent-Core-Solaris_5.11-9.x.x-xxxx.x86_64.p5p pkg:/security/ds-agent`

  SPARC: `pkg update -g file:///mnt/Agent-Solaris_5.11-9.x.x-xxxx.x86_64/Agent-Solaris_5.11-9.x.x-xxxx.sparc.p5p pkg:/security/ds-agent`

- Solaris 11, multiple zones (run in the global zone):

  ```
  mkdir <path>
  ```

  ```
  pkgrepo create <path>
  ```

  ```
  pkgrecv -s file://<dsa core p5p file location> -d <path> '*'
  ```

  ```
  pkg set-publisher -g <path> trendmicro
  ```

  ```
  pkg update pkg://trendmicro/security/ds-agent
  ```

  ```
  pkg unset-publisher trendmicro
  ```

  ```
  rm -rf <path>
  ```

- Solaris 10: Create an installation configuration file named `ds_adm.file` with the following content, and then save it in the root directory. Next, run this command to install the package:

  `pkgadd -G -v -a /root/ds_adm.file -d Agent-Core-Solaris_5.10_U7-10.0.0-1783.x86_64.pkg`

## Content of ds_adm.file

```
mail=
```

```
instance=overwrite
```

```
partial=nocheck
runlevel=quit
idepend=nocheck
rdepend=quit
space=quit
setuid=nocheck
conflict=quit
action=nocheck
proxy=
basedir=default\
```

Upgrade the agent on AIX

1. Export the new agent ZIP from the manager. See "Export the agent installer" on page 524 for instructions. If multiple new agents are available for your platform, choose the latest one.
2. Copy the ZIP to the agent computer and extract it. A BFF file becomes available.
3. Copy the BFF file to a temporary folder such as `/tmp` on the AIX computer. For detailed instructions, see "Install the agent manually" on page 548.
4. Upgrade the agent. Use these commands:

   ```
   /tmp> rm -f ./.toc
   ```

   ```
   /tmp> installp -a -d /tmp/<agent_BFF_file_name> ds_agent
   ```

   where `<agent_BFF_file_name>` is replaced with the name of the BFF installer file you extracted.

## Upgrade best practices for agents

If you have critical workloads running on your agent servers, we recommend that you follow these best practices when upgrading:

- Upgrade when the computers are less busy.
- Test the upgrade procedure first in a staging environment before upgrading production servers.
- When upgrading production servers, upgrade one server at a time for the first few servers. Allow a soak period in between each server upgrade.
- After individually upgrading a number of production servers for a given OS version (and application role, on Solaris or AIX), upgrade the remaining servers in groups.
- Also review the "Best practices for upgrades" on page 1531.

# Upgrade Deep Security Manager VM for Azure Marketplace

To determine which version of Deep Security Manager you have, go to **Support > About**. The version number of the currently available version is listed on the description page for the Deep Security Manager in Azure Marketplace. Compare these two numbers to determine if you need to upgrade.

Each node must have the same version of Deep Security Manager VM for Azure Marketplace. If you are planning on adding a new node, the version of the new node must match the version used by the existing nodes. This might mean that you have to upgrade the version on the existing nodes to make sure they match the new node.

## Will my virtual machines still be protected during the upgrade?

Your virtual machines will still continue to be protected throughout the entire upgrade process. There will be a brief outage for the Deep Security Manager nodes when they are upgraded but all existing Deep Security Agents will continue to function normally during this period. New agents cannot be activated until the Deep Security Manager services have been restored.

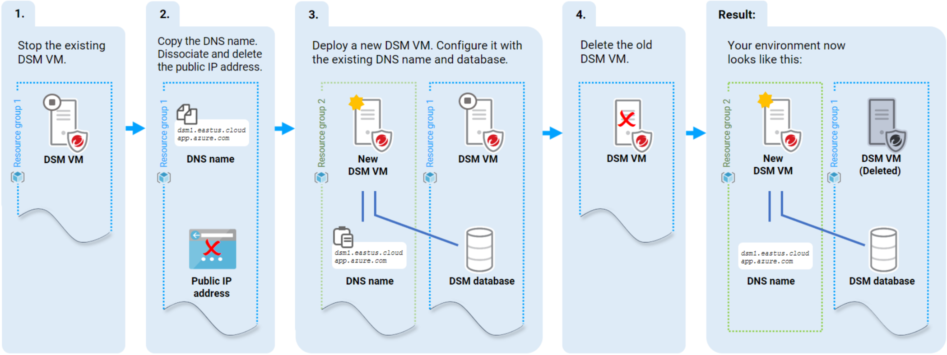
## Before you begin

Before you upgrade to the latest version of Deep Security Manager VM for Azure Marketplace, ensure that you have the following information about your current version:

- Resource group name
- Database credentials: hostname, name, admin name, and admin password
- License type: You can view this by going to **Administration > Licenses** in Deep Security Manager.

## Upgrade to the latest version

The diagram below provides an overview of the upgrade process. Detailed instructions follow the diagram.


1.
Stop the existing DSM VM.
Resource group 1
DSM VM
2.
Copy the DNS name. Dissociate and delete the public IP address.
Resource group 1
dsm1.eastus.cloudapp.azure.com
DNS name
Public IP address
3.
Deploy a new DSM VM. Configure it with the existing DNS name and database.
Resource group 2
New DSM VM
dsm1.eastus.cloudapp.azure.com
DNS name
Resource group 1
DSM VM
DSM database
4.
Delete the old DSM VM.
DSM VM
Result:
Your environment now looks like this:
Resource group 2
New DSM VM
dsm1.eastus.cloudapp.azure.com
DNS name
Resource group 1
DSM VM (Deleted)
DSM database

DSM: Deep Security Manager

First, stop the existing Deep Security Manager:

**Warning:** Do not delete the existing Deep Security Manager.

1. Log in to the Azure portal.
2. On the left, click **Resource groups**.
3. In the main pane, click the resource group that contains your existing Deep Security Manager.
4. In the main pane, click the Deep Security Manager VM link to show its dashboard page.
5. Near the top of the page, click **Stop**. Wait for the onscreen message indicating a successful stop.

Next, copy the DNS name, dissociate the public IP address, and then delete it:

1. On the left, click **Resource groups**, and then click the resource group that contains your Deep Security Manager.
2. In the main pane, look for the **Public IP address** line, and click the associated link to open the public IP address details.
3. Copy the **DSN name** value to the clipboard or to a file. The value looks similar to: `dsm1.eastus.cloudapp.azure.com`.
4. Click **Dissociate** and then click **Delete** to deleted the public IP address.

   This step ensure that the DNS name stays the same after the upgrade, and this is recommended to ensure that agents keep functioning properly.

Next, deploy a new Deep Security Manager VM and configure it with the old DNS name:

1. Make sure your existing Deep Security Manager is still present and stopped.
2. In the search bar at the top of the Azure portal, begin typing `Deep Security` and select **Deep Security Manager (BYOL)** from the search results. The **Deep Security Manager (BYOL)** page appears.
3. Click **Create**.
4. Under **Deep Security Manager VM name**, specify the name of the new VM. The name can be the same or different from your existing Deep Security Manager VM.
5. Under **Your Username**, specify a user name. You will use this user name to log in to the new Deep Security Manager VM.
6. Under **Authentication type**, select **Password** or **SSH public key** and then specify a password or SSH public key.
7. Under **Subscription**, select the Azure subscription you want to use with the Deep Security Manager VM. Usage fees accrued under this subscription are billed by Microsoft (not Trend Micro).
8. Under **Resource Group**, select **Create new** and enter a name to create a new resource group. Alternatively, click **Select existing** to use an existing *empty* resource group.
9. Under **Location**, select an Azure region. Make sure you select the same location as your original Deep Security Manager VM.
10. Under **VM Size**, accept the default or click **Change size** to select another size. If no sizes are selectable, clear the filters.
11. Under **Public IP address**, keep the default or enter another name to set the label of the public IP address resource. This label appears in the Azure portal interface.
12. Under **Deep Security Manager URL**, enter the host name of your *original* Deep Security Manager. This host name combined with the trailing domain name must match the original Deep Security Manager 'DNS name' that you copied in an earlier step. For example: `dsm1.eastus.cloudapp.azure.com`.
13. Under **Deep Security Manager console port** and **Heartbeat Port**, accept the defaults or specify different port numbers. For details on ports, see "Port numbers, URLs, and IP addresses" on page 478.
14. Click **OK**. The **Deep Security Database** blade appears.
15. Under **Azure SQL Database**, click **Use Existing** and enter the credentials you recorded in the "Before you begin" on page 1549 section above. Click **OK**.
16. Wait for a **Validation passed** message near the top of the screen. Click **OK**. The **Create** page appears with the terms of use.
17. Leave the check box at the bottom of the agreement deselected unless you want Microsoft to contact you.
18. Click **Create**. On the top-right, click the notifications icon to view the progress of the deployment.

19. Verify that the upgrade was successful:
    a. Open a browser and go to the following address: `https://<DNS name>` where `<DNS name>` is replaced with the DNS name of your new Deep Security Manager. For example, `https://dsm1.eastus.cloudapp.azure.com`. The Deep Security Manager login page appears.
    b. Log in. The Deep Security Manager dashboard page appears.
    c. At the top-right, go to **Support > About** and check the version number. It should be the same as the version number listed on the **Deep Security Manager (BYOL)** page in Azure.

Finally, delete the old Deep Security Manager VM and its resources:

1. In the Azure portal, on the left, click **Resource groups**.
2. In the main pane, click the resource group containing the original Deep Security Manager VM to view its details.
3. Delete the original Deep Security resources of **Type**:
    - Virtual machine
    - Disk (optional)
    - Network interface
    - Network security group
    - Storage account (optional)
    - Virtual network

## Post-upgrade tasks

After the upgrade, you may choose to complete the following tasks:

- Replace the server certificate: After the upgrade, the Deep Security Manager's server certificate is preserved, unless you performed a fresh install. If your certificate was created using a weak cryptographic algorithm, such as SHA-1, consider replacing the certificate. Using stronger cryptography ensures compliance with the latest standards and provides better protection against the latest exploits and attacks. See "Replace the Deep Security Manager TLS certificate" on page 1494.

# Upgrade the database

If you're planning on upgrading the Deep Security VM from Azure Marketplace, you may also need to upgrade the Deep Security database. Check this list of currently-supported databases, and then, if required, migrate to a new database following the instructions below.

## The upgrade path

The upgrade path for the database is as follows:

1. Upgrade the database software first.
2. Upgrade the Deep Security VM from Azure Marketplace.

The database you choose must be supported by both the *new* and *currently-installed* version of the Deep Security VM from Azure Marketplace. See these lists:

- Databases supported by the current release of the manager.
- Databases supported by previous versions of the manager. (The adjacent link takes you to a page that provides access to the documentation for previous releases. You can drill down into the documentation to find database support.)

## Upgrade the database

To upgrade the database, follow these instructions:

> **Warning:** To prevent data loss, complete the database migration before upgrading the Deep Security VM from Azure Marketplace.

1. Stop the Deep Security Manager service. Deep Security Agents continue with their current protection policies while the manager is stopped.
2. Back up the database(s).
3. Back up the database connection settings file: `[Deep Security install directory]/webclient/webapps/ROOT/WEB-INF/dsm.properties`
4. Migrate to the new database server. For specific requirements, see "Database requirements" on page 501.
5. If the migration did not preserve existing databases, load the database backup(s) into the new database engine.
6. If required, edit `dsm.properties` to use the migrated database.
7. Restart the Deep Security Manager service.

## Error: The installer could not establish a secure connection to the database server

When installing or upgrading Deep Security Manager, the following error message can occur if you are using Microsoft SQL Server as your Deep Security database:

*The installer could not establish a secure connection to the database server. Please upgrade or configure your database server to support TLS 1.2 encryption*.

The error message appears if the `java.security` file on the Deep Security Manager includes `TLSv1` and `TLSv1.1` in the `jdk.tls.disabledAlgorithms=` setting, which disables early TLS and only allows TLS 1.2. (The `java.security` file is set this way if you are doing a fresh install of Deep Security Manager 11.1 or higher, where only TLS 1.2 is allowed, or if you are upgrading and previously enforced TLS 1.2.) During the upgrade or installation, the database drivers on the manager try to communicate with the SQL Server using TLS 1.2, and if your SQL Server version does not support TLS 1.2, you'll see this error.

To solve the problem, you must upgrade your SQL Server database to a version that supports TLS 1.2 and then retry the Deep Security Manager installation or upgrade. For a list of SQL Server versions that support TLS 1.2, see this Microsoft article.

# Uninstall Deep Security

## Uninstall Deep Security

When you manually uninstall the activated Deep Security Agent or relay from a computer, the computer does not notify Deep Security Manager that the software has been uninstalled. On the **Computers** page in Deep Security Manager, the computer's status is still displayed as Managed (Offline) or similar, depending on the context. To avoid this, on Deep Security Manager, do one of the following:

- Deactivate the agent or relay *before* uninstalling it.
- Delete the computer from the list *after* uninstalling the agent.

# Uninstall a Deep Security relay

A Deep Security relay is an agent with the relay feature enabled. To remove the relay, you must uninstall the agent software.

## Uninstall a relay on Windows

Before updating or uninstalling a Deep Security Agent or relay on Windows, you need to disable agent self-protection. To do this, on the Deep Security Manager, go to **Computer editor**[1] **> Settings > General**. In **Agent Self Protection**, either deselect **Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent** or enter a password for local override.

From the Windows Control Panel, select **Add / Remove Programs**, double-click **Trend Micro Deep Security Agent**, and then click **Remove**.

Alternatively, you can uninstall from the command line by executing the following:

```
msiexec /x <package name including extension>
```

For a silent uninstall, add `/quiet` to the preceding command.

## Uninstall a relay on Linux

To completely remove the relay and any configuration files it created on a platform that uses the Red Hat package manager (RPM), such as CentOS, Amazon Linux, Oracle Linux, SUSE, or Cloud Linux, execute the following command:

```
# sudo rpm -ev ds_agent
 Stopping ds_agent: [ OK ]
 Unloading dsa_filter module [ OK ]
```

If iptables was enabled prior to the installation of the relay-enabled agent, it will be re-enabled when the relay-enabled agent is uninstalled.

**Note:** Remember to remove the relay-enabled agent from the Deep Security Manager's list of managed computers and from the relay group.

[1] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

# Uninstall Deep Security Agent

## Uninstall an agent on Windows

Before updating or uninstalling a Deep Security Agent or relay on Windows, you must disable agent self-protection. To do this, on the Deep Security Manager, go to Computer editor[1] > **Settings > General**. In **Agent Self Protection**, and then either deselect **Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent** or enter a password for local override.

1. Deactivate the agent using Deep Security Manager by navigating to the **Computers** page, right-clicking the computer, and selecting **Actions > Deactivate**.
   If you cannot deactivate the agent because Deep Security Manager is unable to communicate with the agent, you need to execute the following before continuing to the next step:
   ```
    C:\Program Files\Trend Micro\Deep Security Agent>dsa_control --selfprotect 0
   ```
2. Open the Windows Control Panel and select **Uninstall a program**.
3. Look for Trend Micro Deep Security Agent and click **Uninstall**.

Alternatively, you can uninstall from the command line by executing the following:

```
msiexec /x <package name including extension>
```

For a silent uninstall, add `/quiet` to the preceding command.

## Uninstall an agent on Linux

Before uninstalling an agent on Linux, check whether or not agent self-protection is enabled. If it is enabled, you need to disable it on the policy or computer level. For more information, see Enable or disable agent self-protection.

If your version of Linux provides a graphical package management tool, you can search for the `ds_agent` package and use the tool remove the package. Otherwise, use the command line.

To completely remove the agent and any configuration files it created on a platform that uses the Red Hat package manager (RPM), such as CentOS, Amazon Linux, Oracle Linux, SUSE, or Cloud Linux, execute the following command:

[1] To open the Computer editor, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

```
# sudo rpm -ev ds_agent
 Stopping ds_agent: [ OK ]
 Unloading dsa_filter module [ OK ]
```

If iptables was enabled prior to installing Deep Security Agent, it is re-enabled when the agent is uninstalled.

If the platform uses Debian package manager (dpkg), such as Debian and Ubuntu, execute the following command:

```
$ sudo dpkg -r ds-agent
 $ sudo dpkg --purge ds-agent
 Removing ds-agent...
 Stopping ds_agent: .[OK]
```

## Uninstall an agent on Solaris 10

Execute the following command:

```
pkgrm ds-agent
```

Uninstall may require a reboot.

## Uninstall an agent on Solaris 11

Execute the following command:

`pkg uninstall ds-agent`

Uninstall may require a reboot.

## Uninstall an agent on AIX

Execute the following command:

`installp -u ds_agent`

## Uninstall an agent on Red Hat OpenShift

Execute the following command:

`helm uninstall ds-agent`

## Uninstall Deep Security Notifier

Open the Windows Control Panel, select **Add / Remove Programs**, double-click **Trend Micro Deep Security Notifier**, and then click **Remove**.

To uninstall from the command line, execute the following command:

```
msiexec /x <package name including extension>
```

For a silent uninstall, add `/quiet` to the preceding command.

## Uninstall Deep Security Manager

### Uninstall the manager on Windows

From the Windows Start Menu, go to **Trend Micro > Trend Micro Deep Security Manager Uninstaller** and follow the steps to complete the uninstall.

To initiate the same Windows uninstall procedure from the command line, go to the installation folder and enter the following:

```
<installation folder>\Uninstall.exe
```

For a silent uninstall from the command line, add `-q`, as follows:

```
<installation folder>\Uninstall.exe -q
```

During a silent uninstall via the command line, the configuration files are kept so that if you reinstall, the installer repairs or upgrades the agent using existing settings.

### Uninstall the manager on Linux

To uninstall via the command line, go to the installation folder and enter the following:

```
sudo ./uninstall
```

For a silent uninstall, add `-q` to the preceding command.

During a silent uninstall via the command line, the configuration files are kept by default so that if you reinstall, the installer repairs upgrades the agent using existing settings.

>If you do not keep the configuration files during the uninstall and you later decide to reinstall Deep Security Manager, perform a manual clean-up before reinstalling. To remove the Deep Security Manager installation directory, execute the following command:

```
sudo rm -rf <installation location>
```

The default installation location is `/opt/dsm`.

# Configure Deep Security Manager memory usage

## Configure the installer's maximum memory usage

The installer is configured to use 1GB of contiguous memory by default. If the installer fails to run, you can configure the installer to use more memory:

1. Go to the directory where the installer is located.
2. Prepare an installation properties file. For example, you can name the file `install.prop` and use it for silent installation (see Sample properties file).
   When you run the silent installation, append the `-J-Xmx2g` parameter to the installer command to have 2GB of memory. For example, `Manager-Linux-`*`Version`*`.x64.sh -q -console -varfile` *`PropertiesFile`* `-J-Xmx2g`
   To have a different amount of memory, adjust the value of the appended parameter. For example, `-J-Xmx1024m` or `-J-Xmx4g`.

## Configure Deep Security Manager's maximum memory usage

The Deep Security Manager default setting for memory allocated to the Manager JVM process is 4GB. It is possible to change this setting:

1. Go to the Deep Security Manager installation directory. This is the same directory as for the Deep Security Manager executable.
2. Create a new file. Depending on the platform, give it the following name:
   - Windows: `Deep Security Manager.vmoptions`
   - Linux: `dsm_s.vmoptions`
3. Edit the file by adding a line similar to the following:
   -Xmx10g
   In the preceding example, 10g will make 10GB memory available to the Deep Security Manager.

4. Save the file and restart Deep Security Manager.
5. Verify the new setting by going to **Administration > System Information** and in the **System Details** area, expand **Manager Node > Memory**. The **Maximum Memory** value should now indicate the new configuration setting.

> **Note:**
> When you install Deep Security Manager version 20.0.313 (20 LTS Update 2021-01-18) or later, if the installer detects at least 16GB of RAM available, the default amount of memory allocated to the manager JVM process is 8GB.

# Restart the Deep Security Manager

## Linux

To restart the Deep Security Manager, open a CLI and run the following command:

```
sudo systemctl restart dsm_s
```

## Windows

To restart the Deep Security Manager, first log in to the Windows instance on which the Deep Security Manager is running and then follow the steps below for the "Windows desktop" below, the "Command prompt" below or "PowerShell" on the next page:

### Windows desktop

1. Open the Windows Task Manager.
2. Click the **Services** tab.
3. Right click the **Trend Micro Deep Security Manager** service, and then click **Restart**.

### Command prompt

Open the command prompt (`cmd.exe`) and run the following commands:

1. `net stop "Trend Micro Deep Security Manager"`
2. `net start "Trend Micro Deep Security Manager"`

## PowerShell

Open PowerShell and run the following commands:

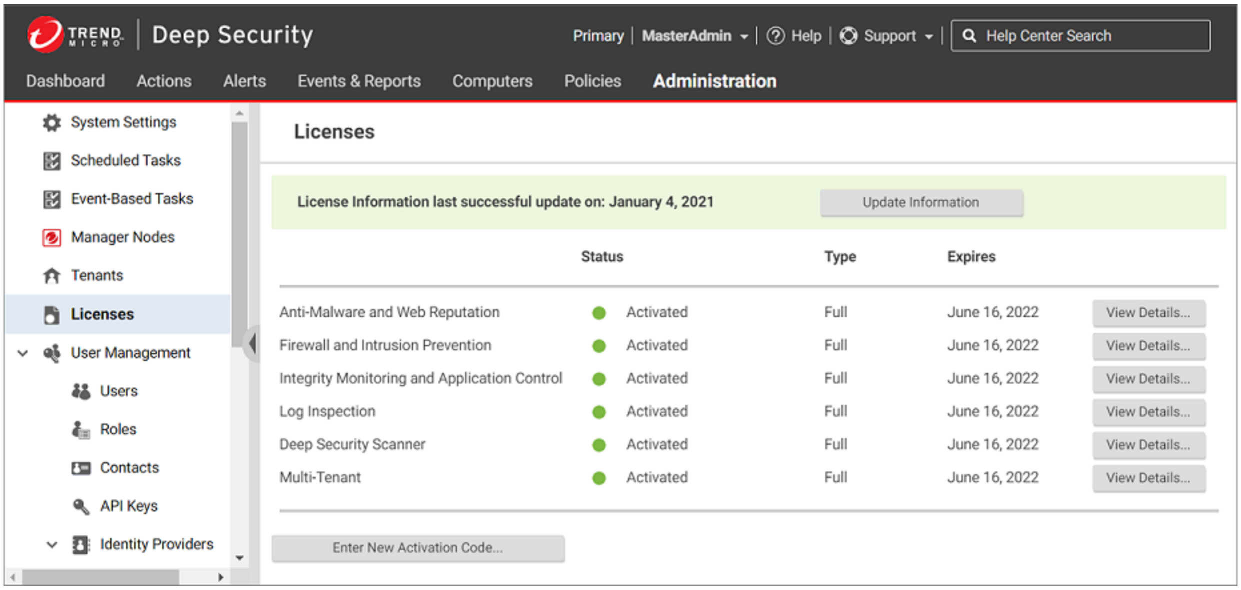
1. `Stop-Service 'Trend Micro Deep Security Manager'`
2. `Start-Service 'Trend Micro Deep Security Manager'`

# Check your license information

**Note:** This information does not apply to a multi-tenant configuration that inherits licensing from the parent tenant.

## Check your current licenses

To see information about your Trend Micro Deep Security product licenses, go to **Administration > Licenses** in the Deep Security Manager console.



Licenses

License Information last successful update on: January 4, 2021

| | Status | Type | Expires | |
|---|---|---|---|---|
| Anti-Malware and Web Reputation | ● Activated | Full | June 16, 2022 | View Details... |
| Firewall and Intrusion Prevention | ● Activated | Full | June 16, 2022 | View Details... |
| Integrity Monitoring and Application Control | ● Activated | Full | June 16, 2022 | View Details... |
| Log Inspection | ● Activated | Full | June 16, 2022 | View Details... |
| Deep Security Scanner | ● Activated | Full | June 16, 2022 | View Details... |
| Multi-Tenant | ● Activated | Full | June 16, 2022 | View Details... |

Deep Security consists of six module packages:

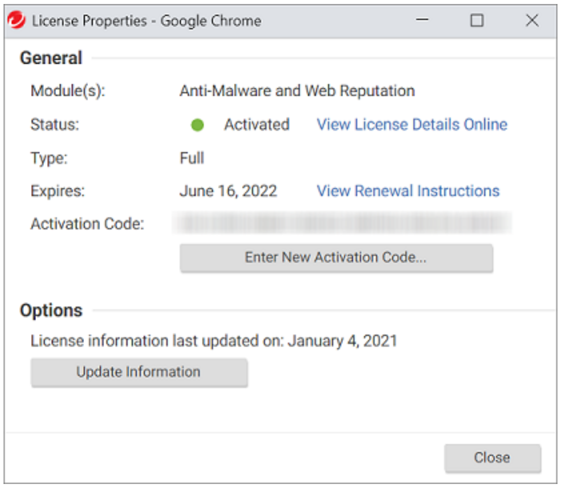
- Anti-Malware and Web Reputation
- Firewall and Intrusion Prevention
- Integrity Monitoring and Application Control

- Log Inspection
- Multi-Tenant

Each module package can be licensed fully or for a trial basis.

## See details about a license

On the Licenses page, click the **View Details** button next to an individual package's license to display additional information:



License Properties - Google Chrome

General

Module(s): Anti-Malware and Web Reputation

Status: ● Activated

Type: Full

Expires: June 16, 2022

Activation Code: [redacted]

Options

License information last updated on: January 4, 2021

View License Details Online
View Renewal Instructions
Enter New Activation Code...
Update Information
Close

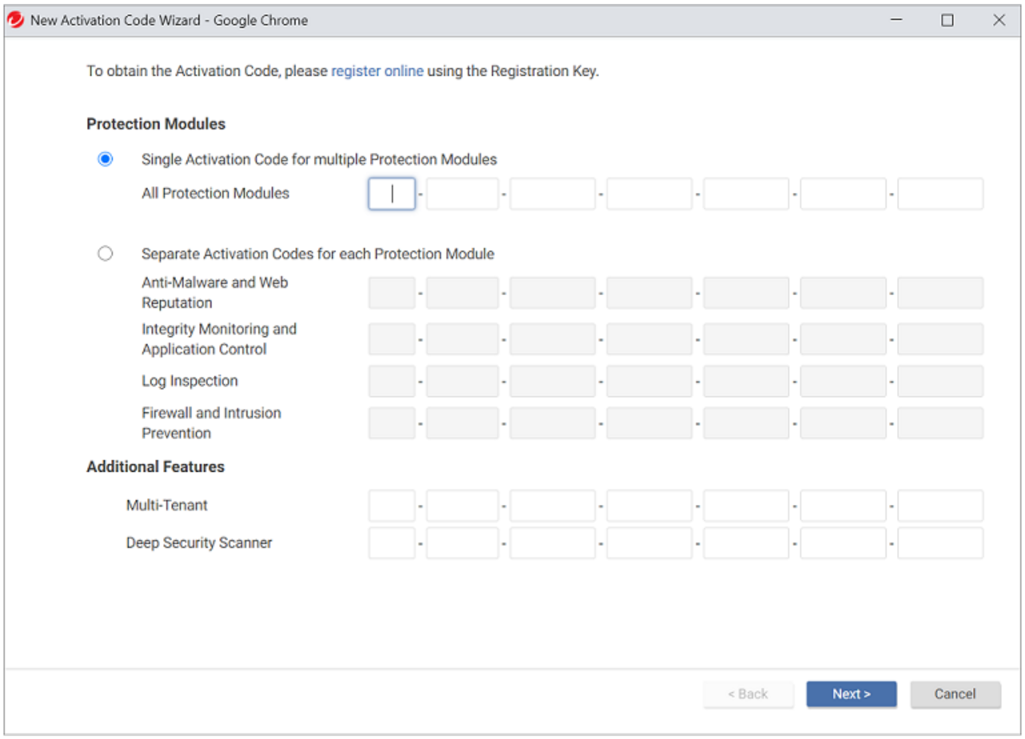
If you need more information, including the number of seats included with the license, click **View License Details Online** to go to the Trend Micro Customer Licensing Portal. The **View Renewal Instructions** link also goes to the Customer Licensing Portal.

Alerts are raised if any module is about to expire or has expired. When a license expires, existing functionality persists but updates are no longer delivered

## Add or upgrade a license

To add or upgrade a license, contact Trend Micro.

If Trend Micro has provided you with a new activation code, click **Enter New Activation Code** and enter it in the window that's displayed:



To obtain the Activation Code, please register online using the Registration Key.

**Protection Modules**

● Single Activation Code for multiple Protection Modules

All Protection Modules

○ Separate Activation Codes for each Protection Module

Anti-Malware and Web Reputation

Integrity Monitoring and Application Control

Log Inspection

Firewall and Intrusion Prevention

**Additional Features**

Multi-Tenant

Deep Security Scanner

Newly licensed features are immediately available

## Licensing for Azure Marketplace

- **Deep Security Manager (BYOL)** is for customers who have already obtained a license to use Deep Security from another source. If you are using this type of license, you need to enter the license string or activation code in Deep Security Manager after it is installed.

# DevOps, automation, and APIs

## About DevOps, automation, and APIs

To support DevOps workflows, Deep Security offers APIs to automate, monitor, and manage security throughout the release lifecycle. See "Use the Deep Security API to automate tasks" on page 1598.

The Trend Micro Hybrid Cloud Security Command Line Interface (THUS) is a tool that can help you easily navigate the API. For more information, see https://github.com/trendmicro/thus.

The deep-security GitHub repositories contain the following useful scripts:

- CloudFormation templates for deploying Deep Security Manager to AWS.
- Bash and Powershell scripts for automating various Agent and Manager tasks.

To get started with the API, see the First Steps Toward Deep Security Automation guide in the Deep Security Automation Center. The Automation Center also includes an API Reference.

Deep Security provides other ways to speed up the protection of your computers and other resources. For more information, see the following:

- "Schedule Deep Security to perform tasks" on page 1600
- "Automatically perform tasks when a computer is added or changed (event-based tasks)" on page 1603
- "AWS Auto Scaling and Deep Security" on page 1609
- "Use deployment scripts to add and protect computers" on page 1623
- "Automatically assign policies using cloud provider tags/labels" on page 1635
- "Command-line basics" on the next page

In addition, Deep Security provides the ability to forward events to SIEMs such as Spunk, QRadar, ArcSight, as well as Amazon SNS. For more information, see the following:

- "Set up Amazon Simple Notification Service" on page 1130

# Trend Micro Hybrid Cloud Security Command Line Interface (THUS)

Trend Micro Hybrid Cloud Security Command Line Interface (THUS) is a tool that you can use to help deploy, configure and maintain your Deep Security environments. THUS is easy to install and configure, all from your terminal.

For more information about setting up the Trend Micro Hybrid Cloud Security Command Line Interface (THUS), see https://github.com/trendmicro/thus.

# Command-line basics

You can use the local command-line interface (CLI) to instruct Deep Security Agents and Deep Security Manager to perform actions. You can also use the CLI to configure some settings and display the system resource usage information.

You can automate various CLI commands using the Deep Security API (see First Steps Toward Deep Security Automation.

- "dsa_control" below
- "dsa_query" on page 1580
- "dsa_scan" on page 1583
- "dsm_c" on page 1587

## dsa_control

The `dsa_control` enables you to configure some of the Deep Security Agent settings and manually trigger such actions as activation, anti-malware scans, and baseline rebuilds.

Note that on Windows OS, when self-protection is enabled, a local user cannot uninstall, update, stop, or otherwise control Deep Security Agent. In addition, the authentication password must be supplied when running CLI commands.

`dsa_control` only supports English strings. Unicode is not supported.

To use `dsa_control`:

On Windows:

1. Open a command prompt as administrator.
2. Change to the Deep Security Agent's installation directory. For example:

   ```
   cd C:\Program Files\Trend Micro\Deep Security Agent\
   ```

3. Execute the `dsa_control` command:

   ```
   dsa_control <option>
   ```

   where `<option>` is replaced with one of the options described in "dsa_control options" on the next page.

On Linux, AIX, and Solaris:

- `sudo /opt/ds_agent/dsa_control <option>`

  where `<option>` is replaced with one of the options described in "dsa_control options" below

Running multiple `dsa_control` commands can result in a more recent command overwriting an earlier one. If you want to run multiple commands, you should list the parameters side by side. For example, `dsa_control -m "RecommendationScan:true" "UpdateComponent:true"`

In general, it is recommended to use the Scheduled Tasks UI (**Administration > Scheduled Tasks**) for managing the Deep Security Agent tasks. For more information, see "Schedule Deep Security to perform tasks" on page 1600.

## dsa_control options

```
        dsa_control [-a <str>] [-b] [-c <str>] [-d] [-g <str>] [-s <num>]
[-m] [-p <str>] [-r] [-R <str>] [-t <num>] [-u <str>:<str>] [-w
<str>:<str>] [-x dsm_proxy://<str>] [-y relay_proxy://<str>] [--
buildBaseline] [--scanForChanges] [Additional keyword:value data to send
to manager during activation or heartbeat...]
```

| Parameter | Description |
|---|---|
| `-a <str>, --activate=<str>` | Activate agent with manager at the specified URL in this format:<br>`dsm://<host>:<port>/`<br>where:<br>• `<host>` could be either the manager's fully qualified domain name (FQDN), IPv4 address, or IPv6 address<br>• `<port>` is the manager's listening port number<br>Optionally, after the argument, you can also specify some settings such as the description to send during activation. See "Agent-initiated heartbeat command ("dsa_control -m")" on page 1571. They must be entered as key:value pairs with a colon as a separator. There is no limit to the number of key:value pairs that you can enter, but the key:value pairs must be separated from each other by a space. Quotation marks |

| Parameter | Description |
|---|---|
| | around the key:value pair are required if it includes spaces or special characters. |
| `-b, --bundle` | Create an update bundle. |
| `-c <str>, --cert=<str>` | Identify the certificate file. |
| `-d, --diag` | Generate an agent package. For details, see "Create an agent diagnostic package via CLI on a protected computer" on page 1726. |
| `-g <str>, --agent=<str>` | Agent URL. Defaults to:<br>`https://localhost:<port>/`<br>where `<port>` is the manager's listening port number. |
| `-m, --heartbeat` | Force the agent to contact the manager now. |
| `-p <str>` or `--passwd=<str>` | The authentication password that you might have configured in Deep Security Manager previously. See "Configure self-protection through Deep Security Manager" on page 1392 for details. If configured, the password must be included with all `dsa_control` commands except `dsa_control -a`, `dsa_control -x`, and `dsa_control -y`.<br>Example: `dsa_control -m -p MyPa$$w0rd`<br>If you type the password directly into the command line, it is displayed on the screen. To hide the password with asterisks (*) while you type, enter the interactive form of the command, `-p *`, which prompts you for the password.<br>Example:<br>`dsa_control -m -p *` |
| `-r, --reset` | Reset the agent's configuration. This removes the activation information from the agent and deactivates it. |

| Parameter | Description |
|---|---|
| `-R <str>, --restore=<str>` | Restore a quarantined file. On Windows, you can also restore cleaned and deleted files. |
| `-s <num>, --selfprotect=<num>` | Enable the agent self-protection (1: enable, 0: disable). Self-protection prevents local end-users from uninstalling, stopping, or otherwise controlling the agent. For details, see "Enable or disable agent self-protection" on page 1392. This is a Windows-only feature.<br>Although `dsa_control` lets you enable self-protection, it does not allow you to configure an associated authentication password. You need Deep Security Manager for that. See "Configure self-protection through Deep Security Manager" on page 1392 for details. Once configured, the password must be entered at the command line using the `-p` or `--passwd=` option.<br>In Deep Security 9.0 and earlier, this option was `-H <num>, --harden=<num>` |
| `-t <num>, --retries=<num>` | If `dsa_control` cannot contact the agent service to carry out accompanying instructions, this parameter instructs `dsa_control` to retry `<num>` number of times. There is a 1 second pause between retries. |
| `-u <user>:<password>` | Used in conjunction with the `-x` option to specify the proxy's username and password, if the proxy requires authentication. Separate the username and password by a colon (:). For example, `# ./dsa_control -x dsm_proxy://<str> -u <new username>:<new password>`.<br>To remove the username and password, type an empty string (""). For example, `# ./dsa_control -x dsm_proxy://<str> -u <existing username>:""`.<br>If you only want to update the proxy's password without changing the proxy's username, you can use the `-u` option without `-x`. For example, `# ./dsa_control -u <existing username>:<new password>`. |

| Parameter | Description |
|---|---|
| | Basic authentication only. Digest and NTLM are not supported.<br>Using `dsa_control -u` only applies to the agent's local configuration. No security policy is changed on the manager as a result of running this command. |
| `-w <user>:<password>` | Used in conjunction with the `-y` option to specify the proxy's username and password, if the proxy requires authentication. Separate the username and password by a colon (:). For example, `# ./dsa_control -y relay_proxy://<str> -w <new username>:<new password>`.<br>To remove the username and password, type an empty string (""). For example, `# ./dsa_control -y relay_proxy://<str> -w <existing username>:""`.<br>If you only want to update the proxy's password without changing the proxy's username, you can use the `-w` option without `-y`. For example, `# ./dsa_control -w <existing username>:<new password>`.<br>Basic authentication only. Digest and NTLM are not supported.<br>Note that using `dsa_control -w` only applies to the agent's local configuration. No security policy is changed on the manager as a result of running this command. |
| `-x dsm_proxy://<str>:<num>` | Configure a proxy between the agent and manager. Provide the proxy's IPv4/IPv6 address or FQDN and port number, separated by a colon (:). Square brackets must surround IPv6 addresses. For example: `dsa_control -x "dsm_proxy://[fe80::340a:7671:64e7:14cc]:808/"`. To remove the address, instead of a URL, type an empty string ("").<br>See also the -u option.<br>For more information, see "Connect to Deep Security Manager via proxy" on page 1337.<br>Note that using `dsa_control -x` only applies to the agent's local configuration. No security policy is changed on the |

| Parameter | Description |
|---|---|
| | manager as a result of running this command. |
| `-y relay_proxy://<str>:<num>` | Configure a proxy between an agent and relay. Provide the proxy's IP address or FQDN and port number, separated by a colon (:). Square brackets must surround IPv6 addresses. For example: `dsa_control -y "relay_proxy://[fe80::340a:7671:64e7:14cc]:808/"`. To remove the address, instead of a URL, type an empty string ("").<br>See also the -w option.<br>For more information, see "Connect to Deep Security Relays via proxy" on page 1338.<br>Note that using `dsa_control -y` only applies to the agent's local configuration. No security policy is changed on the manager as a result of running this command. |
| `--buildBaseline` | Build the baseline for Integrity Monitoring. |
| `--scanForChanges` | Scan for changes for Integrity Monitoring. |
| `--max-dsm-retries` | Number of times to retry an activation. Valid values are 0 to 100, inclusive. The default value is 30. |
| `--dsm-retry-interval` | Approximate delay in seconds between retrying activations. Valid values are 1 to 3600, inclusive. The default value is 300. |

## Agent-initiated activation ("dsa_control -a")

Enabling agent-initiated activation (AIA) can prevent communication issues between the manager and agents, and simplify agent deployment when used with deployment scripts.

For instructions on how to configure AIA and use deployments scripts to activate agents, see "Activate and protect agents using agent-initiated activation and communication" on page 1386.

The command takes the form:

```
dsa_control -a dsm://<host>:<port>/
```

where:

- `<host>` could be either the manager's fully qualified domain name (FQDN), IPv4 address, or IPv6 address.
- `<port>` is the agent-to-manager communication port number (4120 by default).

For example:

```
 dsa_control -a dsm://dsm.example.com:4120/ hostname:www12 "description:Long Description With Spaces"
```

```
dsa_control -a dsm://fe80::ad4a:af37:17cf:8937:4120
```

## Agent-initiated heartbeat command ("dsa_control -m")

You can force the agent to immediately send a heartbeat to the manager.

Like activation, the heartbeat command can also send settings to the manager during the connection.

| Parameter | Description | Example | Use during Activation | Use during Heartbeat |
|---|---|---|---|---|
| `AntiMalwareCancelManualScan` | Boolean.<br>Cancels an on-demand ("manual") scan that is currently occurring on the computer. | `"AntiMalwareCancelManualScan:true"` | no | yes |
| `AntiMalwareManualScan` | Boolean.<br>Initiates an on-demand ("manual") anti-malware scan on the computer. | `"AntiMalwareManualScan:true"` | no | yes |

| Parameter | Description | Example | Use during Activation | Use during Heartbeat |
|---|---|---|---|---|
| `description` | String.<br>Sets the computer's description. Maximum length 2000 characters. | `"description:Extra information about the host"` | yes | yes |
| `displayname` | String.<br>Sets the display name shown in parentheses next to the hostname on **Computers**. Maximum length 2000 characters. | `"displayname:the_name"` | yes | yes |
| `externalid` | Integer.<br>Sets the `externalid` value. This value can be used to uniquely identify an agent. The value can be accessed using the legacy SOAP web service API. | `"externalid:123"` | yes | yes |

| Parameter | Description | Example | Use during Activation | Use during Heartbeat |
|---|---|---|---|---|
| `group` | String.<br>Sets which group the computer belongs to on **Computers**. Maximum length 254 characters per group name per hierarchy level.<br>The forward slash ("/") indicates a group hierarchy. The `group` parameter can read or create a hierarchy of groups.<br>This parameter can only be used to add computers to standard groups under the main "Computers" | `"group:Zone A web servers"` | yes | yes |

| Parameter | Description | Example | Use during Activation | Use during Heartbeat |
|---|---|---|---|---|
| | root branch. It cannot be used to add computers to groups belonging to directories (Microsoft Active Directory), VMware vCenters, or cloud provider accounts. | | | |
| `groupid` | Integer. | `"groupid:33"` | yes | yes |
| `hostname` | String.<br>Maximum length 254 characters.<br>The hostname can specify an IP address, hostname or FQDN that the manager can use to connect to the agent. | `"hostname:www1"` | yes | no |
| `IntegrityScan` | Boolean.<br>Initiates an integrity scan | `"IntegrityScan:true"` | no | yes |

| Parameter | Description | Example | Use during Activation | Use during Heartbeat |
|---|---|---|---|---|
| | on the computer. | | | |
| `policy` | String.<br>Maximum length 254 characters.<br>The policy name is a case-insensitive match to the policy list. If the policy is not found, no policy is assigned.<br>A policy assigned by an event-based task overrides a policy assigned during agent-initiated activation. | `"policy:Policy Name"` | yes | yes |
| `policyid` | Integer. | `"policyid:12"` | yes | yes |
| `relaygroup` | String.<br>Links the computer to a | `"relaygroup:Custom Relay Group"` | yes | yes |

| Parameter | Description | Example | Use during Activation | Use during Heartbeat |
|---|---|---|---|---|
| | specific relay group. Maximum length 254 characters.<br>The relay group name is a case-insensitive match to existing relay group names. If the relay group is not found, the default relay group is used.<br>This does not affect relay groups assigned during event-based tasks. Use either this option or event-based tasks, not both. | | | |
| `relaygroupid` | Integer. | `"relaygroupid:123"` | yes | yes |
| `relayid` | Integer. | `"relayid:123"` | yes | yes |
| `tenantID`and `token` | String. | `"tenantID:12651ADC-D4D5"` | yes | yes |

| Parameter | Description | Example | Use during Activation | Use during Heartbeat |
|---|---|---|---|---|
| | If using agent-initiated activation as a tenant, both `tenantID` and `token` are required. The `tenantID` and `token` can be obtained from the deployment script generation tool. | `and`<br>`"token:8601626D-56EE"` | | |
| `RecommendationScan` | Boolean.<br>Initiate a recommendation scan on the computer. | `"RecommendationScan:true"` | no | yes |
| `UpdateComponent` | Boolean.<br>Instructs Deep Security Manager to perform a security update.<br>When using the `UpdateComponent` parameter on Deep Security | `"UpdateComponent:true"` | no | yes |

| Parameter | Description | Example | Use during Activation | Use during Heartbeat |
|---|---|---|---|---|
| | Agent 12.0 or later, make sure the Deep Security Relay is also at version 12.0 or later. Learn more. | | | |
| `RebuildBaseline` | Boolean.<br>Rebuilds the Integrity Monitoring baseline on the computer. | `"RebuildBaseline:true"` | no | yes |
| `UpdateConfiguration` | Boolean.<br>Instructs Deep Security Manager to perform a "Send Policy" operation. | `"UpdateConfiguration:true"` | no | yes |

## Activate Deep Security Agent

To activate an agent from the command line, you need to know the tenant ID and password. You can get them from the deployment script.

1. In the top right corner of Deep Security Manager, click **Support > Deployment Scripts**.
2. Select your platform.
3. Select **Activate Agent automatically after installation**.
4. In the deployment script, locate the strings for `tenantID` and `token`.

### Windows

In PowerShell:

```
& $Env:ProgramFiles"\Trend Micro\Deep Security Agent\dsa_control" -a <manager
URL> <tenant ID> <token>
```

In cmd.exe:

```
C:\Windows\system32>"\Program Files\Trend Micro\Deep Security Agent\dsa_
control" -a <manager URL> <tenant ID> <token>
```

### Linux, AIX, and Solaris

```
/opt/ds_agent/dsa_control -a <manager URL> <tenant ID> <token>
```

## Force the agent to contact the manager

### Windows

In PowerShell:

```
& "\Program Files\Trend Micro\Deep Security Agent\dsa_control" -m
```

In cmd.exe:

```
C:\Windows\system32>"\Program Files\Trend Micro\Deep Security Agent\dsa_
control" -m
```

### Linux, AIX, and Solaris

```
/opt/ds_agent/dsa_control -m
```

## Initiate a manual anti-malware scan

### Windows

1. Open a command prompt (cmd.exe) as Administrator.
2. Enter these commands:

   ```
   cd C:\Program Files\Trend Micro\Deep Security Agent\
   ```

   ```
   dsa_control -m "AntiMalwareManualScan:true"
   ```

### Linux, AIX, and Solaris

```
/opt/ds_agent/dsa_control -m "AntiMalwareManualScan:true"
```

## Create a diagnostic package

If you need to troubleshoot a Deep Security Agent issue, your support provider might ask you to create and send a diagnostic package from the computer. For more detailed instructions, see "Create an agent diagnostic package via CLI on a protected computer" on page 1726.

You can produce a diagnostic package for a Deep Security Agent computer through the Deep Security Manager but if the agent computer is configured to use Agent/Appliance Initiated communication, then the manager cannot collect all the required logs. So when Technical Support asks for a diagnostic package, you need to run the command directly on the agent computer.

## Reset the agent

This command removes the activation information from the target agent and deactivates it.

### Windows

In PowerShell:

```
& "\Program Files\Trend Micro\Deep Security Agent\dsa_control" -r
```

In cmd.exe:

```
C:\Windows\system32>"\Program Files\Trend Micro\Deep Security Agent\dsa_
control" -r
```

### Linux, AIX, and Solaris

```
/opt/ds_agent/dsa_control -r
```

# dsa_query

You can use the `dsa_query` command to display agent information.

## dsa_query options

```
dsa_query [-c <str>] [-p <str>] [-r <str]
```

| Parameter | Description |
|---|---|
| `-p,--passwd` | Authentication password used with the optional agent self-protection feature. Required if you specified a password when enabling self-protection. |

| Parameter | Description |
|---|---|
| `<string>` | For some query-commands, authentication can be bypassed directly, in which case password is not required. |
| `-c,--cmd <string>` | Execute query-command against the agent. The following commands are supported:<br>• `"GetHostInfo"`: to query which identity is returned to the manager during a heartbeat<br>• `"GetAgentStatus"`: to query which protection modules are enabled, the status of Anti-Malware or Integrity Monitoring scans in progress, and other miscellaneous information<br>• `"GetComponentInfo"`: to query version information of anti-malware patterns and engines<br>• `"GetPluginVersion"`: to query version information of the agent and protection modules<br>• `“GetProxyInfo”`: to query proxy information of all proxy types |
| `-r,--raw <string>` | Returns the same query-command information as `"-c"` but in raw data format for third party software interpretation. |
| `pattern` | 1. Wild card pattern to filter result. Optional.<br>**Example:**<br>`dsa_query -c "GetComponentInfo" -r "au" "AM*"`<br>1. As an option to print more detailed content.<br>**Example:**<br>`dsa_query -c GetProxyInfo details=true` |

## Check CPU usage and RAM usage

### Windows

Use the Task Manager or procmon.

### Linux and Solaris

```
top
```

### AIX

```
topas
```

## Check that ds_agent processes or services are running

### Windows

Use the Task Manager or procmon.

### Linux, AIX, and Solaris

```
ps -ef|grep ds_agent
```

## Restart an agent on Linux

```
service ds_agent restart
```

or

```
/etc/init.d/ds_agent restart
```

or

```
systemctl restart ds_agent
```

Some actions require either a `-tenantname` parameter or a `-tenantid` parameter. If execution problems occur when you use the tenant name, try the command using the associated tenant ID.

## Restart an agent on Solaris

```
svcadm restart ds_agent
```

## Restart an agent on AIX

```
stop agent: stopsrc -s ds_agent
```

```
start agent: startsrc -s ds_agent
```

# dsa_scan

If you have Administrator privileges on Windows or root access rights on Linux, you can use the `dsa_scan` command to execute a scan task with specified files or directories, including subdirectories.

`dsa_scan` allows for concurrent execution of up to ten Deep Security Agent instances.

This command ignores the agent's current scan policy on inclusions and exclusions settings (**Policy > Anti-Malware > Inclusion > Manual and Policy > Anti-Malware > Exclusions > Manual**).

To use `dsa_scan`:

On Windows:

1. Open the Command Prompt as an Administrator.
2. Change to the agent's installation directory:
   `cd C:\Program Files\Trend Micro\Deep Security Agent\`
3. Run the `dsa_scan` command:
   `dsa_scan <option>`
   where `<option>` is one or more options described in "dsa_scan options" below.

On Linux, execute the following command:

`sudo /opt/ds_agent/dsa_scan <option>`
where `<option>` is one or more options described in "dsa_scan options" below

The `dsa_scan` command is not supported on macOS.

## dsa_scan options

`dsa_scan [--target <str>] [--action <str>] [--log <str>]`

| Parameter | Description |
|---|---|
| `--target` | File paths or directories with the delimiter "\|" to separate the input file absolute paths and directories.<br>Example file path and directories: `"c:\user data\|c:\app\config.exe\|c:\workapps"`<br>Example command: `dsa_scan --target "c:\user` |

| Parameter | Description |
|---|---|
| | `data\|c:\app\config.exe\|c:\workapps"` |
| `--action` | Optional<br>Supported actions are pass, delete, quarantine.<br>The current agent scan actions of Manual Scan Configuration are applied if the parameter action is not supplied.<br>Example command: `dsa_scan --action delete --target "c:\user data\|c:\app\config.exe"` |
| `--log` | Optional<br>The absolute file path of an output log file.<br>If this option is not supplied, the scan result outputs to the command-line console.<br>Example output file: `"c:\temp\scan.log"`<br>Example command: `dsa_scan --target "c:\users\" --log "c:\temp\scan.log"` |
| `--scanLargeFile` | Optional<br>Enable scan of large files.<br>When large files containing viruses are detected, the scan returns [Infected] and pass action.<br>Note that large files included in the compressed files cannot be scanned.<br>Example command: `dsa_scan --target "c:\user data\|c:\app\config.exe" --scanLargeFile` |

## dsa_scan output

The following table describes the scan status labels that you would encounter after executing the `dsa_scan` command:

| Label | Description |
|---|---|
| Skipped | The scan file size limit was reached. |
| Infected | The file was detected by the scan engine and the action had been taken. |
| Warning | The file was detected by the scan engine but it encountered issues on the action taken.<br>Check the error code. |

The following is an example scan output:

```
DSA on-demand scan utility

System date/time: 2023/10/12 16:04:10

trace id: 7acf6855-8547-46fc-a58f-9218d108e727

Scanning...

[Skipped] Path: /home/user1/Documents/oversize.zip

[Skipped] Path: /home/user1/Documents/xxx.big

[Infected] Path: /home/user1/Documents/readme, Action: Passed, Malware Name: EICAR, QuarantineID: 0, Error code: 0

[Infected] Path: /home/user1/Documents/sales.doc, Action: Cleaned, Malware Name: BRAIN.A, QuarantineID: 0, Error code: 0

[Warning] Path: /home/user1/Documents/po.ppt, Action: Quarantine, Malware Name: RANSOM.A, QuarantineID: 0, Error code: 5

[Infected] Path: /home/user1/Documents/shipment.zip(po.exe), Action: Deleted, Spyware Name: BLKFRI.A, QuarantineID: 0, Error code: 0

25 files scanned, 2 skipped in 10 seconds.

4 files out of 25 were infected.

End of Scan.
```

## Scan exit codes

The `dsa_scan` command exit codes indicate either the scan success or failure.

### Success exit codes

The success exit code indicates the `dsa_scan` utility completed the scan tasks without detecting any issues or viruses or skipping files, as per the following table:

| Exit code | Description | Resolution |
|---|---|---|
| 0 | Scan completed and no malware found. | Scan task completed without malware found. |
| 1 | Scan completed with at least one malware found. | Check lines labelled as Infected and Warning in the output. |
| 2 | Scan completed, no malware found but some files skipped. | Check lines labelled as Skipped in the output. |
| 3 | Scan completed, but at least malware found and some files skipped. | Check lines labelled as Infected, Warning, and Skipped in the output. |

### Fatal exit codes

If the `dsa_scan` utility encountered any fatal errors, the `dsa_scan` broke the scan task and exited with an error code, as per the following table:

| Exit code | Description | Resolution |
|---|---|---|
| 246 | The argument string is too long. | The string size limit is 2048 characters.<br>Shorten the target parameter and try again. |
| 247 | The Security Platform is shutting down. | The agent is stopping. Try again later. |
| 248 | Too many instances. | There cannot be more than ten concurrent `dsa_scan` running instances.<br>Reduce the number of instances. |
| 249 | No permission. | The command requires root on Linux and Administrator on Windows.<br>Enable Allow the Agent to Trigger or Cancel a Manual Scan on the scan policy. |
| 250 | Manual Scan Configuration is not set. | Configure the Manual Scan setting on the scan policy. |
| 251 | AM feature is not enabled. | Enable the AM feature on the scan policy. |

| Exit code | Description | Resolution |
|---|---|---|
| 252 | The platform is not supported. | The `dsa_scan` is not supported on the current OS platform. |
| 253 | The agent is not running. | Deep Security Agent is not running. Enable the agent or contact the administrator. |
| 254 | Invalid parameters. | The input parameters are incorrect. |
| 255 | Unexpected error. | Try again later. If the issue persists, contact the administrator. |

# dsm_c

You can use the `dsm_c` command to configure some settings on the manager and to unlock user accounts.

> **Note:** Some commands may cause Deep Security Manager to restart. After executing the commands, ensure that Deep Security Manager has started again.

## dsm_c options

`dsm_c -action` *`actionname`*

To print help on the command, use the `-h` option: `dsm_c -h`

Some actions require either a `-tenantname` parameter or a `-tenantid` parameter. If execution problems occur when you use the tenant name, try the command using the associated tenant ID. Note that all of the parameters shown in brackets in the following table are mandatory.

| Action Name | Description | Usage |
|---|---|---|
| `addazureendpoint` | Add an Azure endpoint to the allowed endpoint list. This command | `dsm_c -action addazureendpoint -endpoint ENDPOINT` |

| Action Name | Description | Usage |
|---|---|---|
| | requires an `ENDPOINT` parameter that must be specified in the format `https://<fqdn>`. The allowed endpoint list is used to validate endpoints that are specified when adding an Azure account to Deep Security Manager. If you do not specify any endpoints, then only the default built-in endpoints are allowed.<br>For more on adding an Azure account, see "Add a Microsoft Azure account to Deep Security" on page 602.<br>Related dsm_c options:<br>`listazureendpoint` and `removeazureendpoint` | |

| Action Name | Description | Usage |
|---|---|---|
| `addcert` | Add a trusted certificate. | `dsm_c -action addcert -purpose PURPOSE -cert CERT` |
| `addregion` | Add a private cloud provider region. | `dsm_c -action addregion -region REGION -display DISPLAY -endpoint ENDPOINT` |
| `changesetting` | Change a setting.<br>You must back up your deployment before running the command. Do not use this command unless you understand the effects of the setting. Misconfigurations can make your service unavailable or your data unreadable. Usually, you only use this command if requested by your technical support provider telling you which setting `NAME` to change. Sometimes this command is | `dsm_c -action changesetting -name NAME [-value VALUE \| -valuefile FILENAME] [-computerid COMPUTERID] [-computername COMPUTERNAME] [-policyid POLICYID] [-policyname POLICYNAME] [-tenantname TENANTNAME \| -tenantid TENANTID]` |

| Action Name | Description | Usage |
|---|---|---|
| | required during regular use, in which case the setting is described in that section of the documentation, such as masterkey. | |
| `createinsertstatements` | Create insert statements (for export to a different database). | `dsm_c -action createinsertstatements [-file FILEPATH] [-generateDDL] [-databaseType sqlserver\|oracle] [-maxresultfromdb count] [-tenantname TENANTNAME \| -tenantid TENANTID]` |
| `diagnostic` | Create a diagnostic package for the system.<br>If needed, you can "Increase verbose diagnostic package process memory" on page 1727. | `dsm_c -action diagnostic [-verbose 0\|1] [-tenantname TENANTNAME \| -tenantid TENANTID]` |
| `disablefipsmode` | Disable FIPS mode. | `dsm_c -action disablefipsmode` |
| `enablefipsmode` | Enable FIPS mode. | `dsm_c -action enablefipsmode` |
| `fullaccess` | Give an administrator the full access role. | `dsm_c -action fullaccess -username USERNAME [-tenantname TENANTNAME \| -tenantid TENANTID]` |

| Action Name | Description | Usage |
|---|---|---|
| `listazureendpoint` | List all allowed Azure endpoints.<br>Related dsm_c options:<br>`addazureendpoint` and `removeazureendpoint` | `dsm_c -action listazureendpoint` |
| `listcerts` | List trusted certificates. | `dsm_c -action listcerts [-purpose PURPOSE]` |
| `listregions` | List private cloud provider regions. | `dsm_c -action listregions` |
| `masterkey` | Generate, import, export, or use a custom master key to encrypt the:<br>• database password<br>• keystore password<br>• personal data<br>If a custom master key is not configured, Deep Security uses a hard-coded seed. | If you already configured a master key during a **new install**, the installer has completed this setup for you. If you skipped master key creation, and want to configure one now, start with the commands in step 1. Enter all commands in order. To generate a new master key, start with the commands in step 1 and enter all commands in order.<br>If you configured the master key during an **upgrade**, back up your database and properties files, and then start with the commands in step 4.<br>1. `dsm_c -action masterkey -subaction [generatekmskey -arn AWSARN \| generatelocalkey]` – Generate the master key using either the Amazon Resource Name (ARN) of a Key Management System (KMS) key, or a local environment variable named `LOCAL_KEY_SECRET`. If using the |

| Action Name | Description | Usage |
|---|---|---|
| | | local environment variable on a multi-node Deep Security Manager, it must be configured on all nodes at the system-level (not user-level), and must include, at a minimum:<br>• a capital letter<br>• a lower cased letter<br>• a number<br>• a special character<br>• 8-64 characters<br>Permissions and reliable network access to KMS or `LOCAL_KEY_SECRET` are required by Deep Security Manager if you configure the master key. The manager uses them to encrypt and decrypt the master key during use. If they temporarily cannot be reached, Deep Security Manager is unable to decrypt required data and the service is unavailable. Symptoms can include intermittent event logs and alerts for restart failures and various other errors.<br>2. `dsm_c -action masterkey -subaction export -file FILEPATH` – Export the master key to a password-encrypted file for backup. You will be prompted for the password.<br>You must back up the master key by exporting it to a safe location. If the master key is lost or destroyed and you do not have a backup, all encrypted data becomes unreadable. If that happens, you must reinstall Deep Security Manager, all relays, |

| Action Name | Description | Usage |
|---|---|---|
| | | and all agents. If the key is stolen, security of your Deep Security deployment is compromised. Some compliance regulations such as General Data Protection Regulation (GDPR) in Europe may require you by law to notify law enforcement of personal data breaches within 72 hours, and noncompliance can result in fines. Consult your lawyer for more information.<br>To verify your backup for disaster recovery, you can test it by importing the master key:<br>`dsm_c -action masterkey -subaction [importkmskey -file FILEPATH -arn AWSARN \| importlocalkey -file FILEPATH]` — Import a backup of the master key. This can be useful either for disaster recovery of a corrupted key, or to migrate the master key to another KMS. Before you run this command, you must delete the existing master key from the primary tenant (T0) database.<br>For example, you might enter the SQL command:<br>`delete from systemsettings where uniquekey = 'settings.configuration.keyEncryptingKey'`<br>3. `dsm_c -action masterkey -subaction encryptproperties` — Use the master key to encrypt keystore and database passwords in dsm.properties and configuration.properties. You must restart Deep Security Manager for this setting to take effect. |

| Action Name | Description | Usage |
|---|---|---|
| | | 4. `dsm_c -action masterkey -subaction encrypttenantkey -tenantid [all \| TENANTNUM]` — If you have a multi-tenant deployment, use the master key to encrypt existing tenant key seeds. Tenant key seeds derive subkeys that you can use in the next step. You can execute this command multiple times (this does not apply additional layers of encryption to an already encrypted seed).<br>Optionally, to apply encryption only to new tenants while slowly rolling out to each existing tenant, you can start by executing the following command:<br>`dsm_c -action changesetting -name settings.configuration.encryptTenantKeyForNewTenants -value true`<br>If you only have one (primary) tenant in the environment, `tenantid` can be either `all` or `0`.<br>5. `dsm_c -action masterkey -subaction encryptpii -tenantid [all \| TENANTNUM]` — If you have a multi-tenant deployment, use each tenant's key to encrypt their administrators' and contacts' personal data in the database. If you only have one (primary) tenant in the environment, `tenantid` can be either `all` or `0`.<br>6. `dsm_c -action masterkey -subaction encryptdsmprivatekey -tenantid [all \| TENANTNUM]` — Use the master key to encrypt the private key used for activation and other agent-manager communications |

| Action Name | Description | Usage |
|---|---|---|
| | | via SSL/TLS. If you only have one (primary) tenant in the environment, `tenantid` can be either `all` or `0`.<br>7. `dsm_c -action masterkey -subaction isconfigured` – Check to see whether or not the master key was created. |
| `removeazureendpoint` | Remove an Azure endpoint from allowed endpoint list.<br>You can only remove endpoints added using the `dsm_c -action addazureendpoint` command. Default built-in endpoints cannot be removed.<br>Related dsm_c options:<br>`addazureendpoint` and `listazureendpoint` | `dsm_c -action removeazureendpoint -endpoint ENDPOINT` |
| `removecert` | Remove a trusted certificate. | `dsm_c -action removecert -id ID` |
| `removeregion` | Remove a private cloud | `dsm_c -action removeregion -region REGION` |

| Action Name | Description | Usage |
|---|---|---|
| | provider region. | |
| `resetcounters` | Reset counter tables to an empty state. | `dsm_c -action resetcounters [-tenantname TENANTNAME \| -tenantid TENANTID]` |
| `script` | Perform batch processing of dsm_c commands in a script file. | `dsm_c -action script -scriptfile FILEPATH [-tenantname TENANTNAME \| -tenantid TENANTID]` |
| `setports` | Set Deep Security Manager port(s). | `dsm_c -action setports [-managerPort port] [-heartbeatPort port]` |
| `trustdirectorycert` | Trust the certificate of a directory. | `dsm_c -action trustdirectorycert -directoryaddress DIRECTORYADDRESS -directoryport DIRECTORYPORT [-username USERNAME] [-password PASSWORD] [-tenantname TENANTNAME \| -tenantid TENANTID]` |
| `unlockout` | Unlock a user account. | `dsm_c -action unlockout -username USERNAME [-newpassword NEWPASSWORD] [-disablemfa][-tenantname TENANTNAME \| -tenantid TENANTID]` |
| `upgradetasks` | Runs the upgrade task actions which may be required as part of an in-service upgrade. | `dsm_c -action upgradetasks [-listtasksets] [-listtasks -taskset UPGRADE_TASK_SET [-force]] [-tenantlist] [-tenantsummary] [-run -taskset UPGRADE_TASK_SET [-force] [-filter REGULAR_EXPRESSION]] [-showrollbackinfo -task TASKNAME] [-purgehistory [-task TASKNAME]] [-showhistory [-task TASKNAME]] [-tenantname TENANTNAME \| -tenantid TENANTID]`<br>• `[-listtasksets]`: List sets of tasks for the |

| Action Name | Description | Usage |
|---|---|---|
| | | system as a whole or the tenant specified by `-tenantname`.<br>- `[-listtasks -taskset UPGRADE_TASK_SET [-force]]`: List the modifications to run. Include `-force` to list all tasks.<br>- `[-tenantlist]`: Shows the version of outstanding upgrade actions for the specified tenant.<br>- `[-tenantsummary]`: Shows a summary of the tenants that are not up to date.<br>- `[-run -taskset UPGRADE_TASK_SET [-force] [-filter REGX]]`: Run the upgrade actions for each tenant. Include `-force` to run all tasks even if they have already been done. Include -filter to limit the actions to a regular expression.<br>- `[-showrollbackinfo -task TASKNAME]`: Shows rollback information for the specified task. One tenant or all tenants can be shown.<br>- `[-purgehistory [-task TASKNAME]]`: Purge the history for the tenant specified and the task specified. If no tenant or task is specified, all items are matched.<br>- `[-showhistory [-task TASKNAME]]`: Show the history for the tenant specified and the task specified. If no tenant or task specified, all items are matched. |
| `versionget` | View information about the current software version, the database schema version, or both. | `dsm_c -action versionget [-software] [-dbschema]` |

| Action Name | Description | Usage |
|---|---|---|
| `viewsetting` | View a setting value. | `dsm_c -action viewsetting -name NAME [-computerid COMPUTERID] [-computername COMPUTERNAME] [-policyid POLICYID] [-policyname POLICYNAME] [-tenantname TENANTNAME \| -tenantid TENANTID]` |

## Return codes

The `dsm_c` command returns an integer value that indicates whether or not the command has executed successfully. The following values can be returned:

- `0`: Successful execution.
- `-1`: Failure of an unknown nature, such as corrupt software installation.
- `1`: Failure during execution, such as the database is not currently accessible.
- `2`: Invalid arguments were provided.

# Use the Deep Security API to automate tasks

Deep Security 11.1 and higher have a new RESTful API that enables you to automate the provisioning and maintenance of security via Deep Security. Go to the Deep Security Automation Center to download the SDKs in the language of your choice and learn how to use the API:

- API Reference
- Task-oriented guides with ample code examples
- Support resources

The API is continuously updated with new features and improvements. When you start new automation projects, if the new API meets your needs you should use it to benefit from continued support and maintenance in the long term.

To get started with the API, see the First Steps Toward Deep Security Automation guide in the Deep Security Automation Center.

# Legacy REST and SOAP APIs

**Note:** The REST and SOAP APIs that were provided before Deep Security 11.1 have not changed. They have been deprecated, so new features will not be added but the existing API functionality will continue to function as usual.

Deep Security still includes the legacy REST and SOAP APIs. For guidance on using them, see the following guides on the Deep Security Automation Center:

- Transition from the SOAP API
- Use the Legacy REST API

The following sections explain how to use Deep Security Manager to accomplish tasks that are related to using the SOAP and REST API. For more information about when you need to perform these tasks, see the guides listed above.

## Enable the Status Monitoring API (optional)

To use status monitoring with the legacy REST API, you must enable it. The API is disabled by default as it does not require authentication.

1. On Deep Security Manager, go to **Administration > System Settings > Advanced**.
2. In the Status Monitoring API section, select **Enabled**, then click **Save**.

## Create a Web Service user account

Create a role for Web Service-only access, and assign it to a new user.

1. On Deep Security Manager, go to **Administration** > **User Management** > **Roles** .
2. Click **New**.
3. Deselect the **Allow Access to Deep Security Manager User Interface** check box and select the **Allow Access to Web Service API check box**.
4. When all other configuration is complete, click **Save**.
5. Go to **Administration** > **User Management** > **Users** and click **New**.
6. Create a new user for use only with the Web Service API. Assign the new Role previously created to this user.
   *Make note of the new user account user name and password.*

# Schedule Deep Security to perform tasks

Deep Security has many tasks that you might want to perform automatically on a regular basis. Scheduled tasks are useful when deploying Deep Security in your environment and also later, to keep your system up to date and functioning smoothly. They are especially useful for running scans on a regular basis during off-peak hours.

Tip: You can automate scheduled task creation and configuration using the Deep Security API. For examples, see the Maintain Protection Using Scheduled Tasks guide in the Deep Security Automation Center.

## Create scheduled tasks

To set up a scheduled task in the Deep Security Manager, click **Administration** > **Scheduled Tasks** > **New**. This opens the "New Scheduled Task Wizard", which takes you through the steps to create a scheduled task.

**Check for Security Updates:** Regularly check for security updates and import them into Deep Security when they are available. For most organizations, performing this task once daily is ideal.

Note: With Deep Security 11.0 Update 2 or later, the "Check for Security Updates" task ignores offline hosts that have been uncommunicative for 30 days or more.

**Check for Software Updates:** Regularly check for Deep Security Agent software updates and download them when they are available.

**Discover Computers:** Periodically check for new computers on the network by scheduling a Discovery operation. You will be prompted for an IP range to check and asked to specify which computer group the new computer will be added to. This task is useful for discovering computers that are not part of your cloud connector.

**Generate and Send Report:** Automatically generate reports and optionally have them emailed to a list of users.

**Scan Computers for Integrity Changes:** Causes the Deep Security Manager to perform an Integrity Scan to compare a computer's current state against its baseline.

**Scan computers for Malware:** Schedules a Malware Scan. The configuration of the scan is specified on the Policy or Computer Editor > Anti-Malware page for each computer. For most organizations, performing this task once weekly (or according to your organization’s policies) is ideal. When you configure this task, you can specify a timeout value for the scan. The timeout option is available for daily, weekly, monthly, and once-only scans. It is not available for hourly scans. When a scheduled malware scan is running and the timeout limit has been reached, any tasks that are currently running or pending are canceled.

Tip: When a **Scan Computers for Malware** task times out, the next scheduled scan starts over from the beginning (it does not start where the previous scan ended). The goal is to perform a complete scan, so consider making some configuration changes if your scans regularly reach the timeout limit. You can change the malware scan configuration to add some exceptions, or extend the timeout period.

**Scan Computers for Open Ports:** Schedule periodic port scans on one or more computers. You can specify individual computers or all computers belonging to a particular computer group. Deep Security Manager will scan the port numbers defined on the Scanning tab in the Policy or Computer Editor > Settings page.

**Scan Computers for Recommendations:** Causes the Deep Security Manager to scan the computer(s) for common applications and then make recommendations based on what is detected. Performing regular recommendation scans ensures that your computers are protected by the latest relevant rule sets and that those that are no longer required are removed. If you have set the "Automatically implement Recommendations" option for each of the three protection modules that support it, Deep Security will assign and unassign rules that are required. If rules are identified that require special attention, an alert will be raised to notify you. For most organizations, performing this task once a week is ideal.

Note: Recommendation Scans can be CPU-intensive, so when scheduling Recommendation Scans, it is best practice to set the task by group (for example, per policy or for a group of computers, no more than 1,000 machines per group) and spread it in different days (for example, database server scans scheduled every Monday; mail server scans scheduled every Tuesday, and so on). Schedule Recommendation Scans more frequently for systems that change often.

**Scheduled Agent Upgrade Task:** Schedules an agent upgrade. You can reference Upgrade best practices for agents to help you determine the best schedule for agent upgrades.

Tip: You can configure this task to upgrade the agent to the latest version, or one of the two versions before it. The exact version the agent will upgrade to is determined when the scheduled task is executed. The examples provided within the scheduled task configuration wizard are based on the Red Hat Enterprise Linux agent versions.

**Send Outstanding Alert Summary:** Generate an email listing all outstanding (unresolved) alerts.

**Send Policy:** Regularly check for and send updated policies. Scheduled updates allow you to follow an existing change control process. Scheduled tasks can be set to update machines during maintenance windows, off hours, etc.

**Synchronize Cloud Account:** Synchronize the Computers list with an added cloud account. (Only available if you have added a cloud account to the Deep Security Manager. Applies to Azure and vCoud accounts only. Not available for other cloud account types such as AWS and Google Cloud Platform (GCP).)

**Synchronize Directory:** Synchronize the Computers list with an added LDAP directory. (Only available if you have added an LDAP directory to the Deep Security Manager.)

**Synchronize Users/Contact:** Synchronize the Users and Contacts lists with an added Active Directory. (Only available if you have added an Active Directory to the Deep Security Manager.)

## Enable or disable a scheduled task

Existing scheduled tasks can be enabled or disabled. For example, you might want to temporarily disable a scheduled task while you perform certain administrative duties during which you don't want any activity to occur. The control to enable or disable a scheduled task is on the General tab of the Task's Properties window.

## Set up scheduled reports

Scheduled reports are scheduled tasks that periodically generate and distribute reports to users and contacts (this feature used to be named "Recurring Reports"). Most of the options are identical to those for single reports, with the exception of the time filter.

**Tip:** To generate a report on specific computers from multiple computer groups, create a user who has viewing rights only to the computers in question and then either create a scheduled task to regularly generate an "All Computers" report for that user or sign in as that user and run an "All Computers" report. Only the computers to which that user has viewing rights will be included in the report.

# Automatically perform tasks when a computer is added or changed (event-based tasks)

**Note:** In this article, references to protecting virtual machines apply only to Deep Security On-Premise software installations.

Event-based tasks let you monitor protected computers for specific events and perform tasks based on certain conditions.

## Create an event-based task

In Deep Security Manager, click **Administration > Event-Based Tasks > New**. The wizard that appears will guide you through the steps of creating a new task. You will be prompted for different information depending on the type of task.

## Edit or stop an existing event-based task

To change the properties for an existing event-based task, go to click **Administration > Event-Based Tasks**. Select the event-based task from the list and click **Properties**.

## Events that you can monitor

- **Computer Created (by System):** A computer being added to the manager during synchronization with an Active Directory or Cloud Provider account, or the creation of a virtual machine on a managed ESXi server running a virtual appliance.
- **Computer Moved (by System):**A virtual machine being moved from one vApp to another within the same ESXi, or a virtual machine on an ESXi being move from one datacenter to another or from one ESXi to another (including from an unmanaged ESXi server to a managed ESXi server running a virtual appliance.)
- **Agent-Initiated Activation:** An agent is activated using agent-initiated activation.
- **IP Address Changed:** A computer has begun using a different IP.
- **NSX Security Group Changed:** The following situations will trigger this event (the event will be recorded on each affected VM):
  - A VM is added to a group that is (indirectly) associated with the NSX Deep Security Service Profile

    - A VM is removed from an NSX Group that is associated with the NSX Deep Security Service Profile
    - An NSX Policy associated with the NSX Deep Security Service Profile is applied to an NSX Group
    - An NSX Policy associated with the NSX Deep Security Service Profile is removed from an NSX Group
    - An NSX Policy is associated with the NSX Deep Security Service Profile
    - An NSX Policy is removed from the NSX Deep Security Service Profile
    - An NSX Group that is associated with an NSX Deep Security Service Profile changes name
- **Computer Powered On (by System)**: Enables users to trigger activation by the VMware Virtual Machine power on event.

  > **Note:** The Computer Powered On event is only compatible with virtual machines hosted on ESX environments in VMWare. Use this event cautiously because if a large number of computers are turned on at the same time, this event could cause a slowdown.

## Conditions

You can require specific match conditions to be met in order for a task to be carried out. For example, you might require an AWS 'tag' of `ProductionSystem` to be present in an Amazon EC2 instance in order for the **Activate Computer** action (see "Actions" on page 1607, below) to occur on it.

When adding conditions:

- Click the "plus" button to add multiple conditions. In a multi-condition setup, ALL conditions must be met for the action to be carried out.
- Use Java regular expression syntax (regex). Some examples of how to use regex are provided in the table below. For details on regex, see https://docs.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html.

## List of conditions and descriptions of each

- **Cloud Instance Image ID**: AWS cloud instance AMI ID.

  > **Note:** This match condition is only available for AWS instances added to the manager through **Computers > Add > Add AWS Account**.

- **Cloud Instance Metadata:** The metadata being matched corresponds to AWS tags, Azure tags, or GCP labels that have been added to your AWS, Azure, or GCP instances.

  > **Note:** This match condition is available for AWS instances and Azure or GCP VMs added to the manager through **Computers > Add > [Add AWS Account**, **Add Azure Account**, or **Add GCP Account**]. Metadata currently associated with a computer is displayed on the **Overview** page in its editor window. To define the conditions to match for, you must provide two pieces of information: the metadata key and the metadata value. For example, to match a computer which has a metadata key named "**AlphaFunction**" that has a value of "**DServer**", you would enter "**AlphaFunction**" and "**DServer**" (without the quotes). If you wanted match more than one possible condition, you could use regular expressions and enter "**AlphaFunction**" and "**.*Server**", or "**AlphaFunction**" and "**D.***".

- **Cloud Instance Security Group Name**: The security group the cloud instance applies to.

  > **Note:** This match condition is only available for AWS cloud instances.

- **Cloud Account Name**: The "Display Name" field in the Cloud Account properties window.
- **Cloud Vendor**: The cloud environment vendor of the instance. This condition is used to match on instances from a specific cloud vendor. Currently, you can match on AWS, Azure, and GCP vendors.

  > **Note: Cloud Vendor** only works if you added your cloud instances to the manager through **Computers > Add > [Add AWS Account**, **Add Azure Account**, or **Add GCP Account**].

- **Computer Name**: The "Hostname" field in the computer properties window.
- **ESXi Name**: The "Hostname" field of the ESXi server on which the VM computer is hosted.
  **ESXi Name**: The "Hostname" field of the ESXi server on which the VM computer is hosted.
- **Folder Name**: The name of the folder or directory in which the computer is located in its local environment.

> **Note:** This match condition looks for a match against the name of **any** parent folder of the computer, including the root datacenter for vCenter server integrations. If you add a "*" character to the beginning of the regular expression, the condition must match the name on **all** parent folders. This is particularly useful when combined with negation in a regular expression. For example, if you want to match computers in folders that do not include "Linux" in the folder name, you could use a regular expression like `*^((?!Linux).)*$`.

- **GCP Network Tag**: Network tags that have been added to GCP VMs.

> **Note:** If the GCP VM has multiple GCP network tags, and a match is found on *any* one of them, the VM is considered as matched.

- **NSX Security Group Name:** The list of potential groups in this condition refers only to NSX Groups associated with NSX Policies associated with the NSX Deep Security Service Profile. The VM may be a member of other NSX Groups but for the purposes of this match, condition it is not relevant.
- **Platform**: The operating system of the computer.
- **vCenter name:** The "Name" field of the computer's vCenter properties that was added to Deep Security Manager.

These next two conditions match True or False conditions:

- **Appliance Protection Available:** A Deep Security Virtual Appliance is available to protect VMs on the ESXi on which the VM is hosted. The VM may or may not be in a "Activated" state.
- **Appliance Protection Activated**: A Deep Security Virtual Appliance is available to protect VMs on the ESXi on which the VM is hosted and the VM is "Activated".

This condition looks for matches to an IP in an IP list:

- **Last Used IP Address:** The current or last known IP address of the computer.

> **Note:** Depending on the source of the new computer, some fields may not be available. For example, "Platform" would not be available for computers added as a result of the synchronization with an Active Directory.

## Java regex examples

| To match: | Use this: |
|---|---|
| any string (but not nothing) | .+ |
| empty string (no text) | ^$ |
| Folder Alpha | Folder\ Alpha |
| FIN-1234 | FIN-\d+<br>**or**<br>FIN-.* |
| RD-ABCD | RD-\w+<br>**or**<br>RD-.* |
| AB<br>**or**<br>ABC<br>**or**<br>ABCCCCCCCCC | ABC* |
| Microsoft Windows 2003<br>**or**<br>Windows XP | .*Windows.* |
| Red Hat 7<br>**or**<br>Some_Linux123 | .*Red.*\|.*Linux.*\| |

## Actions

The following actions can be taken depending on which of the above events is detected:

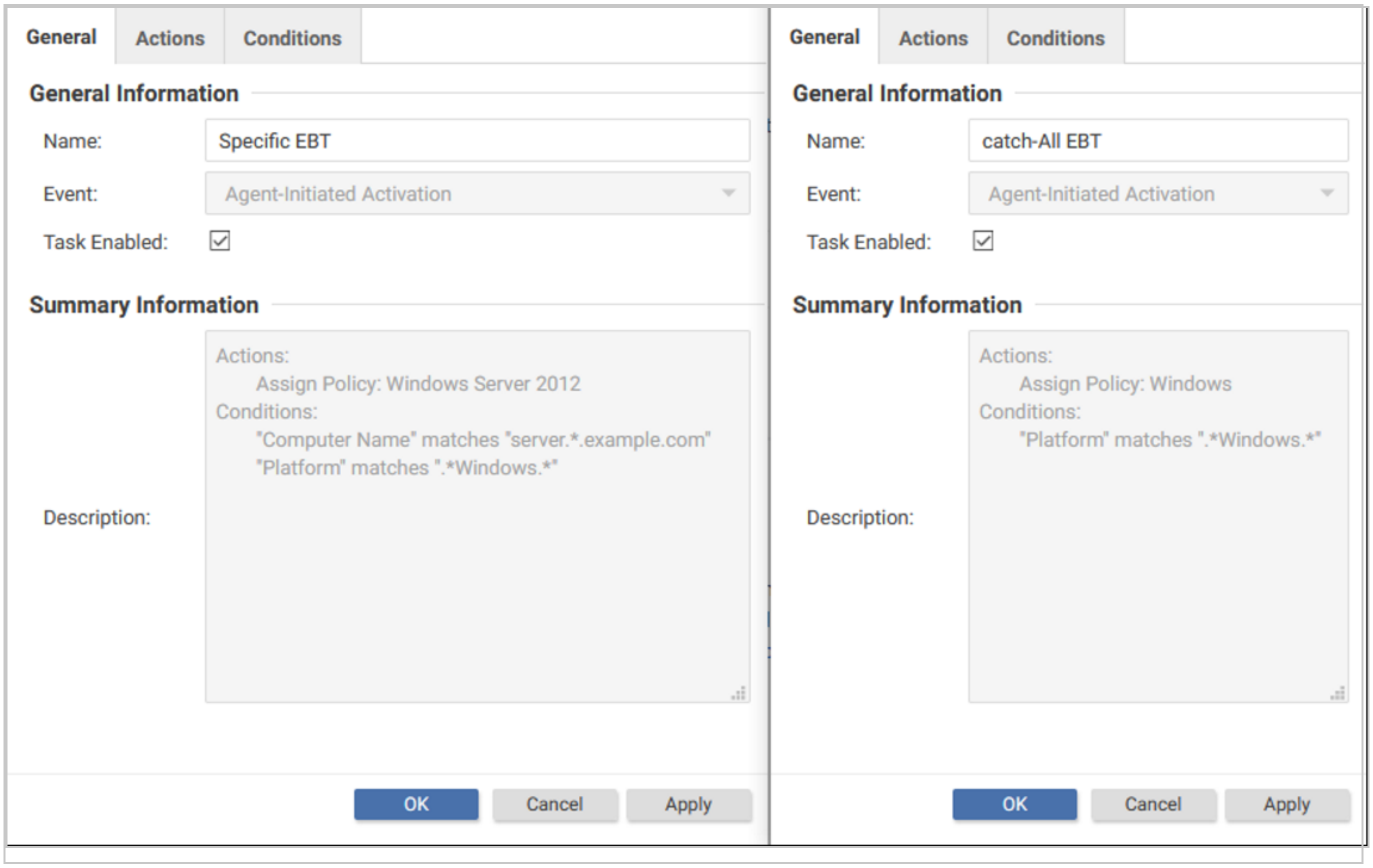
- **Activate Computer:** Deep Security protection is activated on the computer.
  - **Delay activation by (minutes):** Activation is delayed by a specified number of minutes.
- **Note:** If the event-based task is intended to apply protection to a VM that is being vMotioned to an ESXi protected by a Deep Security Virtual Appliance, add a delay before activation to allow any pending VMware administrative tasks to complete. The amount of delay varies depending on your environment.
- **Deactivate Computer:**Deep Security protection is deactivated on the computer.
- **Assign Policy:** The new computer is automatically assigned a policy. (The computer must be activated first.)

- **Assign Relay Group:** The new computer is automatically assigned a relay group from which to receive security updates.
- **Assign to Computer Group:** The computer is placed in one of the computer groups on the Computers page.

## Order of execution

When using event based tasks, you should create and use conditions that are unique to each task. This is because when identical conditions are encountered, Deep Security will process them in a specific order, and this order does not take into account the number of conditions within a task to rank said tasks against each other.

For example, if the *server01.example.com* computer on a *Windows Server 2012* platform encountered the following event-based tasks:



General Information

Name: Specific EBT

Event: Agent-Initiated Activation

Task Enabled: ☑

Summary Information

Actions:
Assign Policy: Windows Server 2012
Conditions:
"Computer Name" matches "server.*.example.com"
"Platform" matches ".*Windows.*"

Description:

General Information

Name: catch-All EBT

Event: Agent-Initiated Activation

Task Enabled: ☑

Summary Information

Actions:
Assign Policy: Windows
Conditions:
"Platform" matches ".*Windows.*"

Description:

The event-based task with more conditions is not automatically executed first. Instead, the "Platform" condition is matched twice, and the event-based tasks are executed based on the name of the task and your database type.

- **PostgreSQL**: "a task", "A task", "b task", "B task"
- **Oracle**: "A task", "B task", "a task", "b task" (ASCIIBetical order)
- **Microsoft SQL Server**: Depends on the locale of the operating system.

However, keep in mind that this order does not stop on the first match, and instead stops on the last match. This, in practice, means that if you're using Oracle, the example above would be assigned a policy by the "catch-All EBT" because using ASCIIBetical order dictates that the "c" in "catch" comes after "S" in "Specific".

To avoid unexpected results, use a specific naming convention for your event-based tasks, such as CamelCase.

**Note:** The order of task names is actually dictated by what collation scheme you use for the column "name" of the table "scheduledtasks" within your database. For example, Oracle uses the collation scheme "NLS_COMP:BINARY" and "NLS_SORT:BINARY" as its default collation scheme for all columns, and that sorts task name strings in ASCIIBetical order.

## Temporarily disable an event-based task

To prevent an existing event-based task from running, right-click it and then click **Disable** . For example, you may want to temporarily disable an event-based task while you perform certain administrative duties during which you don't want any activity to occur.

To re-enable an event-based task, right-click it and then click **Enable**.

# AWS Auto Scaling and Deep Security

You can set up automatic protection in Deep Security for new instances created by AWS Auto Scaling.

Each instance created by Auto Scaling will need to have a Deep Security agent installed on it. There are two ways that you can do this: you can include a pre-installed agent in the EC2 instance used to create the AMI, or you install the agent by including a deployment script in the launch configuration for the AMI. There are pros and cons for each option:

- If you include a pre-installed agent, instances will spin up more quickly because there is no need to download and install the agent software. The downside is that the agent software might not be the latest. To work around this issue, you can enable the upgrade on activation

feature.
- If you use a deployment script to install the agent, it will always get the latest version of the agent software from the Deep Security Manager.

## Pre-install the agent

If you have an EC2 instance already configured with a Deep Security Agent, you can use that instance to create the AMI for Auto Scaling. Before creating the AMI, you must deactivate the agent on the EC2 instance and stop the instance:

```
dsa_control -r
```

Each new EC2 instance created by Auto Scaling needs to have its agent activated and a policy applied to it, if it doesn't have one already. There are two ways to do this:

- You can create a deployment script that activates the agent and optionally applies a policy. Then add the deployment script to the AWS launch configuration so that it is run when a new instance is created. For instructions, see the "Install the Agent with a deployment script" section below, but omit the section of the deployment script that gets and installs the agent. You will only need the dsa_control -a section of the script.

  **Note:** For the deployment scripts to work, agent-initiated communication must be enabled on your Deep Security Manager. For details on this setting, see "Activate and protect agents using agent-initiated activation and communication" on page 1386

- You can set up an event-based task in Deep Security Manager that will activate the agent and optionally apply a policy when an instance it launched and the "Computer Created (By System)" event occurs.

## Install the agent with a deployment script

Deep Security provides the ability to generate customized deployment scripts that you can run when EC2 instances are created. If the EC2 instance does not contain a pre-installed agent, the deployment script should install the agent, activate it, apply a policy, and optionally assign the machine to a computer group and relay group.

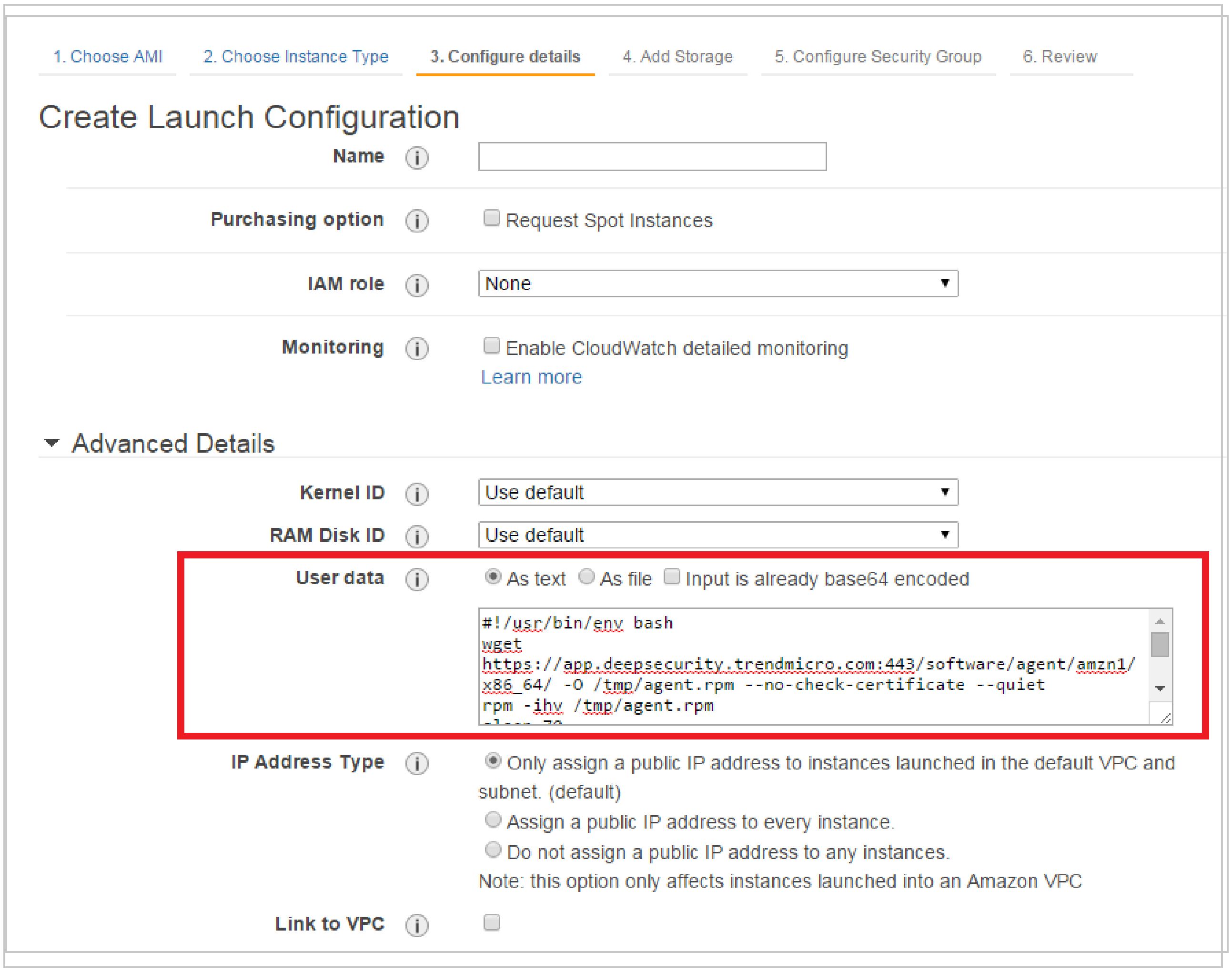
**Tip:** You can generate deployment scripts to automate the agent installation using the Deep Security API. For more information, see Generate an agent deployment script.

In order for the deployment script to work:

- You must create AMIs from machines that are stopped.
- Agent-initiated communication must be enabled on your Deep Security Manager. For details on this setting, see "Activate and protect agents using agent-initiated activation and communication" on page 1386.

**To set up automatic protection for instances using a deployment script:**

1. Sign in to Deep Security Manager.
2. From the **Support** menu in the top right-hand corner, select **Deployment Scripts**.
3. Select your platform.
4. Select **Activate Agent automatically after installation**.
5. Select the appropriate **Security Policy**, **Computer Group** and **Relay Group**.
6. Click **Copy to Clipboard.**
7. Go to the AWS launch configuration, expand **Advanced Details** and paste the deployment script into **User Data**.



Create Launch Configuration

Name

Purchasing option □ Request Spot Instances

IAM role None ▾

Monitoring □ Enable CloudWatch detailed monitoring
Learn more

Advanced Details

Kernel ID Use default ▾

RAM Disk ID Use default ▾

User data ● As text ○ As file □ Input is already base64 encoded

```
#!/usr/bin/env bash
wget
https://app.deepsecurity.trendmicro.com:443/software/agent/amzn1/
x86_64/ -O /tmp/agent.rpm --no-check-certificate --quiet
rpm -ihv /tmp/agent.rpm
```

IP Address Type
● Only assign a public IP address to instances launched in the default VPC and subnet. (default)
○ Assign a public IP address to every instance.
○ Do not assign a public IP address to any instances.
Note: this option only affects instances launched into an Amazon VPC

Link to VPC □

> **Note:** If you are encountering issues getting the PowerShell deployment script to run on a Microsoft Windows-based AMI, the issues may be caused by creating the AMI from a running instance. AWS supports creating AMIs from running instances, but this option disables ALL of the `Ec2Config` tasks that would run at start time on any instance created from the AMI. This behavior prevents the instance from attempting to run the PowerShell script.

> **Note:** When you build an AMI on Windows, you need to re-enable user-data handling manually or as part of your image-building process. The user-data handling only runs in the first boot of the Windows base AMI unless it's explicitly told otherwise (it's disabled during the initial boot process), so instances built from a custom AMI won't run user-data unless the feature is re-enabled. Configuring a Windows Instance Using the EC2Config Service has a detailed explanation and instructions for how to reset the feature or ensure it's not disabled on first boot. The easiest mechanism is to include `<persist>true</persist>` in your user data, providing that you have EC2Config version 2.1.10 or later.

## Delete instances from Deep Security as a result of Auto Scaling

After you have added an AWS Account in the Deep Security Manager, instances that no longer exist in AWS as a result of Auto Scaling will be automatically removed from the Deep Security Manager.

See "About adding AWS accounts" on page 582 for details on adding an AWS account.

# Azure virtual machine scale sets and Deep Security

Azure virtual machine scale sets (VMSS) provide the ability to deploy and manage a set of identical VMs. The number of VMs can increase or decrease automatically based on configurable scaling rules. For more information, see What are virtual machine scale sets in Azure?

You can set up your VMSS to include a base VM image that has the Deep Security Agent pre-installed and pre-activated. As the VMSS scales up, the new VM instances in the scale set automatically include the agent.

To add the agent to your VMSS:

- "Step 1: (Recommended) Add your Azure account to Deep Security Manager" below
- "Step 2: Prepare a deployment script" below
- "Step 3: Add the agent through a custom script extension to your VMSS instances" on the next page

## Step 1: (Recommended) Add your Azure account to Deep Security Manager

When you add your Azure account to Deep Security Manager, all the Azure instances created under that account are loaded into Deep Security Manager and appear under **Computers**. The instances appear regardless of whether they have an agent installed or not. The ones that do not include an agent have a **Status** of **No Agent**. After you install and activate the agent on them, their **Status** changes to **Managed (Online)**.

If the scale set is manually or automatically scaled up after adding your Azure account, Deep Security detects the new Azure instances and adds them to its list under **Computers**. Similarly, if the scale set is scaled down, the instances are removed from view. Thus, Deep Security Manager always shows the current list of available Azure instances in your scale set.

However, if you do not add your Azure account to Deep Security Manager, but instead add individual Azure instances using another method, then Deep Security does not detect any scaling down that might occur, and does not remove the non-existent Azure instances from its list. To prevent an ever-expanding list of Azure VMs in your Deep Security Manager, and to always show exactly which Azure instances are available in your scale set at any one time, it is highly recommended that you add your Azure account to Deep Security Manager.

For instructions on adding your Azure account, see "Add a Microsoft Azure account to Deep Security" on page 602.

## Step 2: Prepare a deployment script

In Deep Security Manager, prepare a deployment script from Deep Security Manager. For instructions, see "Use deployment scripts to add and protect computers" on page 1623. This deployment script will be referenced in a custom script extension that you'll configure next.

**Note:** To run a custom script with the following VMSS script, the script must be stored in Azure Blob storage or in any other location accessible through a valid URL. For instructions on how to upload a file to Azure Blob storage, see Perform Azure Blob storage operations with Azure PowerShell.

## Step 3: Add the agent through a custom script extension to your VMSS instances

Below are a couple of examples on how to use PowerShell to add the agent.

- Example 1 shows how to create a new VMSS that includes the agent
- Example 2 shows how to add the agent to an existing VMSS

Both examples:

- use the Add-AzureRmVmssExtension cmdlet to add an extension to the VMSS
- use Azure PowerShell version 5.1.1

**Note:** For instructions on creating a new VMSS using PowerShell cmdlets, refer to this Microsoft tutorial. For the Linux platform, see https://github.com/Azure/custom-script-extension-linux.

### Example 1: Create a new VMSS that includes the agent

```
$resourceGroupName = <The resource group of the VMSS>
$vmssname = <The name of the VMSS>

# Create ResourceGroup
New-AzureRmResourceGroup -ResourceGroupName $resourceGroupName -Location
EastUS

# Create a config object
$vmssConfig = New-AzureRmVmssConfig `
    -Location EastUS `
    -SkuCapacity 2 `
    -SkuName Standard_DS2 `
    -UpgradePolicyMode Automatic

# Define the script for your Custom Script Extension to run on the Windows Platform
$customConfig = @{
    "fileUris" = (,"A URL of your copy of deployment script, ex. deploymentscript.ps1");
    "commandToExecute" = "powershell -ExecutionPolicy Unrestricted -File deploymentscript.ps1"
}

# Define the script for your Custom Script Extension to run on the Linux Platform
#$customConfig = @{
# "fileUris" = (,"A URL of your copy of deployment script, ex. deploymentscript.sh");
# "commandToExecute" = "bash deploymentscript.sh"
#}

# The section is required only if deploymentscript has been located within Azure StorageAccount
$storageAccountName = <StorageAccountName if deploymentscript is locate in Azure Storage>
$key = (Get-AzureRmStorageAccountKey -Name $storageAccountName -ResourceGroupName $resourceGroupName).Value[0]
$protectedConfig = @{
    "storageAccountName" = $storageAccountName;
    "storageAccountKey" = $key
}
```

```

# Use Custom Script Extension to install Deep Security Agent (Windows)
Add-AzureRmVmssExtension -VirtualMachineScaleSet $vmssConfig `
    -Name "customScript" `
    -Publisher "Microsoft.Compute" `
    -Type "CustomScriptExtension" `
    -TypeHandlerVersion 1.8 `
    -Setting $customConfig `
    -ProtectedSetting $protectedConfig

# Use Custom Script Extension to install Deep Security Agent (Linux)
#Add-AzureRmVmssExtension -VirtualMachineScaleSet $vmssConfig `
# -Name "customScript" `
# -Publisher "Microsoft.Azure.Extensions" `
# -Type "customScript" `
# -TypeHandlerVersion 2.0 `
# -Setting $customConfig `
# -ProtectedSetting $protectedConfig

# Create a public IP address
# Create a frontend and backend IP pool
# Create the load balancer
# Create a load balancer health probe on port 80
# Create a load balancer rule to distribute traffic on port 80
# Update the load balancer configuration
# Reference a virtual machine image from the gallery
# Set up information for authenticating with the virtual machine
# Create the virtual network resources
# Attach the virtual network to the config object

# Create the scale set with the config object (this step might take a few minutes)
New-AzureRmVmss `
    -ResourceGroupName $resourceGroupName `
    -Name $vmssname `
    -VirtualMachineScaleSet $vmssConfig
```

## Example 2: Add the agent to an existing VMSS

```
$resourceGroupName = <The resource group of the VMSS>
$vmssname = <The name of the VMSS>

# Get the VMSS model
$vmssobj = Get-AzureRmVmss -ResourceGroupName $resourceGroupName -VMScaleSetName $vmssname

# Show model data if you prefer
# Write-Output $vmssobj

# Define the script for your Custom Script Extension to run on the Windows platform
$customConfig = @{
    "fileUris" = (,"A URL of your copy of deployment script, ex. deploymentscript.ps1");
    "commandToExecute" = "powershell -ExecutionPolicy Unrestricted -File deploymentscript.ps1"
}

```

```
# Define the script for your Custom Script Extension to run on the Linux platform
#$customConfig = @{
# "fileUris" = (,"A URL of your copy of deployment script, ex. deploymentscript.sh");
# "commandToExecute" = "bash deploymentscript.sh"
#}

# The section is required only if deploymentscript has been located within Azure StorageAccount
$storageAccountName = <StorageAccountName if deploymentscript is locate in Azure Storage>
$key= (Get-AzureRmStorageAccountKey -Name $storageAccountName -ResourceGroupName $resourceGroupName).Value[0]
$protectedConfig = @{
    "storageAccountName" = $storageAccountName;
    "storageAccountKey" = $key
}

# Use Custom Script Extension to install Deep Security Agent (Windows)
$newvmssobj = Add-AzureRmVmssExtension `
    -VirtualMachineScaleSet $vmssobj `
    -Name "customScript" `
    -Publisher "Microsoft.Compute" `
    -Type "CustomScriptExtension" `
    -TypeHandlerVersion 1.8 `
    -Setting $customConfig `
    -ProtectedSetting $protectedConfig

```

```
# Use Custom Script Extension to install Deep Security Agent (Linux)
#$newvmssobj = Add-AzureRmVmssExtension `
#    -VirtualMachineScaleSet $vmssobj `
#    -Name "customScript" `
#    -Publisher "Microsoft.Azure.Extensions" `
#    -Type "customScript" `
#    -TypeHandlerVersion 2.0 `
#    -Setting $customConfig `
#    -ProtectedSetting $protectedConfig

# Update the virtual machine scale set model
Update-AzureRmVmss -ResourceGroupName $resourceGroupName -name $vmssname -VirtualMachineScaleSet $newvmssobj -Verbose

# Get Instance ID for all instances in this VMSS, and decide which instance you'd like to update
# Get-AzureRmVmssVM -ResourceGroupName $resourceGroupName -VMScaleSetName $vmssname

# Now start updating instances
# If upgradePolicy is Automatic in the VMSS, do NOT execute the next command Update-AzureRmVmssInstance. Azure will auto-update the VMSS.
# There's no PowerShell command to update all instances at once. But you could refer to the output of Update-AzureRmVmss, and loop all instances into this command.
Update-AzureRmVmssInstance -ResourceGroupName $resourceGroupName -VMScaleSetName $vmssname -InstanceId 0
```

# GCP auto scaling and Deep Security

You can set up automatic protection in Deep Security for new GCP VM instances created through GCP managed instance groups (MIGs) to support auto scaling.

Each GCP VM instance created through a MIG will need to have a Deep Security agent installed on it. There are two ways that you can do this: you can include a pre-installed agent in the GCP VM instance used to create the instance template, or you can install the agent by including a deployment script in the instance template for the image. There are pros and cons for each option:

- If you include a pre-installed agent, instances will spin up more quickly because there is no need to download and install the agent software. The downside is that the agent software might not be the latest. To work around this issue, you can enable the upgrade on activation feature.
- If you use a deployment script to install the agent, it will always get the latest version of the agent software from the Deep Security Manager.

## Pre-install the agent

If you have a GCP VM instance already configured with a Deep Security Agent, you can use that instance to create the instance template for the MIG. Before creating the instance template, you must deactivate the agent on the GCP VM instance and stop the instance:

```
dsa_control -r
```

Each new GCP VM instance created by the MIG needs to have its agent activated and a policy applied to it, if it doesn’t have one already. There are two ways to do this:

- You can create a deployment script that activates the agent and optionally applies a policy. Then add the deployment script to the GCP instance template so that it is run when a new instance is created. For instructions, see the "Install the agent with a deployment script" on the next page section below, but omit the section of the deployment script that gets and installs the agent. You will only need the `dsa_control -a` section of the script.

  > **Note:** For the deployment scripts to work, agent-initiated communication must be enabled on your Deep Security Manager. For details on this setting, see "Activate and protect agents using agent-initiated activation and communication" on page 1386.

- You can set up an event-based task in Deep Security Manager that will activate the agent and optionally apply a policy when an instance is launched and the "Computer Created (By System)" event occurs.

## Install the agent with a deployment script

Deep Security provides the ability to generate customized deployment scripts that you can run when GCP VM instances are created. If the GCP VM instance does not contain a pre-installed agent, the deployment script should install the agent, activate it, apply a policy, and optionally assign the machine to a computer group and relay group.

> Tip: You can generate deployment scripts to automate the agent installation using the Deep Security API. For more information, see Generate an agent deployment script.

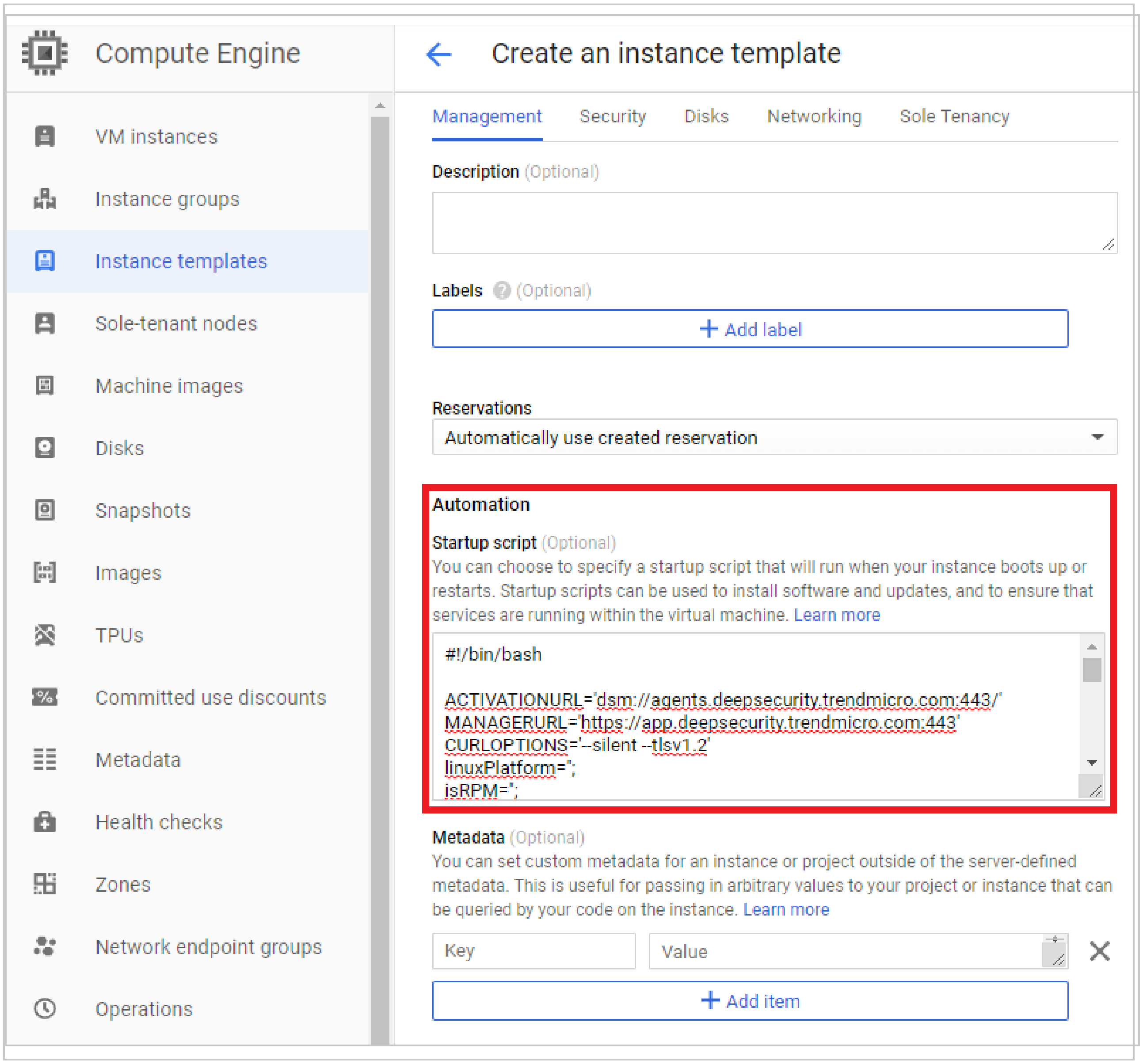
In order for the deployment script to work:

- You must create images from machines that are stopped.
- Agent-initiated communication must be enabled on your Deep Security Manager. For details on this setting, see "Activate and protect agents using agent-initiated activation and communication" on page 1386.

To set up automatic protection for instances using a deployment script:

1. Sign in to Deep Security Manager.
2. From the **Support** menu in the top right-hand corner, select **Deployment Scripts**.
3. Select your platform.
4. Select **Activate Agent automatically after installation**.
5. Select the appropriate **Security Policy**, **Computer Group** and **Relay Group**.
6. Click **Copy to Clipboard**.
7. Go to the GCP instance templates, expand **Management, security, disks, networking,**

**sole tenancy** and paste the deployment script into **Startup script**.



Create an instance template

Description (Optional)

Labels (Optional)

Reservations

Automatically use created reservation

Automation

Startup script (Optional)

You can choose to specify a startup script that will run when your instance boots up or restarts. Startup scripts can be used to install software and updates, and to ensure that services are running within the virtual machine. Learn more

```
#!/bin/bash

ACTIVATIONURL='dsm://agents.deepsecurity.trendmicro.com:443/'
MANAGERURL='https://app.deepsecurity.trendmicro.com:443'
CURLOPTIONS='--silent --tlsv1.2'
linuxPlatform='';
isRPM='';
```

Metadata (Optional)

You can set custom metadata for an instance or project outside of the server-defined metadata. This is useful for passing in arbitrary values to your project or instance that can be queried by your code on the instance. Learn more

# Delete instances from Deep Security as a result of GCP MIGs

After you have added a GCP account in Deep Security Manager, instances that no longer exist in GCP as a result of Managed Instance Group will be automatically removed from the Deep Security Manager.

See "Add a Google Cloud Platform account" on page 614 for details on adding a GCP account.

# Use deployment scripts to add and protect computers

Adding a computer to your list of protected resources in Deep Security and implementing protection is a multi-step process. Almost all of these steps can be performed from the command line on the computer and can therefore be scripted. The Deep Security Manager contains a deployment script writing assistant which can be accessed from the **Support** menu.

The deployment scripts generated through Deep Security Manager do the following:

- install the Deep Security Agent on a chosen platform
- activate the agent
- assign a policy to the agent

## Generate a deployment script

1. Before you begin:
   a. Make sure you have imported the agent software to Deep Security Manager. See "Get Deep Security Agent software" on page 520 for details.
   b. Make sure your agent version control settings are configured as desired. See "Configure agent version control" on page 1367 for details.
   c. Make sure you have enabled agent-initiated activation (AIA). AIA is required if you want your deployment script to activate the agent after installation. See "Activate and protect agents using agent-initiated activation and communication" on page 1386 for details.
2. In the upper right corner of the Deep Security Manager console, click **Support > Deployment Scripts**.
3. Select the platform on which you are deploying the software.
4. Select **Activate agent automatically after installation**.

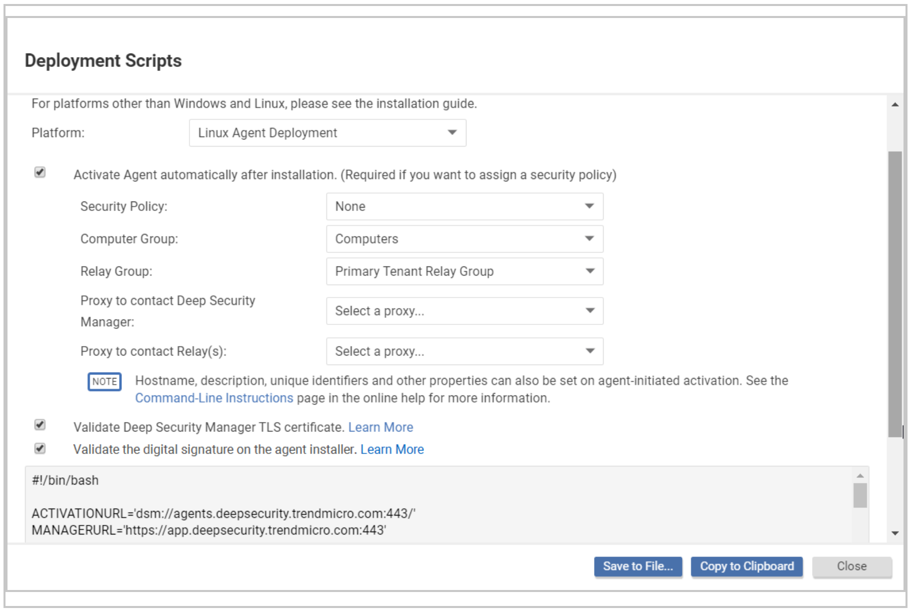
   Agents must be activated before you apply a policy to protect the computer. Activation registers the agent with the manager during an initial communication.

5. Optionally, select the **Security Policy**, **Computer Group**, **Relay Group**, **Proxy to contact Deep Security Manager**, and **Proxy to contact Relay(s)**.
6. Optionally (but highly recommended), select **Validate Deep Security Manager TLS certificate**.

   When this option is selected, it checks that Deep Security Manager is using a valid TLS certificate from a trusted certificate authority (CA) when downloading the agent software, which can help prevent a "man in the middle" attack. You can check whether Deep Security

Manager is using a valid CA certificate by looking at the browser bar in the Deep Security Manager console. By default, Deep Security Manager uses a self-signed certificate, which is not compatible with the **Validate Deep Security Manager TLS certificate** option. If your Deep Security Manager is not behind a load balancer, see "Replace the Deep Security Manager TLS certificate" on page 1494 for instructions on replacing the default self-signed certificate with a certificate from a trusted certificate authority. If the manager is behind a load balancer, you will need to replace the load balancer's certificates.

7. Optionally (but highly recommended), select **Validate the signature on the agent installer** to have the deployment script initiate a digital signature check on the agent installer file. If the check is successful, the agent installation proceeds. If the check fails, the agent installation is aborted. Before you enable this option, understand that:
   - This option is only supported for Linux and Windows installers (RPM, DEB, or MSI files).
   - (Linux only) This option requires that you import the public signing key to each agent computer where the deployment script will run. For details, see "Check the signature on an RPM file" on page 497 and "Check the signature on a DEB file" on page 499.
8. The deployment script generator displays the script. Click **Copy to Clipboard** and paste the deployment script in your preferred deployment tool, or click **Save to File**.



Deployment Scripts

For platforms other than Windows and Linux, please see the installation guide.

Platform: Linux Agent Deployment

☑ Activate Agent automatically after installation. (Required if you want to assign a security policy)

Security Policy: None

Computer Group: Computers

Relay Group: Primary Tenant Relay Group

Proxy to contact Deep Security Manager: Select a proxy...

Proxy to contact Relay(s): Select a proxy...

NOTE Hostname, description, unique identifiers and other properties can also be set on agent-initiated activation. See the Command-Line Instructions page in the online help for more information.

☑ Validate Deep Security Manager TLS certificate. Learn More

☑ Validate the digital signature on the agent installer. Learn More

```
#!/bin/bash

ACTIVATIONURL='dsm://agents.deepsecurity.trendmicro.com:443/'
MANAGERURL='https://app.deepsecurity.trendmicro.com:443'
```

**Note:** The deployment scripts generated by Deep Security Manager for Windows agent deployments require Windows PowerShell version 4.0 or later. You must run PowerShell as an Administrator and you may have to run the following command to be able to run scripts: `Set-ExecutionPolicy RemoteSigned`

**Note:** If you want to deploy an agent to an early version of Windows or Linux that doesn't include PowerShell 4.0 or curl 7.34.0 at a minimum, make sure that early TLS is allowed on the manager and relays. See "Determine whether TLS 1.2 is enforced" on page 1664 and "Enable early TLS (1.0)" on page 1662 for details. Also edit the deployment script as follows:

- **Linux:** Remove the `--tls1.2` tag.
- **Windows:** Remove the `#requires -version 4.0` line. Also remove the `[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12;` line so that early TLS (version 1.0) is used to communicate with the manager.

If you are using Amazon Web Services and deploying new Amazon EC2, Amazon WorkSpace, or VPC instances, copy the generated script and paste it into the **User Data** field. This will let you launch existing Amazon Machine Images (AMIs) and automatically install and activate the agent at startup. The new instances must be able to access the URLs specified in the generated deployment script. This means that your Deep Security Manager must be either Internet-facing, connected to AWS via VPN or Direct Link, or that your Deep Security Manager be deployed on Amazon Web Services too.

When copying the deployment script into the **User Data** field for a **Linux** deployment, copy the deployment script as-is into the "User Data" field and CloudInit will execute the script with sudo. (If there are failures, they will be noted in `/var/log/cloud-init.log`.)

**Note:** The **User Data** field is also used with other services like CloudFormation. For more information, see: https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-waitcondition.html

## Troubleshooting and tips

- If you are attempting to run a deployment script and see exit code 2 **"TLS certificate validation for the agent package download has failed. Please check that your Deep Security Manager TLS certificate is signed by a trusted root certificate authority. For more information, search for "deployment scripts" in the Deep Security Help Center."**, the deployment script was created with the **Validate Deep Security Manager TLS certificate** check box selected. This error appears if Deep Security Manager is using a certificate that is not publicly trusted (such as the default self-signed certificate) for the connection between Deep Security Manager and its agents, or if there is a problem with a third-party certificate, such as a missing certificate in the trust chain between your certificate and the trusted CA. For information on certificates, see "Replace the Deep Security Manager TLS certificate" on page 1494. As an alternative to replacing the trusted certificate, you can clear the **Validate Deep Security Manager TLS certificate** check box when generating a deployment script. Note that this is not recommended for security reasons.

- If you are attempting to deploy the agent from PowerShell (x86), you will receive the following error : `C:\Program Files (x86)\Trend Micro\Deep Security Agent\dsa_control' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.`

  The PowerShell script expects the environment variable for `ProgramFiles` to be set to "Program Files", not "Program Files (x86)". To resolve the issue, close PowerShell (x86) and run the script in PowerShell as an administrator.

- On Windows computers, the deployment script will use the same proxy settings as the local operating system. If the local operating system is configured to use a proxy and the Deep Security Manager is accessible only through a direct connection, the deployment script will fail.
- The deployment script can be modified to perform agent updates instead of new installs by changing the `rpm -ihv` to `rpm -U`.
- If there is a need to control the specific agent version used by the deployment scripts there are 2 options to meet this goal:
  - Use agent version control. See "Configure agent version control" on page 1367 for details. This approach has the advantage that you do not have to hard-code the agent version itself into each script which can be a more flexible approach for some deployments.
  - Either modify the deployment script, or write your own scripts, to meet requirements specific to your deployment. Details on the URL format to download agents can be found here "URL format for download of the agent" on the next page.
- Instead of using the deployment scripts generated by the manager, you can use your own automation method coupled with an agent download URL to automate the download and installation of the agent. For details, see "URL format for download of the agent" on the next page.

# URL format for download of the agent

The Deep Security Agent software package can be downloaded from Deep Security Manager, using a well-defined URL format.

In most cases, use of the standard deployment scripts (which, by the way, also use this same URL format described in this section to download the agent software) is the quickest way to get started and will meet the majority of your deployment requirements.

Use of this URL format directly is useful if you require further customization for the download and install of agents. For example, in some cases it may be necessary to have the deployment scripts that run on each server point to a local storage location (for example, AWS S3) rather than have each server reach out to the manager to download software. You can use this URL format to build your own automation to periodically download new agent versions to your local storage location, and then point the agent deployment scripts that run on each server to your local storage location to meet this objective.

Topics:

## Agent download URL format

The URL format used to download the agent is:

```
https://<dsm fqdn>/software/agent/<platform>/<arch>/<agent
version>/<filename>
```

All the parameters that comprise the URL format are described below.

## <dsm fqdn> parameter

The `<dsm fqdn>` parameter is the fully-qualified domain name of the manager, including the listening port number.

Example:

```
example.com:4119
```

## <filename> parameter

The `<filename>` parameter is the file name of the agent installer file. The file name is dependent on the installation process used by each platform:

| Platform | <filename> |
|---|---|
| Linux<br>Red Hat Enterprise Linux, CentOS, Oracle, CloudLinux, Amazon Linux, SUSE | `agent.rpm` |
| Linux<br>Debian, Ubuntu | `agent.deb` |
| Windows | `agent.msi` |
| AIX | `agent.bff.gz` |
| Solaris 11+ | `agent.p5p.gz` |
| Solaris 10 or earlier | `agent.pkg.gz` |

**Note:** The manager does not validate the file name itself; however when a file name is specified, the extension must be one of `.rpm`, `.msi`, `.deb`, `.gz`. If any other file name is specified, the file name returned by the manager will always be one of the names provided in the table above.

## <agent version> parameter

The `<agent version>` parameter is optional.

When this parameter is not specified, the latest agent in the manager's local inventory for the target platform is returned.

When this parameter is specified, this represents the agent version string. For example "12.0.0.123".

### Should I include the <agent version> explicitly in my scripts?

If your intent is to only use a specific version of the agent in a controlled environment, then explicitly adding the agent version to the URL will accomplish this goal.

When deploying agents at scale, it should be noted that adding the agent version in the URL (which hardcodes this agent version into every script you distribute) can create challenges for security operations teams that will be distributing scripts to many applications teams.

Consider the process that will be needed when the time arrives to use a newer version of the agent. If the `<agent version>` is hardcoded in each script you distribute, this will require that each of these scripts requires an update to start using the new agent version. If you have many internal application teams, the process to request changes to each one of these scripts in use can be significant.

Deep Security provides two options to deal with this challenge:

- Simply use scripts that omit the `<agent version>` component from the path.

  If using the latest agent in the manager's local inventory meets your requirements, this is the most straightforward option to use.

- Use agent version control

  Agent version control provides the ability for the Deep Security administrator to select on a per-platform basis exactly what agent version is returned from the manager. More detail on agent version control and how to leverage this feature from your scripts can be found at "Using agent version control to define which agent version is returned" on page 1633.

## <platform>, <arch>, and <filename> parameters

The `<platform>`, `<arch>`, and `<filename>` parameters should be replaced with the strings listed in the table below.

**Note:** `<platform>` and `<arch>` are case-sensitive.

| Platform | Distribution | <platform> | <arch> | <filename> | Example |
|---|---|---|---|---|---|
| Linux | Amazon 1 | amzn1 | x86_64 | agent.rpm | /software/agent/amzn1/x86_64/agent.rpm |
| | Amazon 2 | amzn2 | x86_64 | agent.rpm | /software/agent/amzn2/x86_64/agent.rpm |
| | CloudLinux 6 | CloudLinux_6 | x86_64 | agent.rpm | /software/agent/CloudLinux_6/x86_64/agent.rpm |
| | CloudLinux 7 | CloudLinux_7 | x86_64 | agent.rpm | /software/agent/CloudLinux_7/x86_64/agent.rpm |
| | CloudLinux 8 | CloudLinux_8 | x86_64 | agent.rpm | /software/agent/CloudLinux_8/x86_64/agent.rpm |
| | Debian 7 | Debian_7 | x86_64 | agent.deb | /software/agent/Debian_7/x86_64/agent.deb |
| | Debian 8 | Debian_8 | x86_64 | agent.deb | /software/agent/Debian_8/x86_64/agent.deb |
| | Debian 9 | Debian_9 | x86_64 | agent.deb | /software/agent/Debian_9/x86_64/agent.deb |
| | Oracle Linux 6 | Oracle_OL6 | x86_64 | agent.rpm | /software/agent/Oracle_OL6/x86_64/agent.rpm |
| | Oracle Linux 6 | Oracle_OL6 | i386 | agent.rpm | /software/agent/Oracle_OL6/i386/agent.rpm |
| | Oracle Linux 7 | Oracle_OL7 | x86_64 | agent.rpm | /software/agent/Oracle_OL7/x86_64/agent.rpm |
| | RedHat 6 | RedHat_EL6 | x86_64 | agent.rpm | /software/agent/RedHat_EL6/x86_64/agent.rpm |

| Platform | Distribution | <platform> | <arch> | <filename> | Example |
|---|---|---|---|---|---|
| | RedHat 6 | RedHat_EL6 | i386 | agent.rpm | /software/agent/RedHat_EL6/i386/agent.rpm |
| | RedHat 7 | RedHat_EL7 | x86_64 | agent.rpm | /software/agent/RedHat_EL7/x86_64/agent.rpm |
| | RedHat 8 | RedHat_EL8 | x86_64 | agent.rpm | /software/agent/RedHat_EL8/x86_64/agent.rpm |
| | SuSE 11 | SuSE_11 | x86_64 | agent.rpm | /software/agent/SuSE_11/x86_64/agent.rpm |
| | SuSE 11 | SuSE_11 | i386 | agent.rpm | /software/agent/SuSE_11/i386/agent.rpm |
| | SuSE 12 | SuSE_12 | x86_64 | agent.rpm | /software/agent/SuSE_12/x86_64/agent.rpm |
| | SuSE 15 | SuSE_15 | x86_64 | agent.rpm | /software/agent/SuSE_15/x86_64/agent.rpm |
| | Ubuntu 16.04 | Ubuntu_16.04 | x86_64 | agent.deb | /software/agent/Ubuntu_16.04/x86_64/agent.deb |
| | Ubuntu 18.04 | Ubuntu_18.04 | x86_64 | agent.deb | /software/agent/Ubuntu_18.04/x86_64/agent.deb |
| Windows | | Windows | x86_64 | agent.msi | /software/agent/Windows/x86_64/agent.msi |
| | | Windows | i386 | agent.msi | /software/agent/Windows/i386/agent.msi |
| Unix | Solaris 10 Updates 4-6 | Solaris_5.10_U5 | x86_64 | agent.pkg.gz | /software/agent/Solaris_5.10_U5/x86_64/agent.pkg.gz |
| | | Solaris_5.10_U5 | sparc | agent.pkg.gz | /software/agent/Solaris_5.10_U5/sparc/agent.pkg.gz |
| | Solaris 10 | Solaris_5.10_U7 | x86_64 | agent.pkg.gz | /software/agent/Solaris_5.10_U7/x86_64/agent.pkg.gz |

| Platform | Distribution | <platform> | <arch> | <filename> | Example |
|---|---|---|---|---|---|
| | Updates 7-11 | | | | |
| | | Solaris_5.10_U7 | sparc | agent.pkg.gz | /software/agent/Solaris_5.10_U7/sparc/agent.pkg.gz |
| | Solaris 11 Updates 1-3 | Solaris_5.11 | x86_64 | agent.p5p.gz | /software/agent/Solaris_5.11/x86_64/agent.p5p.gz |
| | | Solaris_5.11 | sparc | agent.p5p.gz | /software/agent/Solaris_5.11/sparc/agent.p5p.gz |
| | Solaris 11 Update 4 | Solaris_5.11_U4 | x86_64 | agent.p5p.gz | /software/agent/Solaris_5.11_U4/x86_64/agent.p5p.gz |
| | | Solaris_5.11_U4 | sparc | agent.p5p.gz | /software/agent/Solaris_5.11_U4/sparc/agent.p5p.gz |
| | AIX 5.3 (Deep Security Agent 9.0) | AIX_5.3 | powerpc | agent.bff.gz | /software/agent/AIX_5.3/powerpc/agent.bff.gz |
| | AIX 6.1 (Deep Security Agent 9.0) | AIX_6.1 | powerpc | agent.bff.gz | /software/agent/AIX_6.1/powerpc/agent.bff.gz |
| | AIX 7.1, 7.2 (Deep Security Agent 9.0) | AIX_7.1 | powerpc | agent.bff.gz | /software/agent/AIX_7.1/powerpc/agent.bff.gz |
| | AIX 6.1, 7.1, 7.2 (Deep Security | AIX | powerpc | agent.bff.gz | /software/agent/AIX/powerpc/agent.bff.gz |

| Platform | Distribution | <platform> | <arch> | <filename> | Example |
|---|---|---|---|---|---|
| | Agent 12 and up) | | | | |

### Examples

Without `<agent version>`:

- `https://example.com:4119/software/agent/RedHat_EL7/x86_64/agent.rpm`
- `https://example.com:4119/software/agent/Windows/x86_64/agent.msi`

With `<agent version>`:

- `https://example.com:4119/software/agent/RedHat_EL7/x86_64/12.0.0.481/agent.rpm`
- `https://example.com:4119/software/agent/Windows/x86_64/12.0.0.481/agent.msi`

## Exceptions for backwards compatibility

If no `<filename>` is provided after `[...]/<platform>/<arch>/`, the manager will return the agent download for that platform as described in the previous table.

If the path ends at `[...]<platform>/<arch>` (because both `<agent version>` and `<filename>` were not specified), the manager will return the agent download for that platform as described in the table above.

Examples:

- `https://example.come:4119/software/agent/RedHat_EL7/x86_64/`
- `https://example.come:4119/software/agent/Windows/x86_64`

## Using agent version control to define which agent version is returned

The agent version control feature provides the ability to control what agents are returned when any URL request is made to Deep Security to download the agent.

To enable agent version control, send the following HTTP header with your URL request:

```
Agent-Version-Control: on
```

It should be noted that there are specific query parameters that are also required on each platform to use agent version control.  They are:

| Platform | Required query parameters | Example |
|---|---|---|
| Windows | tenantID, windowsVersion, windowsProductType | /software/agent/Windows/x86_64/agent.msi?tenantID=123&windowsVersion=10.0.17134&windowsProductType=3 |
| Linux | tenantID | /software/agent/RedHat_EL7/x86_64/agent.rpm?tenantID=123 |
| Solaris | tenantID | /software/agent/Solaris_5.11_U4/x86_64/agent.p5p.gz?tenantID=123 |
| AIX | tenantID, aixVersion, aixRelease | /software/agent/AIX/powerpc/agent.bff.gz?tenantID=123&aixVersion=7&aixRelease=1 |

**Note:** The parameters in the table above are automatically generated by the deployment scripts.

## Examples

For examples, refer to the sample deployment script generated from the manager.  By default the deployment scripts generated by the manager use agent version control and demonstrate how to acquire these parameters for each platform.

## Interactions between the <agent version> parameter and agent version control

Given the intent of the agent version control feature is to provide the Deep Security administrator control over which agent version is returned, there is a natural conflict with a URL request that also includes the `<agent version>` parameter.

For this reason you should not specify the `<agent version>` as part of your request when sending the `Agent-Version-Control: on` HTTP header.

If we see both the `Agent-Version-Control: on` HTTP header and the `<agent version>` parameter in the request, the version of the agent returned will be determined by the value taken from the agent version control configuration. (We will ignore the <agent version> in the URL.)

# Automatically assign policies using cloud provider tags/labels

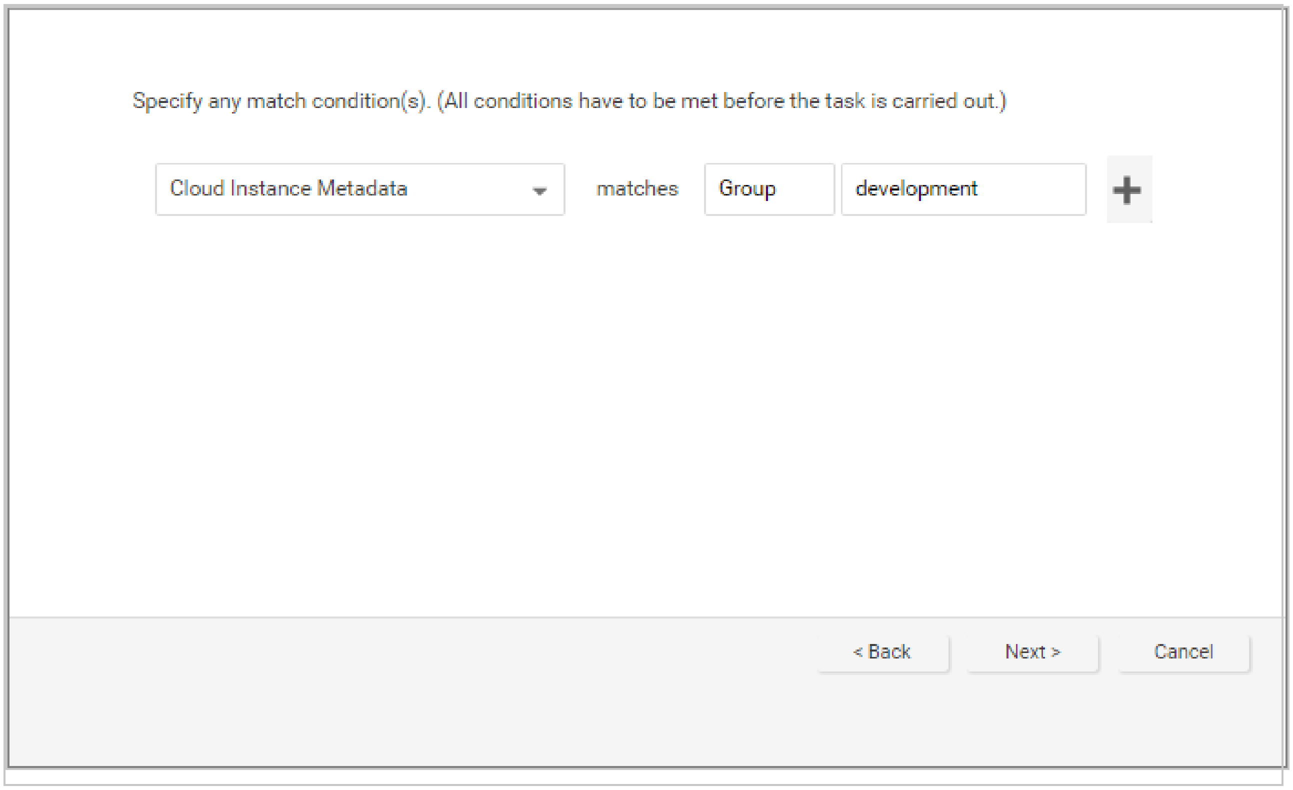
AWS tags, Azure tags, and GCP labels allow you to categorize your resources by assigning metadata to AWS EC2 instances, Azure VMs, or GCP VM instances in the form of keys and values. You can also tag Amazon WorkSpaces with the similar key and value pair. Deep Security can use this metadata to trigger the automatic assigning of a policy to a Deep Security Agent when that agent is activated. This is done by creating an event-based task in Deep Security and defining the event, policy, and metadata. Event-based tasks are used to monitor protected resources for specific events and then perform tasks based on certain conditions: in this case the event is agent-initiated activation and a specific AWS instance tag is the condition.

This article describes how to do this using the following examples:

- Policy: AIA_Policy
- AWS tag key: Group
- AWS tag value: development

**Note:** The example below is based on the assumption that the policy AIA_Policy has already been created.

1. Go to **Administration** -> **Event-Based Tasks** in the Deep Security Manager console and click **New**.
2. Select **Agent-Initiated Activation** from the **Event** list and click **Next**.
3. Select the **Assign Policy** check box, select **AIA_Policy** from the list, and click **Next**.
4. Select **Cloud Instance Metadata** from the list, type **Group** in the key field, and **development** into the value field.



Specify any match condition(s). (All conditions have to be met before the task is carried out.)

Cloud Instance Metadata matches Group development

5. (Optional) To restrict the scope to only one cloud vendor, select **Cloud Vendor** from the list and select **AWS**, **Azure**, or **GCP** as the matching criteria. If you want to apply the rule to all three, don't define the Cloud Vendor condition.
6. Click **Next**.
7. Type and name for the event-based task and click **Finish** to save it.

You have now created an event-based task that will apply the AIA_Policy to an instance tagged with the key "Group" and the value "development" when the agent is activated on that instance.

# Trust and compliance

## About compliance

Trend Micro helps to accelerate compliance by consolidating multiple security controls into one product, while also delivering comprehensive auditing and reporting. For more information, see Regulatory Compliance on the Trend Micro website.

Depending on your requirements, see:

- "Meet PCI DSS requirements with Deep Security" on the next page
- "GDPR" on page 1639
- "FIPS 140 support" on page 1639
- Set up AWS Config Rules
- "Bypass vulnerability management scan traffic in Deep Security" on page 1650
- "Use TLS 1.2 with Deep Security" on page 1652
- "Enable TLS 1.2 strong cipher suites" on page 1665

# Agent package integrity check

Deep Security verifies your signature on the Deep Security Agent to ensure that the software files have not changed since the time of signing. An integrity check occurs when:

1. You're upgrading the Deep Security Agent.
2. You're enabling a new security module so the kernel support is being updated.

If the validation fails, plugin installations and agent upgrades are blocked.

## Troubleshoot

| ID | Event | Reason | Solution |
|---|---|---|---|
| 5302 | Agent/Plugin package signature download failed. | The signature files used to check the integrity of the agent are not available in your update source. Your Deep Security Relay might not be upgraded to the required version. | 1. On the **Alerts** page, check for the "Relay Upgrade Required For Agent Integrity Check" alert. If the alert exists, see "Supported Deep Security Relay versions" on the next page and "Upgrade Deep Security Relay" on page 1541 accordingly. Confirm signature files sync to your update source.<br>2. Confirm your signature files have synced to your update source.<br>3. Attempt to upgrade your agent or send your updated policy again.<br>4. If the issue isn't resolved, "Create a diagnostic package" on page 1723 and send it to the Trend Micro support team. |

| ID | Event | Reason | Solution |
|---|---|---|---|
| 5300 | Agent/Plugin package signature validation failed. | The agent package might have been tampered with or something is wrong on the package. | 1. Backup and delete the possibly tampered file from your update source.<br>2. Delete the corresponding agent package from Deep Security Manager.<br>3. Re-download the agent package from the Download Center and import it to Deep Security Manager.<br>4. Confirm the package has synced to your update source.<br>5. Attempt to upgrade your agent or send your updated policy again.<br>6. If the issue isn't resolved, "Create a diagnostic package" on page 1723 and send it to the Trend Micro support team. |
| 5301 | Agent/Plugin package validation failed. | | |
| 5303 | Agent/Plugin package signature mismatch with the one in our policy. | | |

## Supported Deep Security Relay versions

The following Deep Security Relay versions are supported:

- Deep Security 20
- Deep Security FR 2020-04-16 (12.5.0.834)(Windows)
- Deep Security FR 2020-05-19 (12.5.0.936)(Linux)
- Deep Security 12.0 update 8 (12.0.0.967)
- Deep Security 11.0 update 23 (11.0.1617)

# Meet PCI DSS requirements with Deep Security

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard that promotes the safety of cardholder data. Deep Security can be used to help secure PCI data in accordance with the PCI DSS.

**Tip:**
For PCI compliance, see also "Use TLS 1.2 with Deep Security" on page 1652 or "Enable TLS 1.2 strong cipher suites" on page 1665.

# GDPR

The European Union’s (EU) General Data Protection Regulation (GDPR) mandates that organizations anywhere in the world processing EU citizen data reassess their data processing controls and put a plan in place to better protect it. For information about GDPR and Trend Micro, see the Trend Micro GDPR Compliance site.

For information about personal data collection in Deep Security, see "Privacy and personal data collection disclosure" on page 1671.

# FIPS 140 support

Federal Information Processing Standard (FIPS) is a set of standards for cryptographic modules. For more information, see the National Institute of Standards and Technology (NIST) website. Deep Security provides settings that enable cryptographic modules to run in a mode that is compliant with FIPS 140 standards. Trend Micro obtained certification for Java crypto module and Native crypto module (OpenSSL).

Currently, Deep Security supports FIPS 140-2 standards. As new versions of FIPS-140 are released, Trend Micro will obtain certification to support those standards.

There is a number of differences between a Deep Security deployment running in FIPS mode instead of non-FIPS mode. For more information, see "Differences when operating Deep Security in FIPS mode" on the next page.

If you intend to replace the Deep Security Manager SSL certificate, do so before enabling FIPS mode. If you need to replace the certificate after enabling FIPS mode, you need to disable FIPS mode, then follow the instructions provided in "Replace the Deep Security Manager TLS certificate" on page 1494, and then re-enable FIPS mode.

To operate Deep Security in a FIPS 140 mode, do the following:

1. Review "Differences when operating Deep Security in FIPS mode" on the next page to make sure the Deep Security features you require are available when operating in FIPS 140 mode.
2. Ensure that your Deep Security Manager and Deep Security Agents meet the "System requirements for FIPS mode" on page 1641.
3. "Enable FIPS mode for your Deep Security Manager" on page 1642.

4. If your Deep Security Manager needs to connect to an external service (such as an Active Directory, vCenter, or NSX Manager) using SSL, see "Connect to external services when in FIPS mode" on page 1642.
5. "Enable FIPS mode for the operating system of the computers you are protecting" on page 1643.
6. "Enable FIPS mode for the Deep Security Agent on the computers you are protecting" on page 1644
7. With some versions of the Linux kernel, such as, for example, Red Hat Enterprise Linux (RHEL) 7.0 GA, you must enable Secure Boot to enable FIPS mode. See "Configure Linux Secure Boot for agents" on page 527 for instructions.

You can also "Disable FIPS mode" on page 1649.

## Differences when operating Deep Security in FIPS mode

The following is available for Deep Security Manager 20.0.619 (20 LTS Update 2022-03-22) and later:

- Load balancer settings, accessible via **Administration > System Settings > Advanced > Load Balancers**.
- The STARTTLS option, accessible via **Administration > System Settings > SMTP**.
- Multi-tenant environment.

The following is not available when operating in FIPS mode:

- Connecting to virtual machines hosted on VMware vCloud, as described in "Add virtual machines hosted on VMware vCloud" on page 621. The **Administration > System Settings > Agents > Agentless vCloud Protection** settings are also unavailable.
- Deep Security Scanner (integration with SAP Netweaver).
- Threat Intelligence.

## Check if FIPS mode is enabled on Deep Security Manager

To see if FIPS mode is enabled on Deep Security Manager, go to **Administration > System Information**. Under **System Details**, expand a **Manager Node**. The **FIPS** field indicates whether FIPS mode is enabled or disabled.

When FIPS is enabled for Deep Security Manager deployed on multiple nodes, all Manager Nodes should show FIPS enabled.

# System requirements for FIPS mode

## Deep Security Manager requirements

The Deep Security Manager requirements with FIPS mode enabled are identical to those described in "System requirements" on page 383, with a number of exceptions.

Only the following operating systems are supported:

- Red Hat Enterprise Linux 10 (64-bit)
- Red Hat Enterprise Linux 9 (64-bit)
- Red Hat Enterprise Linux 8 (64-bit)
- Red Hat Enterprise Linux 7 (64-bit)
- Windows Server 2019 (64-bit)
- Windows Server 2016 (64-bit)
- Windows Server 2012 or 2012 R2 (64-bit)

Only the following databases are supported:

- PostgreSQL 17 (see "Use FIPS mode with a PostgreSQL database" on page 1645)
- PostgreSQL 16 (see "Use FIPS mode with a PostgreSQL database" on page 1645)
- PostgreSQL 15 (see "Use FIPS mode with a PostgreSQL database" on page 1645)
- PostgreSQL 14 (see "Use FIPS mode with a PostgreSQL database" on page 1645)
- Microsoft SQL Server 2019 Enterprise Edition (see "Using FIPS mode with a Microsoft SQL Server database" on page 1648)
- Microsoft SQL Server 2016 Enterprise Edition (see "Using FIPS mode with a Microsoft SQL Server database" on page 1648)
- Microsoft SQL Server 2014 Enterprise Edition (see "Using FIPS mode with a Microsoft SQL Server database" on page 1648)
- Microsoft SQL Server 2012 Enterprise Edition (see "Using FIPS mode with a Microsoft SQL Server database" on page 1648)

Oracle Database is not supported, even if it has enabled FIPS mode for SSL connections.

Microsoft SQL Server named pipes are not supported.

AWS Marketplace does not support FIPS mode.

### Deep Security Agent requirements

The Deep Security Agent requirements with FIPS mode enabled are identical to those described in "System requirements" on page 383. FIPS mode is not supported with all operating systems. To check which operating systems are supported, see "Supported features by platform" on page 425.

# Enable FIPS mode for your Deep Security Manager

## Enable FIPS mode for a Deep Security Manager on Windows

1. Use the **Services** window of the Microsoft Management Console to stop the Trend Micro Deep Security Manager service.
2. In the Windows command line, go to the Deep Security Manager's working folder. For example, `C:\Program Files\Trend Micro\Deep Security Manager`.
3. Enter the following command to enable FIPS mode:

   ```
   dsm_c -action enablefipsmode
   ```

4. Restart the Deep Security Manager service.

## Enable FIPS mode for a Deep Security Manager on Linux

1. On the Deep Security Manager computer, open a command line and go to the Deep Security Manager's working folder, for example, `/opt/dsm`.
2. Enter the following command to stop the Deep Security Manager service:

   ```
   service dsm_s stop
   ```

3. Enter the following command to enable FIPS mode:

   ```
   dsm_c -action enablefipsmode
   ```

4. Enter the following command to restart the Deep Security Manager service:

   ```
   service dsm_s start
   ```

# Connect to external services when in FIPS mode

When Deep Security Manager is operating in FIPS mode and you want to connect to an external service (such as an Active Directory, vCenter, or NSX Manager) with an SSL connection, you must import the SSL certificate for that external service into the manager before connecting to it. For instructions on how to import the certificate, see "Manage trusted certificates" on page 1525.

For instructions on importing computers from an Active Directory, see "Add Active Directory computers" on page 577.

For instructions on synchronizing user information with an Active Directory, see "Add and manage users" on page 1410.

For instructions on adding a VMware vCenter to Deep Security Manager, see "Add a vCenter - FIPS mode" on page 621.

## Enable FIPS mode for the operating system of the computers you are protecting

For instructions on enabling FIPS mode for supported operating systems, refer to the following documents from the operating system providers:

- **Windows:** System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing security setting effects in Windows XP and in later versions of Windows
- **RHEL 7 or CentOS 7:** Federal Standards and Regulations and How can I make RHEL 6 or RHEL 7 FIPS 140-2 compliant
- **RHEL 8:** RHEL 8 is designed for FIPS 140-2 requirements
- **RHEL 9:** Switching RHEL to FIPS mode
- **RHEL 10:** Switching RHEL to FIPS mode
- **Amazon Linux 2:** Enabling FIPS mode in Amazon Linux 2
- **Amazon Linux 2023:** Enabling FIPS mode in Amazon Linux 2023
- **SUSE Linux Enterprise Server 12:** Enabling FIPS mode in SUSE Linux Enterprise Server 12
- **SUSE Linux Enterprise Server 15:** Enabling FIPS mode in SUSE Linux Enterprise Server 15
- **Oracle Linux 8:** Oracle Linux 8 - Enhancing System Security
- **Oracle Linux 10:** Oracle Linux 10 - Enhancing System Security
- **Rocky Linux 9:** Configure a FIPS-compliant Linux Machine
- **Rocky Linux 10:** Configure a FIPS-compliant Linux Machine
- **Miracle Linux 8:** Installing the system in FIPS mode using the RHEL 8 documentation

- **Miracle Linux 9:** Installing the system in FIPS mode using the RHEL 9 documentation
- **Debian Linux 10:** Enabling FIPS mode in Debian
- **Debian Linux 11:** Enabling FIPS mode in Debian
- **Debian Linux 13:** Enabling FIPS mode in Debian

# Enable FIPS mode for the Deep Security Agent on the computers you are protecting

Note that the following information is not applicable to Deep Security 11.0 and later agents which you install after enabling FIPS mode in Deep Security Manager. In these versions, FIPS mode is already enabled for the agent.

## Enable FIPS mode for a Windows agent

1. In the Windows system root folder (for example, `C:\Windows`), look for a file named `ds_agent.ini`. Open the existing file in a text editor or create a new file.
2. Add the following line to the file:
   ```
   FIPSMode=1
   ```
3. Restart the Deep Security Agent service.

## Enable FIPS mode for Linux agents

The following Linux agents are supported: RHEL 7, RHEL 8, RHEL 9, RHEL 10, CentOS 7, Amazon Linux 2, Amazon Linux 2023, Ubuntu 18, Ubuntu 20, SUSE Linux 12, SUSE Linux 15, Oracle Linux 8, Oracle Linux 10, Rocky Linux 9, Rocky Linux 10, Miracle Linux 8, Miracle Linux 9, Debian Linux 10, Debian Linux 11, Debian Linux 13.

1. In `/etc/`, look for a file named `ds_agent.conf`. Open the file in a text editor or create a new file if you do not have one already.
2. Add the following line to the file:
   ```
   FIPSMode=1
   ```
3. Restart the Deep Security Agent:

   Using a SysV init script: `/etc/init.d/ds_agent restart`

   Using a systemd command: `systemctl restart ds_agent`

For more information about enabling FIPS mode on Ubuntu 18 or Ubuntu 20, see FIPS for Ubuntu.

## Use FIPS mode with a PostgreSQL database

If you are using PostgreSQL as your Deep Security Manager database, there is a number of requirements in addition to those outlined in "Database requirements" on page 501.

In FIPS mode, the keystore must be the BCFKS type. Instead of converting the Java default keystore (`C:\Program Files\Trend Micro\Deep Security Manager\jre\lib\security\cacerts` or `/opt/dsm/jre/lib/security/cacerts`) directly, copy the default keystore to another location and use it as the default keystore for SSL connection:

1. Create the PostgreSQL environment.
2. Copy the `server.crt` file from the PostgreSQL server and paste them into `<Deep_Security_Manager_install_folder>`.
3. Install Deep Security Manager.
4. "Enable FIPS mode for your Deep Security Manager" on page 1642.
5. Copy the default Java cacerts file into the Deep Security Manager root installation folder:

   On Windows:

   ```
   copy "C:\Program Files\Trend Micro\Deep Security
   Manager\jre\lib\security\cacerts" "C:\Program Files\Trend Micro\Deep
   Security Manager\cacerts"
   ```

   On Linux:

   ```
   cp "/opt/dsm/jre/lib/security/cacerts" "/opt/dsm/cacerts"
   ```

6. Convert the keystore file from JKS to BCFKS. The following command creates a `cacerts.bcfks` file in the Deep Security Manager installation folder:

   On Windows:

   ```
   cd C:\Program Files\Trend Micro\Deep Security Manager\jre\scripts
   ```

   ```
   keytool_fips.cmd -importkeystore -srckeystore "C:\Program Files\Trend
   Micro\Deep Security Manager\cacerts" -srcstoretype JKS -deststoretype
   BCFKS -destkeystore "C:\Program Files\Trend Micro\Deep Security
   Manager\cacerts.bcfks" -srcstorepass <changeit> -deststorepass
   <changeit>
   ```

where `<changeit>` is replaced with your own values.

On Linux:

```
cd /opt/dsm/jre/scripts
```

```
keytool_fips.sh -importkeystore -srckeystore "/opt/dsm/cacerts" -
srcstoretype JKS -deststoretype BCFKS -destkeystore
"/opt/dsm/cacerts.bcfks" -srcstorepass <changeit> -deststorepass
<changeit>
```

where `<changeit>` is replaced with your own values.

7. Import the certificate "`Deep_Security_Manager_root_folder/server.crt`":

   On Windows:

   ```
   cd C:\Program Files\Trend Micro\Deep Security Manager\jre\scripts
   ```

   ```
   keytool_fips.cmd -import -alias psql -file "C:\Program Files\Trend
   Micro\Deep Security Manager\server.crt" -keystore "C:\Program
   Files\Trend Micro\Deep Security Manager\cacerts.bcfks" -storepass
   <changeit> -storetype BCFKS
   ```

   where `<changeit>` is replaced with your own value.

   On Linux:

   ```
   cd /opt/dsm/jre/scripts
   ```

   ```
   keytool_fips.sh -import -alias psql -file "/opt/dsm/server.crt" -
   keystore "/opt/dsm/cacerts.bcfks" -storepass <changeit> -storetype
   BCFKS
   ```

   where `<changeit>` is replaced with your own value.

8. The Deep Security installer must use a `.vmoptions` file to assign the JVM parameter:

   On Windows, create a file named `Deep Security Manager.vmoptions` in the installation folder and add the following text in the file:

   ```
   -Djavax.net.ssl.keyStoreProvider=BCFIPS
   ```

   ```
   -Djavax.net.ssl.trustStore=C:\Program Files\Trend Micro\Deep Security
   Manager\cacerts.bcfks
   ```

```
-Djavax.net.ssl.trustStorePassword=<changeit>
```

```
-Djavax.net.ssl.keyStoreType=BCFKS
```

```
-Djavax.net.ssl.trustStoreType=BCFKS
```

where `<changeit>` is replaced with your own value.

On Linux, create a file named `dsm_s.vmoptions` in the installation folder and add the following text in the file:

```
-Djavax.net.ssl.keyStoreProvider=BCFIPS
```

```
-Djavax.net.ssl.trustStore=/opt/dsm/cacerts.bcfks
```

```
-Djavax.net.ssl.trustStorePassword=<changeit>
```

```
-Djavax.net.ssl.keyStoreType=BCFKS
```

```
-Djavax.net.ssl.trustStoreType=BCFKS
```

where `<changeit>` is replaced with your own value.

9. Open the `<Deep Security Manager directory>\webclient\webapps\ROOT\WEB-INF\dsm.properties` file in a text editor and add:

   On Windows:

   ```
   database.PostgreSQL.connectionParameters=sslmode=verify-
   ca&sslcert=C\:\\Program Files\\Trend Micro\\Deep Security
   Manager\\server.crt
   ```

   On Linux:

   ```
   database.PostgreSQL.connectionParameters=sslmode=verify-
   ca&sslcert=/opt/dsm/server.crt
   ```

10. Open the `/opt/postgresql/data/postgresql.conf` file in a text editor and add the following:

    ```
    ssl= on
    ```

    ```
    ssl_cert_file= 'server.crt'
    ```

    ```
    ssl_ksy_file= 'server.key'
    ```

11. Restart PostgreSQL, and then restart the Deep Security Manager service.

12. Check the connection, as follows:

    ```
    cd /opt/postgresql/bin
    ```

    ```
    ./psql -h 127.0.0.1 -Udsm dsm
    ```

    Enter the password when prompted. You should see the following:

    ```
    dsm=> select a.client_addr, a.application_name, a.usename, s.* from pg_
    stat_ssl s join pg_stat_activity a using (pid) where a.datname='dsm';
    ```

## Using FIPS mode with a Microsoft SQL Server database

If you are using Microsoft SQL Server as your Deep Security Manager database, you must set up the database SSL encryption using the following instructions before enabling FIPS mode:

1. Stop the Deep Security Manager service.
2. Create a BCFKS keystore file with the SQL server certificate. You can use the `keytool_fips.cmd` in `C:\Program Files\Trend Micro\Deep Security Manager\jre\scripts`.
3. Use the following command to import the SQL server certificate `C:\sqlserver_cert.cer` to a new keystore file `C:\Program Files\Trend Micro\Deep Security Manager\mssql_keystore.bcfks`:

    ```
    keytool_fips.cmd -import -alias mssql -file "C:\sqlserver_cert.cer" -
    keystore "C:\Program Files\Trend Micro\Deep Security Manager\mssql_
    keystore.bcfks" -storepass <changeit> -storetype BCFKS
    ```

    where *`<changeit>`* is replaced with your own value.

    Both `keytool_fips.cmd` and `keytool_fips.sh` files are only available in DSM 20.0.970 or later version. If these files are not included in your DSM installation, contact Trend Micro support.

    During the import process, answer YES to trust this certificate.

4. If the keystore file is created successfully, you can use the following command to see the certificate listed in the keystore:

    ```
    keytool_fips.cmd -list -v -keystore "C:\Program Files\Trend Micro\Deep
    Security Manager\mssql_keystore.bcfks" -storetype BCFKS -storepass
    <changeit>
    ```

    where *`<changeit>`* is replaced with your own value.

5. Open the `C:\Program Files\Trend Micro\Deep Security Manager\webclient\webapps\ROOT\WEB-INF\dsm.properties` file in a text editor and add the following lines enable SSL/TLS and FIPS settings:

   ```
   database.SqlServer.encrypt=true
   ```

   ```
   database.SqlServer.trustServerCertificate=false
   ```

   ```
   database.SqlServer.fips=true
   ```

   ```
   database.SqlServer.trustStorePassword=<changeit>
   ```

   ```
   database.SqlServer.fipsProvider=BCFIPS
   ```

   ```
   database.SqlServer.trustStoreType=BCFKS
   ```

   ```
   database.SqlServer.trustStore=C\:\\Program Files\\Trend Micro\\Deep
   Security Manager\\mssql_keystore.bcfks
   ```

   where `<changeit>` is replaced with your own value.

6. Optionally, you can change the SQL server and client connection protocols from Named Pipes to TCP/IP. This allows for FIPS support:
   a. In the SQL Server Configuration Manager, go to **SQL Network Configuration > Protocols for MSSQLSERVER** and enable **TCP/IP**.
   b. Go to **SQL Native Client 11.0 Configuration > Client Protocols** and enable **TCP/IP**.
   c. Follow the instruction provided by Microsoft to enable encrypted connections for an instance of the SQL Server database. See Enable Encrypted Connections to the Database Engine.
   d. Edit the `dsm.properties` file to change `database.sqldserver. driver=MSJDBC` and `database.SqlServer.namedPipe=false`.
7. Restart the Deep Security Manager service.
8. "Enable FIPS mode for your Deep Security Manager" on page 1642.

## Disable FIPS mode

1. To disable FIPS mode for Deep Security Manager, follow the instructions that you used to enable it (see "Enable FIPS mode for your Deep Security Manager" on page 1642), but use the following command instead of step 3:

   ```
   dsm_c -action disablefipsmode
   ```

2. To disable FIPS mode for Deep Security Agent, follow the instructions that you used to enable it (see "Enable FIPS mode for the Deep Security Agent on the computers you are protecting" on page 1644), but instead of `FIPSMode=1`, use `FIPSMode=0`.

# Bypass vulnerability management scan traffic in Deep Security

If you are using a vulnerability management provider such as Qualys or Nessus (for PCI compliance, for example), you need to set up Deep Security to bypass or allow this provider’s scan traffic through untouched.

- "Create a new IP list from the vulnerability scan provider IP range or addresses" below
- "Create firewall rules for incoming and outbound scan traffic" on the next page
- "Assign the new firewall rules to a policy to bypass vulnerability scans" on page 1652

After these firewall rules have been assigned to the new policy, the Deep Security Manager will ignore ANY traffic from the IPs you have added in your IP List.

Deep Security will not scan the vulnerability management provider traffic for stateful issues or vulnerabilities - it will be allowed through untouched.

## Create a new IP list from the vulnerability scan provider IP range or addresses

Have handy the IP addresses that the vulnerability scan provider has given you.

1. In the Deep Security Manager, go to **Policies**.
2. In the left pane, expand **Lists** > **IP Lists**.
3. Click **New** > **New IP List**.
4. Type a **Name** for the new IP List, for example "Qualys IP list".
5. Paste the IP addresses that the vulnerability management provider has given you into the **IP(s)** box, one per line.
6. Click **OK**.

## Create firewall rules for incoming and outbound scan traffic

After you’ve created the IP list, you need to create two firewall rules: one for incoming and one for outgoing traffic.

Name them as suggested, below:

```
<name of provider> Vulnerability Traffic - Incoming

<name of provider> Vulnerability Traffic - Outgoing
```

1. In the main menu, click **Policies**.
2. In the left pane, expand **Rules**.
3. Click **Firewall Rules** > **New** > **New Firewall Rule**.
4. Create the first rule to bypass Inbound AND Outbound for TCP and UDP connections that are incoming to and outgoing from vulnerability management provider.

   *Tip: For settings not specified, you can leave them as the default.*

   **Name**: (suggested) <name of provider> Vulnerability Traffic - Incoming

   **Action**: Bypass

   **Protocol**: Any

   **Packet Source**: IP List and then select the new IP list created above.

5. Create a second rule:

   **Name:** <name of provider> Vulnerability Traffic - Outgoing

   **Action:** Bypass

   **Protocol:** Any

   **Packet Destination**: IP List and then select the new IP list created above.

**Note:** For firewall rules to work for a computer, the firewall **Configuration** must be set to "On" or "Inherited (On)" (**Computers > Firewall > General**). For firewall rules to work through a policy, the **Firewall State** must be set to "On" (**Policies > Firewall > General**).

## Assign the new firewall rules to a policy to bypass vulnerability scans

Identify which policies are already used by computers that will be scanned by the vulnerability management provider.

Edit the policies individually to assign the rules in the firewall module.

1. Click **Policies** on the main menu.
2. Click **Policies** in the left pane.
3. In the right pane, for each policy, double-click to open the policy details.
4. In the pop-up, in the left pane, click **Firewall**.
5. Under **Assigned Firewall Rules**, click **Assign/Unassign**.
6. Ensure your view at the top-left shows **All** firewall rules in the .
7. Use the search window to find the rules you created and select them.
8. Click **OK**.

# Use TLS 1.2 with Deep Security

In Deep Security Manager 11.1 and higher, TLS 1.2 is enforced by default for new installations.

Review the table below to determine whether you need to take action.

**Note:** If you want to enable TLS 1.2 with only strong, A+-rated, cipher suites, see instead "Enable TLS 1.2 strong cipher suites" on page 1665. Use of strong cipher suites may cause compatibility issues.

| If you are doing... | And your deployment includes... | Do this... |
|---|---|---|
| A new installation of Deep Security Manager 11.1 or higher | Only 10.0 and higher Deep Security Agents, Relays, and | Nothing.<br>By default, TLS 1.2 is used between all components and enforced on the manager and relays. |

| If you are doing... | And your deployment includes... | Do this... |
|---|---|---|
| | Virtual Appliances | |
| | Pre-9.6 Deep Security Agents, Relays, or Virtual Appliances | (Recommended.) Upgrade all of your components to 9.6 or higher versions which support TLS 1.2. See "Upgrade components to use TLS 1.2" on page 1656. This is the best option to increase the security of your deployment.<br>Alternatively, you can enable early TLS 1.0 to ensure backward compatibility with older components. See "Enable early TLS (1.0)" on page 1662. |
| An upgrade to Deep Security Manager 11.1 or higher | Only 10.0 and higher Deep Security Agents, Relays, or Virtual Appliances | (Recommended.) Enable TLS 1.2 enforcement to increase the security of your deployment. See "Enforce TLS 1.2" on page 1658.<br>Alternatively, you can do nothing. Whatever your TLS settings were in your previous deployment are preserved. If you had enforced TLS 1.2 before, then your enforcement settings are preserved after the upgrade. Conversely, if you had disabled enforcement, then those settings are preserved as well. |
| | Pre-9.6 Deep Security Agents, Relays, or Virtual Appliances | (Recommended.) Although no immediate action is required, you should plan to upgrade older components to 9.6 or higher which support TLS 1.2, and then enforce TLS 1.2. See "Upgrade components to use TLS 1.2" on page 1656 and "Enforce TLS 1.2" on page 1658. This is the best option to increase the security of your deployment.<br>Alternatively, you can do nothing. Whatever your TLS settings were in your previous deployment are preserved. If TLS 1.0 was allowed before, then it will also be allowed after the upgrade. |

Topics on this page:

## TLS 1.2 and Deep Security Agent Compatibility

Deep Security Agents version 10.0 or later installed on any platform communicate with Deep Security Manager over TLS 1.2.

In addition, Deep Security Agents version 9.6 installed on the following platforms communicate with Deep Security Manager over TLS 1.2:

- Windows 2000
- Linux Debian 6
- SuSE 10. Note that the Deep Security Agent 9.6 support extension for this platform expired on 23-May-2021.
- Ubuntu 12.04

TLS 1.2 is also supported on Deep Security Agents version 9.0 on the following platforms:

- AIX. Note that the Deep Security Agent 9.0 support extension for this platform expired on 31-Dec-2020.
- Solaris. Note that the Deep Security Agent 9.0 support extension for this platform expired on 31-Dec-2019.

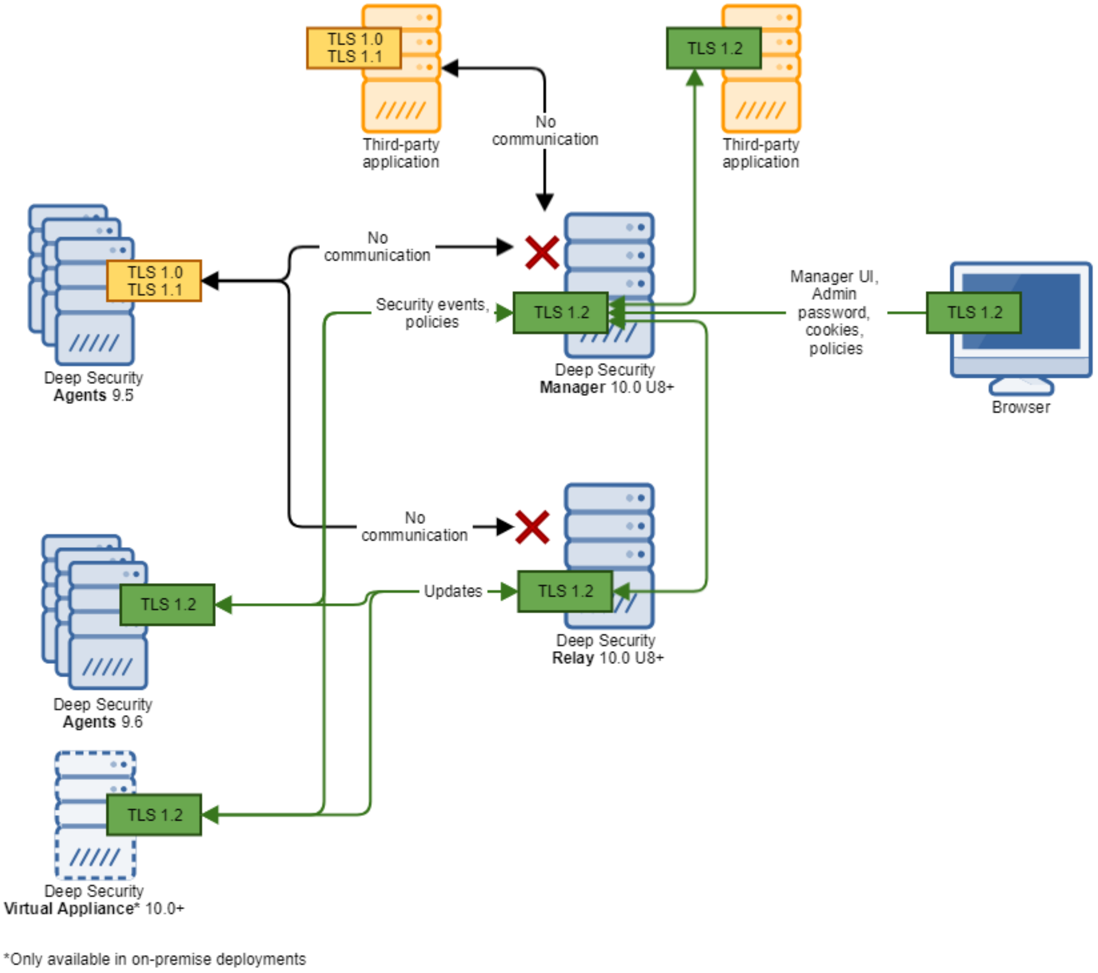
## TLS 1.2 architectures

The diagrams below show the TLS communication in the Deep Security architecture.

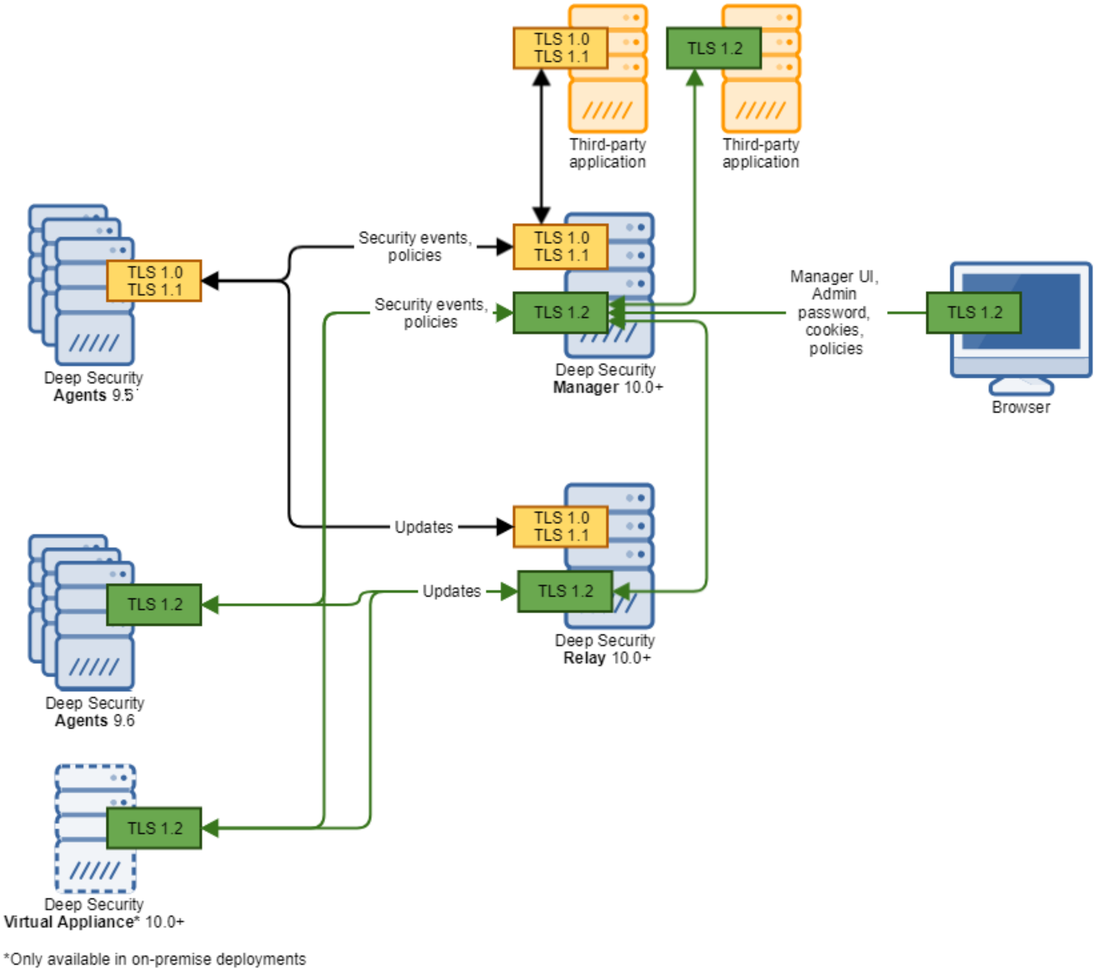
Figure 1 shows the TLS communication when TLS 1.2 *is* enforced (This is the default for new 11.1 or higher Deep Security Manager installations.) You can see that the 9.5 agents can no longer communicate with Deep Security Manager, and neither can older third-party applications.

Figure 2 shows the TLS communication when TLS 1.2 is *not* enforced. You can see that Deep Security Agent 9.6 or later can communicate with Deep Security Manager over TLS 1.2, while 9.5 versions communicate over early TLS. Similarly, newer third-party applications use TLS 1.2, while older ones use early TLS.

### Figure 1: TLS 1.2 is enforced



### Figure 2: TLS 1.2 is *not* enforced


TLS 1.0
TLS 1.1
Third-party application
TLS 1.2
Third-party application
Security events, policies
TLS 1.0
TLS 1.1
Security events, policies
TLS 1.2
Deep Security Manager 10.0+
Manager UI, Admin password, cookies, policies
TLS 1.2
Browser
TLS 1.0
TLS 1.1
Deep Security Agents 9.5
Updates
TLS 1.0
TLS 1.1
Updates
TLS 1.2
Deep Security Relay 10.0+
TLS 1.2
Deep Security Agents 9.6
TLS 1.2
Deep Security Virtual Appliance* 10.0+
*Only available in on-premise deployments

## Upgrade components to use TLS 1.2

If you want your Deep Security components to use TLS 1.2, just make sure that each component supports TLS 1.2.

Follow the instructions below to verify that your Deep Security components support TLS 1.2 and upgrade them if needed.

> **Note:** If you want to *enforce* TLS 1.2 and prevent the use of early TLS, see instead "Enforce TLS 1.2" on page 1658.

## Verify and upgrade your Deep Security Manager

- Make sure you're using one of the following versions of Deep Security Manager, and if not, upgrade it:
  - Use Deep Security Manager 10.0 *update 8* or later if you're planning to "Enforce TLS 1.2" on the next page on the manager. Only 10.0 update 8 and later managers support TLS 1.2 enforcement.
  - Use Deep Security Manager 10.0 or later if you're *not* planning to "Enforce TLS 1.2" on the next page on the manager. Only 10.0 and later managers support TLS 1.2 communication.
- For upgrade instructions, see "Upgrade Deep Security Manager VM for Azure Marketplace" on page 1549.

## Verify your Deep Security Manager database

- If you're using Microsoft SQL Server as your Deep Security Manager database, make sure the database supports TLS 1.2, and if not, upgrade it. See this Microsoft article for guidance.
- If you're using a PostgrSQL database, it supports TLS 1.2 so no action is necessary.
- If you're using an Oracle database, only Oracle's native encryption is supported for database-manager communication, not TLS, so no action is necessary.
- By default, there is no encryption between the database (SQL Server, PostgreSQL, or Oracle) and Deep Security Manager. You can enable it manually.

## Verify your Deep Security Agents

- If you have existing Deep Security Agents, make sure they're at version 10.0 or higher. Only 10.0 or higher agents support TLS 1.2.

**Note:** If some agents are left un-upgraded (that is, they are pre-10.0), those agents communicate over early TLS, and you may need to enable early TLS. For details, see "Enable early TLS (1.0)" on page 1662.

To upgrade your agents, see "Upgrade Deep Security Agent" on page 1542.

## Verify your Deep Security Relays

- Make sure you're using one of the following versions of Deep Security Relay, and if not, upgrade it:
  - Use Deep Security Relay 10.0 *update 8* or later if you're planning to "Enforce TLS 1.2" below on the relay. Only 10.0 update 8 and higher relays support TLS 1.2 enforcement.
  - Use Deep Security Relay 10.0 or later if you're *not* planning to "Enforce TLS 1.2" below on the relay. Only 10.0 and higher relays support TLS 1.2 communication.

  To upgrade a relay, see "Upgrade Deep Security Relay" on page 1541.

# Enforce TLS 1.2

Topics in this section:

- "Where can TLS 1.2 be enforced?" below
- "What happens when TLS 1.2 enforced?" below
- "Is TLS 1.2 enforced by default?" on the next page
- "Under what circumstances is TLS 1.2 enforcement possible? " on the next page
- "Enforce TLS 1.2 on Deep Security Manager" on the next page
- "Enforce TLS 1.2 on the Deep Security Relay" on page 1660
- "Enforce TLS 1.2 on just the manager's GUI port (4119)" on page 1660
- "Test that TLS 1.2 is enforced" on page 1661

## Where can TLS 1.2 be enforced?

There are two enforcement points:

- on the Deep Security Manager
- on the Deep Security Relays

## What happens when TLS 1.2 enforced?

When TLS 1.2 is enforced, the manager and relays stop accepting early TLS connections, and any applications that try to use early TLS are denied access and cease to function properly.

If you choose *not* to enforce TLS 1.2, the manager and relays still accept early TLS as well as TLS 1.2 connections. This means that both older and newer applications are able to connect.

## Is TLS 1.2 enforced by default?

- If you have a new installation of Deep Security Manager 11.1 or higher (not an upgrade), TLS 1.2 is enforced by default.
- If you are upgrading an existing Deep Security Manager to 11.1 or higher, then your existing TLS settings are preserved, so if TLS was not enforced previously, it will continue to not be enforced after the upgrade. Conversely, if it was enforced, it will continue to be enforced.

## Under what circumstances is TLS 1.2 enforcement possible?

You can only enforce TLS 1.2 if *all* Deep Security Agents have been upgraded to 10.0 or higher, which is the version at which TLS 1.2 is supported.

## Enforce TLS 1.2 on Deep Security Manager

1. Before you begin:
   - Make sure that Deep Security Manager is at version *10.0 Update 8* or higher. You need this version to enforce TLS 1.2.
   - Make sure that all other components support TLS 1.2. See "Upgrade components to use TLS 1.2" on page 1656.
2. On the Deep Security Manager computer, run this dsm_c command:

   ```
   dsm_c -action settlsprotocol -MinimumTLSProtocol ShowValue
   ```

   A TLS version appears. This is the minimum TLS version that Deep Security Manager currently accepts.

3. Run this `dsm_c` command:

   ```
   dsm_c -action settlsprotocol -MinimumTLSProtocol TLSv1.2
   ```

   This command sets the minimum TLS version to 1.2. Deep Security Manager now accepts TLS 1.2 connections and disallows TLS 1.0 connections.

   The Deep Security Manager service is restarted automatically.

## Enforce TLS 1.2 on the Deep Security Relay

1. Before you begin:
   - Make sure that Deep Security Relay is at version *10.0 Update 8* or higher. You need this version to enforce TLS 1.2.
   - Make sure that all your components support TLS 1.2. See "Upgrade components to use TLS 1.2" on page 1656.
   - Make sure that you have enforced TLS 1.2 on Deep Security Manager.
2. Resend the policies associated with your relays:
   a. In Deep Security Manager, click **Computers** and find one of your relays in the list of computers. If you're not sure which ones are your relays, at the top, click **Administration**. On the left, expand **Updates** and then click **Relay Management**. In the main pane, expand a relay group to see your relays.
   b. Double-click the relay in the list of computers.
   c. In the main pane, click the **Actions** tab.
   d. Click **Send Policy** to resend the policy.
   e. Resend the policy to each of your relays.

## Enforce TLS 1.2 on just the manager's GUI port (4119)

Only read this section if you were unable to do a full enforcement on the Deep Security Manager and Relays as described previously in "Enforce TLS 1.2 on Deep Security Manager" on the previous page and "Enforce TLS 1.2 on the Deep Security Relay" above.

This section describes how to set the minimum TLS version to TLS 1.2 on port 4119. Applications that connect on port 4119 are typically web browsers and Deep Security API clients. Older Deep Security components that do not support TLS 1.2 can continue to connect to the manager (on port 4120, by default) using TLS 1.0.

1. On Deep Security Manager, enable TLS 1.0 by running this dsm_c command:

   ```
   dsm_c -action settlsprotocol -MinimumTLSProtocol TLSv1
   ```

   Deep Security Manager now accepts TLS 1.0 connections from older agents and applications.

2. Disable early TLS on the manager's GUI port (4119) (it is possible that it's already disabled):
   a. Open the `configuration.properties` file in the root of the Deep Security Manager installation directory.

   b. Under `serviceName=`, look for the `protocols=` setting.

      This setting defines the protocols that can be used to connect to Deep Security Manager when it is acting as a server to web browsers and Deep Security API clients.

   c. If the `protocols=` setting is present, remove it so that only TLS 1.2 is allowed on port 4119.
   d. Save the file.
3. Restart the Deep Security Manager service.

## Test that TLS 1.2 is enforced

1. On a Deep Security component where early TLS 1.2 is enforced, run the following nmap command:

   `nmap --script ssl-enum-ciphers <ds_host> -p <ds_port> -Pn`

   where:
   - `<ds_host>` is replaced with the IP address or hostname of the manager or relay
   - `<ds_port>` is replaced with the listening port where TLS is being used (4119 for manager, 4122 for the relay, and 4118 for the agent–if manager-initiated activation is used)

   The response should only list TLS 1.2. Example response:

```
PORT STATE SERVICE
443/tcp open https
| ssl-enum-ciphers:
| | TLSv1.2:
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
| TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
| TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
| TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
| TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
| TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
| TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
| TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
| compressors:
```

# Enable early TLS (1.0)

By default, early TLS (1.0) is disabled. You'll need to enable it if you have a *new* installation of Deep Security Manager 11.1 or higher (not an upgrade) and:

- you are using pre-10.0 agents. These only support early TLS. Go here to see if a 10.0 or higher agent is available for your OSs.
- you are using third-party components that are older and need to use early TLS to communicate with Deep Security Manager.
- you are using a pre-10.0 version of the Deep Security Virtual Appliance (which is no longer supported).

To enable early TLS (1.0), follow the instructions below.

## Enable TLS 1.0 on Deep Security Manager and the Deep Security Relay

1. On the Deep Security Manager computer, run this dsm_c command:

   ```
   dsm_c -action settlsprotocol -MinimumTLSProtocol ShowValue
   ```

   A TLS version appears. This is the minimum TLS version that Deep Security Manager currently accepts.

2. Run this `dsm_c` command:

   ```
   dsm_c -action settlsprotocol -MinimumTLSProtocol TLSv1
   ```

   This command sets the minimum TLS version to 1.0.

   TLS 1.0 is now re-enabled on your Deep Security Manager.

The Deep Security Manager service is restarted automatically.

3. Resend the policies associated with your relays:
   a. In Deep Security Manager, click **Computers** and find one of your relays in the list of computers. If you're not sure which ones are your relays, at the top, click **Administration**On the left, expand **Updates** and then click **Relay Management**. In the main pane, expand a relay group to see your relays.
   b. Double-click the relay in the list of computers.
   c. In the main pane, click the **Actions** tab.
   d. Click **Send Policy** to resend the policy.
   e. Resend the policy to each of your relays.

   TLS 1.0 is now re-enabled on your relays.

## Enable TLS 1.0 on the manager's GUI port (4119)

Read this section if you previously enforced TLS 1.2 only on the manager's GUI port (4119) and now want to re-enable early TLS 1.0 on this port.

1. Follow the instructions in "Enable TLS 1.0 on Deep Security Manager and the Deep Security Relay" on the previous page. This re-enables TLS 1.0 on the GUI port (4119).

## Enable TLS 1.0 in deployment scripts

Deep Security Agents and Deep Security Relays can be deployed using deployment scripts. You may need to modify these scripts as follows:

1. If you are deploying onto Windows XP, 2003, or 2008, remove these lines from the deployment script:

   ```
   #requires -version 4.0
   ```

   ```
   [Net.ServicePointManager]::SecurityProtocol =
   [Net.SecurityProtocolType]::Tls12;
   ```

   Windows XP, 2003, and 2008 do not support PowerShell 4.0, which is required for TLS 1.2.

2. If you are deploying onto Red Hat Enterprise Linux 6, remove this tag from the deployment script:

   `--tls1.2`

   Red Hat Enterprise Linux 6 uses curl 7.19 by default which does not support TLS 1.2.

3. If you are deploying onto any other supported operating system, leave the deployment scripts as they are.

# Determine whether TLS 1.2 is enforced

If you're not sure whether TLS 1.2 is enforced on Deep Security Manager, follow the instructions below to find out.

1. On the Deep Security Manager computer, open a command prompt and run the following dsm_c command:

   ```
   dsm_c -action settlsprotocol -MinimumTLSProtocol ShowValue
   ```

   The minimum TLS protocol accepted by the manager is displayed. If it shows TLS 1.2, then TLS 1.2 is enforced. If it shows TLS 1.0, then early TLS is allowed and TLS 1.2 is not enforced.

Determining whether TLS 1.2 is enforced on the relay is harder. If you pushed out your TLS settings to the relay through policy according to "Enforce TLS 1.2 on the Deep Security Relay" on page 1660 or "Enable TLS 1.0 on Deep Security Manager and the Deep Security Relay" on page 1662, then those TLS settings apply to the relay. If you did not push out TLS settings through policy, then the relay's default TLS settings apply. The relay's default settings depend on its version: if you're using an 11.1 or higher relay, then TLS 1.2 is enforced by default. For pre-11.1 relays, TLS 1.2 is not enforced by default.

# Guidelines for deploying agents, and relays after TLS 1.2 is enforced

This section discusses special considerations when deploying agents and relays when TLS 1.2 is enforced. If you enabled early TLS (1.0), then there are no special considerations, and you do not need to read this section.

Topics in this section:

## Guidelines for deploying agents, and relays when TLS 1.2 is enforced

- You must deploy 10.0 or higher agents, and relays. Only 10.0 or higher agents and relays support TLS 1.2.
- If you need to deploy a 9.6 or earlier agent or relay you must enable early TLS (1.0).

## Guidelines for using deployment scripts when TLS 1.2 is enforced

If TLS 1.2 is enforced, you can install 10.0 or higher agents and relays using deployment scripts. Below are some guidelines to ensure the deployment scripts work:

1. If you are deploying an agent or relay onto Windows computers, use PowerShell 4.0 or higher, which supports TLS 1.2.
2. If you are deploying an agent or relay onto Linux, use curl 7.34.0 or higher, which supports TLS 1.2.
3. If you are deploying onto Windows XP, 2003, or 2008

   OR

   If you are deploying onto Red Hat Enterprise Linux 6

   ...these OSs don't support TLS 1.2 and you must "Enable early TLS (1.0)" on page 1662 and modify your deployment scripts.

# Enable TLS 1.2 strong cipher suites

Enabling strong cipher suites allows you to be certain that all of the communications to and from your Deep Security components are secure. If a malicious user were to create a connection to your system over a communications channel that uses weak cipher suites, this person could exploit the known weaknesses in these suites to put your system and information at risk.

This page describes how to update the Deep Security Manager, Deep Security Agent and Deep Security Relay so that they use the TLS 1.2 strong cipher suites. These cipher suites have an Advanced+ (A+) rating, and are listed in the table on this page.

Step 1: "Check your environment" on the next page

Step 2: "Update Deep Security components" on the next page

Step 3: "Run a script to enable TLS 1.2 strong cipher suites" on the next page

Step 4: "Verify that the script worked" on page 1667

"Disable TLS 1.2 strong cipher suites" on page 1670

## Check your environment

There are some circumstances where you should not enable strong cipher suites and should use TLS 1.2 with Deep Security instead:

- If you are using FIPS mode.
- If any of the computers in your environment are running Windows Server 2012 R2 or earlier, which doesn't support strong cipher suites. Consider upgrading those computers to Windows Server 2016, which does support strong cipher suites.
- If you can't upgrade all of your Deep Security components to 12.0 or later. For example, if you're using operating systems for which a 12.0 agent is not available.

## Update Deep Security components

Make sure you update all components in the following order; otherwise the agents cannot communicate with the relays and manager:

1. Update all your manager instances to 12.0 or a later update. For upgrade instructions, "Upgrade Deep Security Manager VM for Azure Marketplace" on page 1549.
2. Update all your relays to 12.0 or later. To upgrade a relay, follow the same process as upgrading an agent:
   a. Import the latest relay software into the manager, either manually or automatically. See "Import agent software" on page 522 for details.
   b. Upgrade the relay. See "Upgrade Deep Security Relay" on page 1541.
3. Update all your agents to 12.0 or later. To upgrade your agents:
   a. Import the latest agent software into the manager, either manually or automatically. See "Import agent software" on page 522 for details.
   b. Upgrade your Deep Security Agents. See "Upgrade Deep Security Agent" on page 1542.

## Run a script to enable TLS 1.2 strong cipher suites

1. Copy the `EnableStrongCiphers12.script` file available at https://github.com/deep-security/ops-tools/tree/master/deepsecurity/manager to:
   - On Windows: `<Manager_root>\Scripts`
   - On Linux: `<Manager_root>/Scripts`

where `<Manager_root>` is replaced with the path to your manager's installation directory, by default:

- `C:\Program Files\Trend Micro\Deep Security Manager` (Windows)
- `/opt/dsm/` (Linux)

> **Note:** If you do not see a `\Scripts` directory, create it.

2. Log in to the manager.
3. Click **Administration** at the top.
4. On the left, click **Scheduled Tasks**.
5. In the main pane, click **New**.
6. The **New Scheduled Task Wizard** appears.
7. From the **Type** drop-down list, select **Run Script**. Select **Once Only**. Click **Next**.
8. Accept the date, time, and time zone defaults, and then click **Next**.
9. For the **Script**, select **EnableStrongCiphers.script**. Click **Next**.
10. For the **Name**, enter a name for the script, for example, `Enable Strong Cipher Suites`. Make sure **Task Enabled** is selected. Click **Run Task on 'Finish'**. Click **Finish**.

    The script runs.

11. Restart the Deep Security Manager service.

    Your agents, relays, and manager should now be communicating with each other using TLS 1.2 strong cipher suites exclusively.

# Verify that the script worked

To verify that the script worked, and that only strong TLS 1.2 cipher suites are permitted, you must run a series of nmap commands.

- "Verify the manager using nmap" below
- "Verify the relays using nmap" on the next page
- "Verify the agents using nmap" on page 1669

## Verify the manager using nmap

Run the following command:

```
nmap --script ssl-enum-ciphers -p 4119 <Manager_FQDN>
```

The output should look similar to the following, with the strong cipher suites near the middle:

```
Starting Nmap 7.01 ( https://nmap.org ) at 2018-11-14 09:51 EST
Nmap scan report for <DSM FQDN> (X.X.X.X)
Host is up (0.0049s latency).
PORT STATE SERVICE
4119/tcp open assuria-slm
| ssl-enum-ciphers:
| TLSv1.2:
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256k1) - A
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256k1) - A
| compressors:
| NULL
| cipher preference: client
|_ least strength: A
Nmap done: 1 IP address (1 host up) scanned in 6.82 seconds
```

## Verify the relays using nmap

Run the following command:

`nmap --script ssl-enum-ciphers -p 4122 <Relay_FQDN>`

The output should look similar to the following, again, with the strong cipher suites listed near the middle:

```
Starting Nmap 7.01 ( https://nmap.org ) at 2018-11-14 09:49 EST
Nmap scan report for <DSR FQDN> (X.X.X.X)
Host is up (0.0045s latency).
PORT STATE SERVICE
4122/tcp open unknown
| ssl-enum-ciphers:
| TLSv1.2:
```

```
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
| compressors:
| NULL
| cipher preference: server
|_ least strength: A
Nmap done: 1 IP address (1 host up) scanned in 31.02 seconds
```

## Verify the agents using nmap

Run the following command:

```
nmap --script ssl-enum-ciphers -p 4118 <Agent_FQDN>
```

The output looks similar to the following:

```
Starting Nmap 7.01 ( https://nmap.org ) at 2018-11-14 09:50 EST
Nmap scan report for <DSA FQDN> (X.X.X.X)
Host is up (0.0048s latency).
PORT STATE SERVICE
4118/tcp open netscript
| ssl-enum-ciphers:
| TLSv1.2:
| ciphers:
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
| compressors:
| NULL
| cipher preference: server
|_ least strength: A
```

```
Nmap done: 1 IP address (1 host up) scanned in 2.72 seconds
```

# Disable TLS 1.2 strong cipher suites

If you mistakenly run the script before upgrading all of your agents, relays, or the manager, you can revert this action by doing the following:

1. Open the `configuration.properties` file in `<Manager_root>`, and remove the line starting with `ciphers`. The line looks similar to the following:

   ```
   ciphers=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_
   128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_
   WITH_AES_128_CBC_SHA256
   ```

2. Add the following values to the `protocols` field: `TLSv1` and `TLSv1.1`. Your final property looks similar to this:

   ```
   protocols = TLSv1, TLSv1.1, TLSv1.2
   ```

3. Save and close the file.
4. Open the `java.security` file in `<Manager_root>\jre\lib\security\` and remove the following two protocols from `jdk.tls.disabledAlgorithms`:

   ```
   TLSv1, TLSv1.1
   ```

5. On Deep Security Manager, run the following `dsm_c` commands:

   ```
   dsm_c -action changesetting -name
   settings.configuration.restrictRelayMinimumTLSProtocol -value TLSv1
   ```

   ```
   dsm_c -action changesetting -name
   settings.configuration.enableStrongCiphers -value false
   ```

   Your system should now be able to communicate again. If you still need to enable TLS 1.2 strong cipher suites, make sure you have upgraded all components before running the script.

If you continue to experience communication problems with the Deep Security Manager, run the following additional `dsm_c` command:

```
dsm_c -action changesetting -name
settings.configuration.MinimumTLSProtocolNewNode -value TLSv1
```

# Legal disclosures

## Privacy and personal data collection disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that Trend Micro Deep Security collects and provides detailed instructions on how to disable the specific features that feed back the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Policy:

https://www.trendmicro.com/en_us/about/legal/privacy.html

## Deep Security Product Usage Data Collection

Trend Micro collects protected performance and feature usage data to help improve Deep Security Manager. Trend Micro only uses the collected data internally for product improvement; it is not shared with external parties and does not contain any personally identifiable information.

As the data allows Trend Micro to more effectively support Deep Security, we recommend that you leave data collection enabled. However, if you do not want Deep Security Manager to collect this data, you can disable data collection.

To disable data collection, go to **System Settings > Advanced > Product Usage Data Collection** and deselect **Enable Product Usage Data Collection**.

## Legal disclaimer

Below are the legal disclaimers regarding the following releases:

- "Hot Fix" on the next page
- "Major release, Update, Patch or Service Pack" on the next page

### Hot Fix

This hot fix was developed as a workaround or solution to a customer-reported problem. As such, this hot fix has received limited testing and has not been certified as an official product update.

Consequently, THIS HOT FIX IS PROVIDED "AS IS". TREND MICRO MAKES NO WARRANTY OR PROMISE ABOUT THE OPERATION OR PERFORMANCE OF THIS HOT FIX NOR DOES IT WARRANT THAT THIS HOT FIX IS ERROR FREE. TO THE FULLEST EXTENT PERMITTED BY LAW, TREND MICRO DISCLAIMS ALL IMPLIED AND STATUTORY WARRANTIES, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE.

### Major release, Update, Patch or Service Pack

This release was current as of the release date. However, all customers are advised to check Trend Micro's website for documentation updates.

**Tip:** Register online with Trend Micro within 30 days of installation to continue downloading new pattern files and product updates from the Trend Micro website. Register during installation or online at https://clp.trendmicro.com/FullRegistration?T=TM.

# Integrations

## Integrate with AWS Control Tower

Integrate Deep Security with AWS Control Tower to ensure that every account added through Control Tower Account Factory is automatically provisioned in Deep Security, providing centralized visibility to the security posture of EC2 instances deployed in each account as well as the foundation for policy and billing automation.

### Overview

The Lifecycle Hook solution provides a CloudFormation template which, when launched in the Control Tower Master Account, deploys AWS infrastructure to ensure Deep Security monitors each Account Factory AWS account automatically. The solution consists of 2 Lambda functions;

one to manage our role and access Deep Security, and another to manage the lifecycle of the first Lambda. AWS Secrets Manager is leveraged to store the API key for Deep Security in the Master account and a CloudWatch Events rule is configured to trigger the customization Lambda when a Control Tower account is successfully deployed.

Once Deep Security is integrated with AWS Control Tower, it will be implemented in the following way:

1. During stack launch, the lifecycle Lambda is executed for each existing Control Tower Account, including the Control Tower Master, Audit, and Log accounts.
2. After launch, a CloudWatch Event rule triggers the lifecycle Lambda for each successful Control Tower CreateManagedAccount event.
3. The lifecycle Lambda function retrieves the Deep Security Api Key from AWS Secrets Manager, then gets the External ID for your organization from the Deep Security API.
4. The Lambda function assumes the ControlTowerExecution role in the target Managed Account in order to create the necessary cross account role and associated policy.
5. A call is made to the Deep Security API to add this Managed Account to your tenant.

## Integrate with AWS Control Tower

1. Deploy Deep Security Manager to the AWS Control Tower designated shared security account. We recommend deploying Deep Security Quickstart into your Control Tower Security account and leveraging a public facing ELB in the quickstart deployment to create connectivity between workloads Managed Accounts and the Deep Security Manager.
2. When the CloudFormation stack has launched successfully, record the DeepSecurityConsole value from the top level CloudFormation template. You will need this URL to sign in to the console and to configure the multi-account integration.
3. In Deep Security Manager, go to **Administration > User Management > API Keys** and click **New**. Select a name for the key and the **Full Access** role. Be sure to save the key as it cannot be retrieved later. This key will be used to authenticate the automation from the AWS Control Tower Master to the console API. For more information, see "Create an API key for a user" on page 1431.
4. Sign in to the AWS Control Tower master account. Navigate to the CloudFormation Service, select the region in which AWS Control Tower was deployed, and launch the lifecycle template.
5. In the lifecycle template, enter your API Key generated in step 3. Next, enter the FQDN of your console (without https://) which was displayed as the DeepSecurityConsole value recorded in step 2.

6. Select the box acknowledging that AWS CloudFormation might create IAM resources. Select **Create Stack**, and the integration will start adding your AWS accounts to Deep Security.
7. Once all your accounts have been imported, "Install the agent" on page 548 and activate protection.

## Upgrade the AWS Control Tower integration

As new capabilities are added to Deep Security, it might be necessary to update the permissions for the application's cross-account role. To update the role deployed by the lifecycle hook, update the Deep Security stack with the latest template, which can be found at its original URL. The parameter values should not be modified from their original values unless directed by Trend Micro Support. Updating the CloudFormation stack will update the role used by all existing accounts and the role created for future enrollments.

## Remove AWS Control Tower integration

To remove the lifecycle hook, identify and delete the CloudFormation stack. Protection for Managed Accounts which have already been added will remain in place. For details on removing an AWS account from Deep Security see, "Remove an AWS account" on page 593.

# Integrate with AWS Systems Manager Distributor

AWS Systems Manager Distributor is a feature integrated with AWS Systems Manager that you can use to securely store and distribute software packages in your accounts. By integrating with AWS Systems Manager Distributor, you can distribute Deep Security Agents across multiple platforms, control access to managed instances, and automate your deployments.

## Create an IAM policy

Follow the instructions in Importing existing managed policies.

In the **Import managed policies** window, add the "AmazonSSMManagedInstanceCore" policy.

## Create a role and assign the policy

Follow the instructions in Creating a role for an AWS service.

In the **Attach permissions policies** window, add the “AmazonSSMManagedInstanceCore” permission.

## Create parameters

1. In your AWS console, navigate to **AWS Systems Manager > Application Management > Parameter Store**.
2. There are 4 parameters that need to be created. Click **Create parameter** and enter the **Name** and **Value** as listed in the table below. The other fields can be left on their default values.

| Name | Value |
|---|---|
| dsActivationUrl | dsm://dsm.company.com:4120/ |
| dsManagerUrl | https://dsm.company.com:443 |
| dsTenantId | For single tenant environments, this parameter is not required. For multi-tenants, on the Deep Security Manager, go to **Support > Deployment Scripts**. Scroll to the bottom of the generated script and copy the *tenantID*. |
| dsToken | For single tenant environments, this parameter is not required. For multi-tenants, on the Deep Security Manager, go to **Support > Deployment Scripts**. Scroll to the bottom of the generated script and copy the *token*. |

**Note:** Make sure the values for dsActivationUrl and dsManagerUrl are entered exactly as they appear, taking care to include the trailing slash where applicable.

## Integrate with AWS Systems Manager Distributor

1. In the AWS console, go to **AWS Systems Manager > Node Management > Distributor**.
2. Select the **TrendMicro-CloudOne-WorkloadSecurity** package, then **Install on a Schedule**.
3. The **Create Association** page opens. Fill in the required fields. For **Installation Type**, we recommend you use the *In-place update* option.
4. Create a schedule. Leveraging a scheduled State Manager Association will ensure agents are always installed and up to date.

## Protect your computers

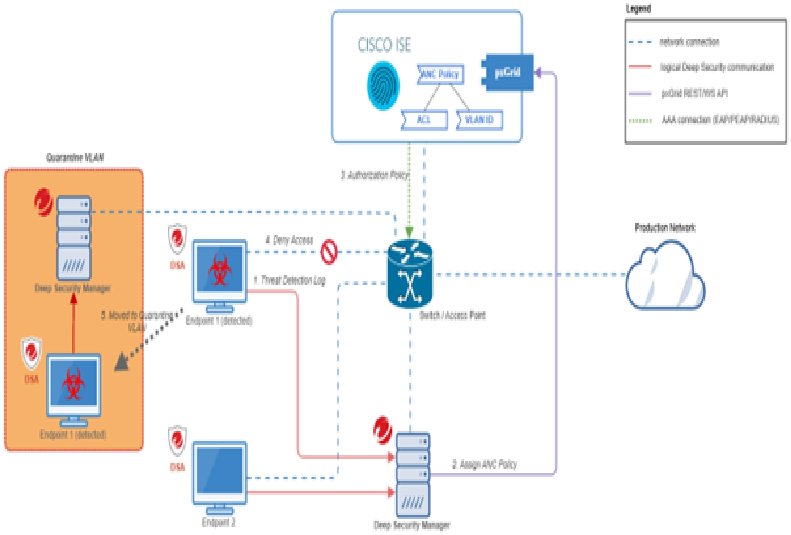
We recommend configuring a cloud connector for each AWS account which will contain managed agents. It might also be necessary to create a policy specific to the systems which will be managed by Distributor.

# Integrate with Cisco Identity Services Engine (ISE)

Cisco Identity Services Engine (ISE) in Deep Security performs network containment by assigning an Adaptive Network Control (ANC) policy to target MAC addresses as soon as a threat is detected on a specific host.

This feature enables the Deep Security Manager to continuously monitor threat detection events, such as those from the Anti-Malware and Intrusion Prevention System protection modules. When detection events meet certain configurable criteria, the manager instructs Cisco ISE to quickly apply the ANC policy to all MAC addresses associated with the host from which the detection events originated. The ANC policy allows Cisco ISE to implement security measures, such as moving the targeted MAC addresses to a quarantine VLAN or shutting down the network device port to which the MAC is connected.

Integration flow is shown in the diagram below.



The integration flow functions as follows:

1. Deep Security Agent sends detection logs to Deep Security Manager.
2. If the detection log meets the configured criteria, such as CVSS score or ransomware malware type, the manager instructs Cisco ISE to apply the Adaptive Network Control (ANC) policy to all MAC addresses associated with the affected endpoint.
3. Cisco ISE applies the network Access Control Lists (ACL) associated with the ANC policy on the underlying network switches that have been configured to use Cisco ISE as the authentication server.

4. The endpoint's network session is reauthenticated by network switch, resulting in denied access.
5. The endpoint may be moved to a quarantine VLAN, where threat diagnosis and remediation are managed by the manager node residing within that VLAN.

**Note:** This article provides guidelines for configuring the Cisco Identity Services Engine (ISE) connection and utilizing its integration with Deep Security. For more information on Cisco ISE, Adaptive Network Control (ANC) policy, and Access Control Lists (ACLs), please refer to the official Cisco ISE documentation.

## Prerequisite Cisco ISE connection configuration

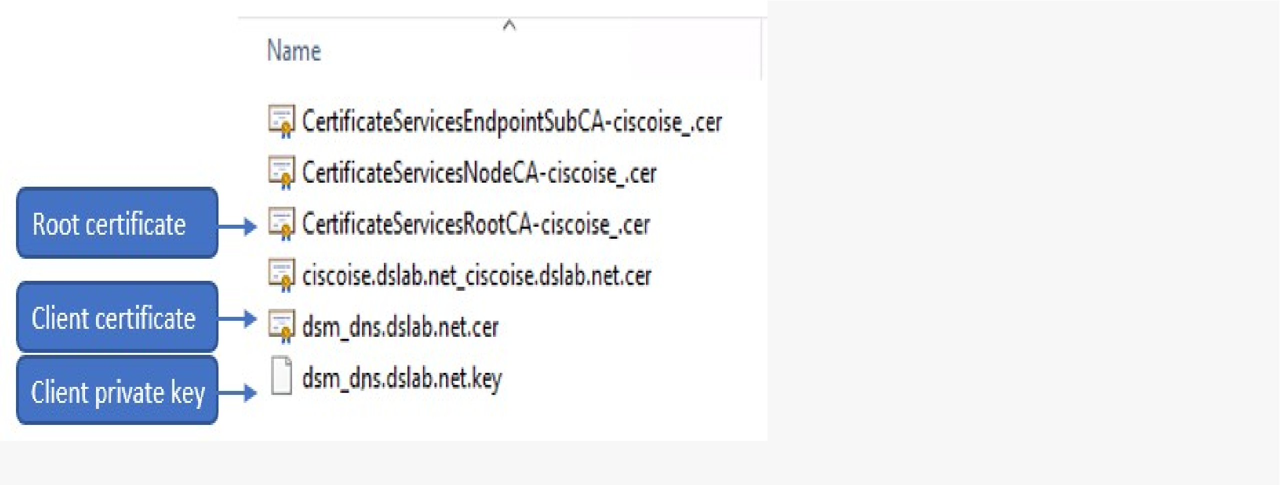
Deep Security Manager connects to Cisco ISE through the Cisco Platform Exchange Grid (pxGrid). pxGrid allows clients to exchange information and communicate via REST API and Websocket. pxGrid ensures secure communication, with only trusted clients gaining access to shared data through controlled pxGrid connections.

Before connecting with Deep Security Manager, the following configurations must be made in the Cisco ISE web console:

1. Go to **Administration** > **pxGrid Services** > **Client Management** > **Certificates**, and click **Create** to generate the pxGrid client certificate, private key, and root certificate in PEM format.
   Your browser will download a ZIP bundle containing the root certificate (files with RootCA in their names), client certificate (files that contain the Common Name specified during pxGrid client certificate creation), and private key.

   **Note:** The ZIP file contains multiple certificates, which use the following naming conventions:
   - Files that include RootCA in their names typically represent the Cisco ISE root certificate for self-signed certificates.
   - Files that contain the Common Name specified during the creation of the pxGrid client certificate generally correspond to the client certificate and the associated client private key.

   The image below shows an example of the files contained within a ZIP bundle.


Name
CertificateServicesEndpointSubCA-ciscoise_.cer
CertificateServicesNodeCA-ciscoise_.cer
CertificateServicesRootCA-ciscoise_.cer
ciscoise.dslab.net_ciscoise.dslab.net.cer
dsm_dns.dslab.net.cer
dsm_dns.dslab.net.key
Root certificate
Client certificate
Client private key

Tip: If Cisco ISE was deployed using a certificate signed by a public Certificate Authority, the root certificate will need to be extracted from the ZIP bundle and submitted when you "Configure the Cisco ISE connection in Deep Security Manager" below.

2. Go to **Operations** > **Adaptive Network Control** > **Policy List** and create or provide an Adaptive Network Control (ANC) policy for use with Deep Security Manager. Make note of the ANC policy name, since you will need it in order to configure the pxGrid connection for Deep Security Manager.
3. Shut down all Deep Security Manager nodes to prevent dangling cache data across manager nodes.
4. Enable fast-path event retrieval via IoT/MQTT to speed up event retrieval to near real-time using the following command:

```
dsm_c -action iotevent -configuration enable -ciscortc
```

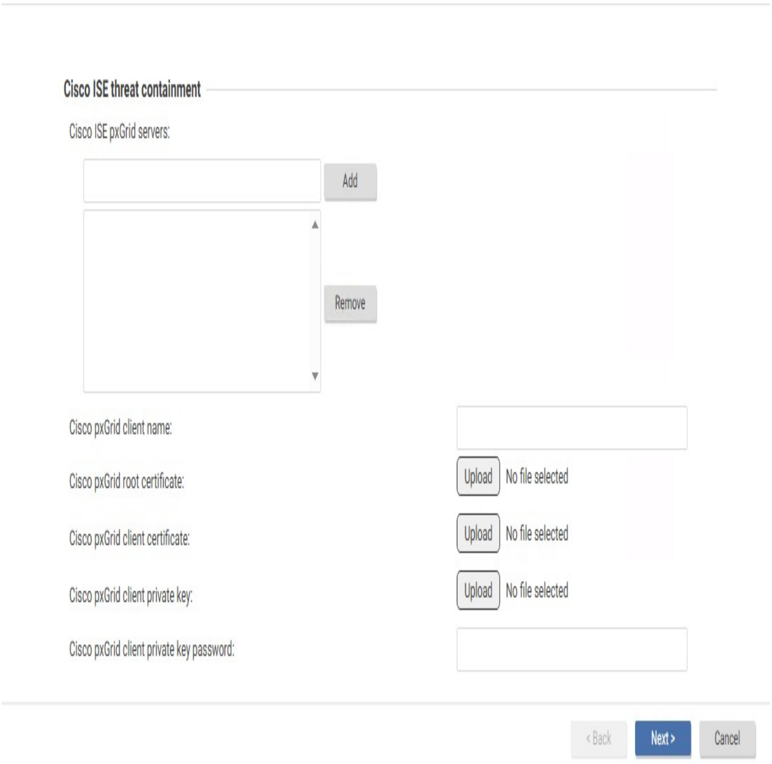
Note: Running this command for one manager will apply the change to all of your manager nodes. This is required in order to provide the near real-time event transmission needed to integrate Cisco ISE with Deep Security Manager.

5. Manually start all manager nodes.

## Configure the Cisco ISE connection in Deep Security Manager

To connect Cisco ISE to Deep Security Manager:

1. Go to **Administration** > **System Settings** > **Cisco Threat Containment**.
2. Select **Enable Cisco Threat Containment** and then click **Configure pxGrid Connection**. The Cisco ISE threat containment window appears.



Cisco ISE threat containment

Cisco ISE pxGrid servers:

Cisco pxGrid client name:

Cisco pxGrid root certificate: No file selected

Cisco pxGrid client certificate: No file selected

Cisco pxGrid client private key: No file selected

Cisco pxGrid client private key password:

3. Add the information and upload the files required for the Cisco pxGrid client. For details, see the following table.

| Field Name | Description |
|---|---|
| Cisco ISE pxGrid servers | Enter the pxGrid server addresses in the format `https://<fqdn>:<port>`. For example, within the URL you may input multiple server addresses; the API invocation will cycle through these addresses using a round-robin mechanism. |
| Cisco pxGrid client name | This is the name used to register the pxGrid client. Once the client registration request has been submitted, this name will appear in the pxGrid client list within the Organization ISE. |
| Cisco pxGrid root certificate | This is the root certificate of the Public Key Infrastructure (PKI) signing path for the pxGrid server certificate. Please refer to the "Prerequisite Cisco ISE connection configuration" on page 1677 above for instructions on how to obtain this file. |
| Cisco pxGrid client certificate | The pxGrid client certificate. Please refer to the "Prerequisite Cisco ISE connection configuration" on page 1677 above for instructions on how to obtain this file. |
| Cisco pxGrid client private key | Private key of pxGrid client certificate. Please refer to the "Prerequisite Cisco ISE connection configuration" on page 1677 above for instructions on how to obtain this file. |
| Cisco pxGrid client private | This is the passphrase used during the generation of the pxGrid client certificate. |

| Field Name | Description |
|---|---|
| key password | |

4. Once all fields have been completed, click **Next**. Deep Security Manager attempts to connect to pxGrid using the information provided.
   - If the connection is successful, the manager submits a client registration request to the pxGrid server which will require approval from the Cisco ISE administrator.
   - If the connection is unsuccessful, you are redirected to the information input page. Return to step 3 above and check that the information entered and files uploaded are correct and complete.
5. To approve a successful client registration request, the Cisco ISE administrator should navigate to Cisco ISE **Administration** > **pxGrid Services** > **Client Management** > **Clients** > **pxGrid Clients**. From there, the administrator can select the appropriate name and click **Approve**.
6. Once the administrator approves your registration request, return to the Deep Security Manager **Cisco Threat Containment** tab and click **Refresh Connection Status**. The connection status label changes to **Enabled**, and the ANC Policy Name and Network Containment Criteria fields are enabled.
7. Select the ANC Policy Name, select the appropriate Alert Criteria checkboxes, and then click **Save**. The configuration is now complete and Deep Security Manager will actively listen to security events that match the specified alert criteria, and will apply the ANC policy to the MAC addresses of the original hosts involved in the events.

## Cisco ISE connection status list

| Status | Description |
|---|---|
| Cisco pxGrid connection information has not been configured. | Cisco pxGrid connection information has not been configured in DSM. |
| Cisco pxGrid client registration has been submitted. | Cisco pxGrid connection information has been configured, and DSM has already sent client account registration request. DSM is waiting for ISE administrator to approve the client request. |
| Cisco pxGrid connected and client status is Enabled. | Cisco pxGrid connection information has been configured and client account approved (enabled). DSM connection to pxGrid is working. However, users should now provide ANC policy name. |
| Cisco pxGrid has been connected and ANC policy has been configured. | DSM connection to pxGrid is working and ANC policy name has been configured in DSM. Furthermore, DSM has already validated that the ANC policy exists in Cisco ISE. Note: This is the fully functional connection status. |

| Status | Description |
|---|---|
| Cisco pxGrid client status is Disabled. | The pxGrid client account is disabled in Cisco ISE. ISE administrator should enable pxGrid client account. |
| Cannot connect to Cisco ISE pxGrid server. | DSM unable to connect to Cisco pxGrid server. Please see DSM log for details of the error. Some possible causes:<br>• Network connection to Cisco pxGrid blocked by firewall or inaccessible.<br>• Root/client certificate expired or client credential revoked/deleted by Cisco ISE administrator. |

## Monitor and troubleshoot

A system event is generated whenever a computer or host has an ANC policy assigned or failed be assigned, and whenever a Cisco pxGrid connection fails or a Cisco pxGrid client certificate expires:

- Event ID: 9210
- Event Name: Cisco ANC policy has been assigned

- Event ID: 9211
- Event Name: Cisco ANC policy assignment failure

- Event ID: 9212
- Event Name: Cisco pxGrid connection failure

- Event ID: 9213
- Event Name: Cisco pxGrid client certificate expired

The description of a system event will include the name of the ANC policy and the MAC addresses associated with the successful assignment.

For more details, see System events.

You can check if a MAC address exists in the ANC assignment list by navigating to **Cisco ISE Operations** > **Adaptive Network Control** > **Endpoint Assignment**.

**Note:** Deep Security Manager will not reassign an ANC policy if the MAC address it uses is already assigned in Cisco ISE. In such cases where a malware or ransomware event is generated by the host but the MAC address has not been assigned an ANC policy, instead of generating an event, the manager will log the following message:

```
    Jun 04, 2025 2:29:42.268000000 PM [+0800]
com.trendmicro.manager.core.cisco.RapidThreatContainmentHandler
assignAncPolicy
    INFO: ThID:258|TID:0|TNAME:Primary|UID:-1|UNAME:|Skipping assign ANC
policy ANC_QUARANTINE to MAC 00:50:56:75:**:** as it has been already
assigned in Cisco ISE.
    Jun 04, 2025 2:29:42.271000000 PM [+0800]
com.trendmicro.manager.core.cisco.RapidThreatContainmentHandler
assignAncPolicy
    INFO: ThID:258|TID:0|TNAME:Primary|UID:-1|UNAME:|Skipping assign ANC
policy ANC_QUARANTINE to HostID 1 as all MACs already assigned in Cisco
ISE
```

# Integrate with Trend Vision One

## Integrate with Trend Vision One (XDR)

XDR in Trend Vision One applies expert analytics and global threat intelligence using data collected across multiple vectors - email, endpoints, servers, cloud workloads, and networks.

**Note:** Personally-identifiable information is collected by Trend Vision One. For more information, see Trend Micro XDR Data Collection Notice.

To integrate Trend Vision One with Deep Security, you need to purchase a license. For information, see "Register with Trend Vision One (XDR)" on the next page.

After registering with Trend Vision One (XDR), security events for protection modules are forwarded to Trend Vision One by default. To forward activity data to Trend Vision One, you need to install Trend Micro Endpoint Basecamp with the relevant deployment script or an installer downloaded from the Trend Vision One console.

## Register with Trend Vision One (XDR)

1. Obtain the Trend Vision One enrollment token from your organization's administrator who should follow instructions provided in Configuring Deep Security Software to obtain the token.

   > **Note:** The token is only valid for 24 hours after it has been generated. If it expires, generate a new one using the same steps.

2. In Deep Security Manager, go to **Administration > System Settings > Trend Vision One**.
3. Click **Register enrollment token**.
4. Use the dialog that opens to paste the enrollment token you received from your organization's administrator, and then click **Register**.

After the registration has been completed, Deep Security automatically forwards data to the Trend Vision One platform for analysis.

To register with Trend Vision One (XDR) via a proxy server, go to **Administration > System Settings > Proxies > Proxy Server Use > Deep Security Manager (Connection to Trend Micro services)** and select the correct proxy setting.

### Forward security events to Trend Vision One (XDR)

After successfully registering to Trend Vision One (XDR), the **Forward security events to Trend Vision One** setting is enabled by default. When this configuration is enabled, events from the following protection modules are forwarded to Trend Vision One:

- Anti-Malware
- Web Reputation
- Device Control
- Integrity Monitoring
- Log Inspection
- Intrusion Prevention

To stop forwarding security events to Trend Vision One, go to **Administration > System Settings > Trend Vision One** and deselect the **Forward security events to Trend Vision One** option.

If you have connected your agents and relays to the primary security update source via a proxy, the same proxy settings are automatically used.

## Forward activity data to Trend Vision One (XDR)

To forward activity data to Trend Vision One, install Trend Micro Endpoint Basecamp with the relevant deployment script or an installer downloaded from the Trend Vision One console.

The deployment script can be deployed with tools like RightScale, Chef, Puppet, or SSH as an administrator. Before you generate the deployment script, check the system requirements and supported operating systems on XDR Sensor System Requirements and be aware of the prerequisite verification executed on the script.

### Generate a deployment script

1. Before you begin, ensure that Deep Security Manager is connected to Trend Vision One.
2. Go to **Administration > System Settings > Trend Vision One**.
3. Under **Activity Data Forwarding**, select your platform. The deployment script generator displays the relevant script.
4. Click **Copy to Clipboard** and paste the deployment script in your preferred deployment tool, or click **Save to File**.

   The deployment scripts generated by Deep Security Manager for Windows requires Windows PowerShell version 4.0 or later. You must run PowerShell as an administrator. If the script is not running, enter the following command:
   `Set-ExecutionPolicy RemoteSigned`
   If you need to deploy an agent to a version of Windows or Linux that doesn't include PowerShell 4.0 or curl 7.34.0:
   - Linux: remove the `--tls1.2` tag.
   - Windows: remove the `[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12;` line.
   Removing the above lines allows an earlier version of TLS (version 1.0) to communicate with the manager. Ensure that an earlier TLS is also allowed on the manager and relays. See "Determine whether TLS 1.2 is enforced" on page 1664 and "Enable early TLS (1.0)" on page 1662 for details.

5. Modify the script to add the proxy server address if a proxy is required.

Once Trend Micro Endpoint Basecamp is installed, enable the sensor on Trend Vision One Endpoint Inventory.

**Note:** Endpoint Basecamp does not support proxy credentials.

#### Download the agent installer

To download the agent installer, go to **Trend Vision One > Endpoint Inventory** and follow the instructions to check the prerequisite verification for agents.

# Integrate with Trend Vision One Service Gateway

## Supported Service Gateway version

Deep Security supports Service Gateway version 1.0, 2.0, and 3.0

## System requirements

For information on the system requirements for Service Gateway, see Service Gateway appliance system requirements.

Trend Micro recommends using Deep Security Agent version 20.0.1-690 or later on Windows and Linux with Service Gateway.

## Deploy Service Gateway

For information on deploying the Service Gateway in your network, see Deploy a Service Gateway and configure firewall exceptions.

# Integrate the Service Gateway forward proxy

You can enable forward proxy on the Service Gateway and apply it to Deep Security. Deep Security then deploys the forward proxy settings to Deep Security Agent.

Once the agent receives the settings, it connects each service server (for example, Smart Protection Service) through forward proxy. If a server cannot be reached, the agent tries an alternative proxy configured in the agent's policy.

Forward proxy must be enabled from Trend Vision One. For instructions, see Managing services in Service Gateway.

Once Deep Security is integrated with Trend Vision One, the forward proxy information appears in the Deep Security console under **Administration > System Settings > Proxies > Proxy Servers**.

After the forward proxy settings are synchronized to Deep Security, the agent receives the settings on its next policies check.

# Integrate the Service Gateway ActiveUpdate service

You can enable ActiveUpdate on Service Gateway to act as the update source for Deep Security.

## Enable the ActiveUpdate services

The ActiveUpdate service needs to be enabled in Trend Vision One before it can integrate with Deep Security. For details, see Managing services in Service Gateway.

## Obtain Deep Security ActiveUpdate source URL

You get the ActiveUpdate source URL from the Deep Security console **Administration > System Settings > Updates > Security Updates > Primary Security Update Source > Trend Micro Update Server**.

## Configure the ActiveUpdate service

For information on configuring the ActiveUpdate service in Trend Vision One, see ActiveUpdate configuration.

## Configure the ActiveUpdate service

To configure the Deep Security update source setting, apply the agent settings, and then get the new ActiveUpdate components from this Trend Vision One:

1. On the Deep Security console, go to **Administration > System Settings > Updates**.
2. Select **Other update source** and paste the ActiveUpdate URL which you generated and copied when configuring the ActiveUpdate service.
3. Click **Save**.

# Integrate the Service Gateway Smart Protection service

You can enable the Smart Protection Services on Service Gateway to be a Deep Security local Smart Protection Server.

## Enable Smart Protection services

Smart Protection services must be enabled from Trend Vision One. For instructions, see Managing services in Service Gateway.

## Configure local File Reputation service on Deep Security Policy

1. On the Deep Security console, go to **Policies > Details > Anti-Malware > General** tab and ensure that **Anti-Malware State** is set to **On**.
2. On the **Smart Protection** tab, ensure that **Smart Scan** is set to **On**.
3. On **Smart Protect server to File Reputation Service**, select **Use locally installed Smart Protection Server**.
4. Enter the value for **File Reputation Server URL**, which you can copy from the **Service Gateway** page, and then click **Add**.
5. Click **Save**.

## Configure local Web Reputation service on Deep Security Policy

1. On the Deep Security console, go to **Policies > Details > Web Reputation > General** tab and ensure that **Web Reputation State** is set to **On**.
2. On **Smart Protect server to Web Reputation Service**, select **Use locally installed Smart Protection Server**.
3. Enter the value for **Web Reputation Server URL**, which you can copy from the **Service Gateway** page, and then click **Add**.
4. Click **Save**.

# FAQs

## Why does my Windows machine lose network connectivity when I turn on protection?

A Windows machine will lose connectivity for a brief period of time during the network driver installation while the Deep Security Agent installs a network driver to examine traffic. This only happens the *first* time a policy is applied that includes one of the following:

- Web reputation
- Firewall
- Intrusion prevention

A Windows machine uses the same driver is used for all three protection modules listed above. Turning on web reputation, firewall or intrusion prevention after one of those features already turned on will not cause another network blip. You may see a similar interruption in network connectivity when the agent is upgraded (as the driver may also need to be upgraded).

# How do I get news about Deep Security?

The Deep Security news feed has been discontinued. Instead, you can find the latest news on product changes in the "What's new?" on page 119 article.

Trend Micro continue to release new rule updates every Tuesday, with additional updates as new threats are discovered. Details about each rule update are provided in the Trend Micro Threat Encyclopedia.

# How does agent protection work for Solaris zones?

The Deep Security Agent can be deployed only on a Solaris global zone. If your Solaris environment uses any non-global zones, the protection that the agent can provide for the global zone and non-global zones will differ with each protection module:

- Intrusion Prevention
- Firewall
- Web Reputation
- Anti-Malware
- Integrity Monitoring
- Log Inspection

See "Install the agent manually" on page 548 for more on installing the Deep Security Agent on Solaris.

# Intrusion Prevention (IPS), Firewall, and Web Reputation

If your Solaris environment uses any non-global zones, the Intrusion Prevention, Firewall, and Web Reputation modules can only provide protection to specific traffic flows between the global zone, non-global zones and any external IP addresses. Which traffic flows the agent can protect depends on if the non-global zones use a shared-IP network interface or an exclusive-IP network interface.

Kernel zones use an exclusive-IP network interface and agent protection to traffic flows is limited to that network configuration.

## Non-global zones use a shared-IP network interface

Agent protection to traffic flows in a shared-IP configuration is as follows:

| Traffic Flow | Protected by agent |
|---|---|
| external address <-> non-global zone | Yes |
| external address <-> global zone | Yes |
| global zone <-> non-global zone | No |
| non-global zone <-> non-global zone | No |

## Non-global zones use an exclusive-IP network interface

Agent protection to traffic flows in a exclusive-IP configuration is as follows:

| Traffic Flow | Protected by agent |
|---|---|
| external address <-> non-global zone | No |
| external address <-> global zone | Yes |
| global zone <-> non-global zone | Yes |
| non-global zone <-> non-global zone | No |

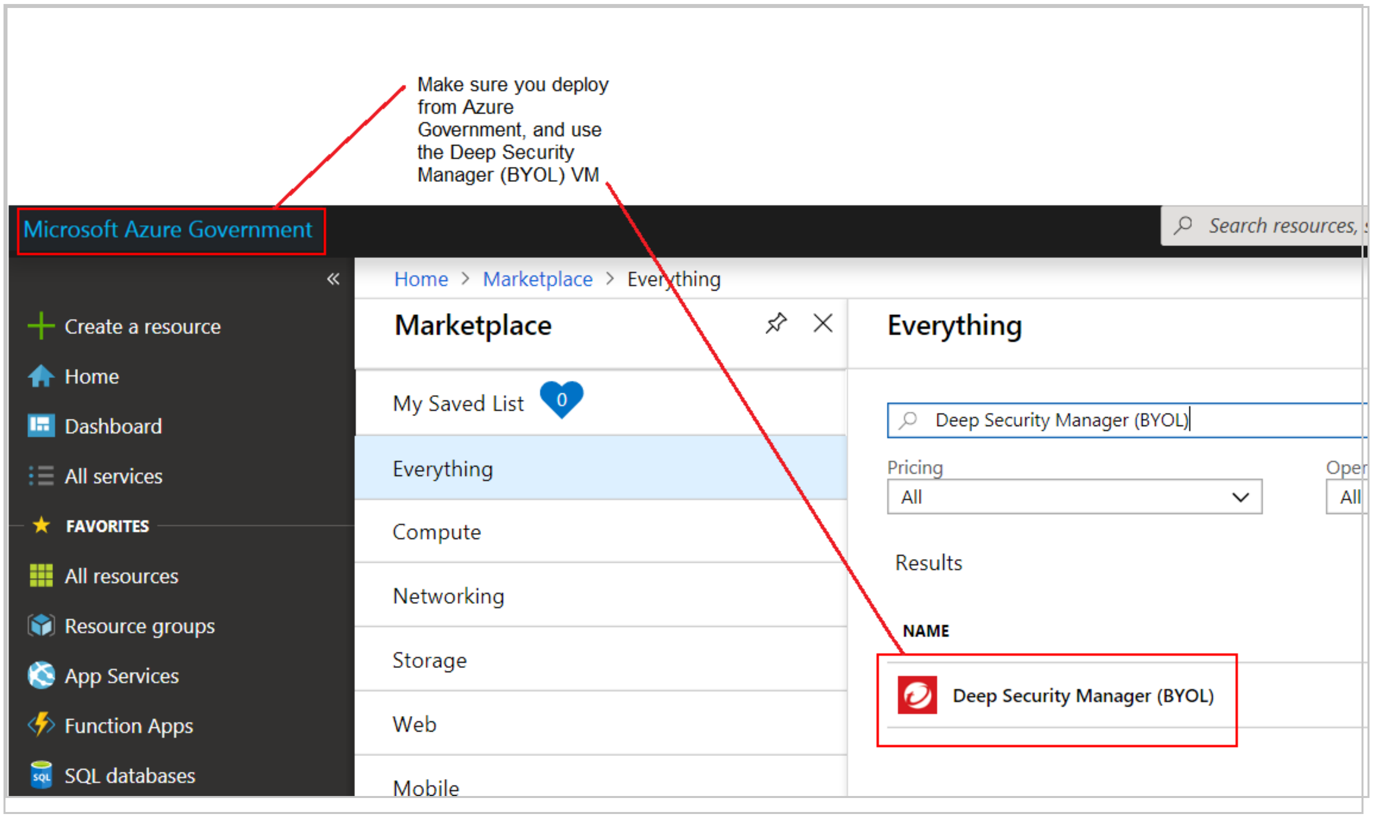
## Anti-Malware, Integrity Monitoring, and Log Inspection

The Anti-Malware, Integrity Monitoring and Log Inspection modules provides protection to the global zone. For non-global zones, any files or directories that are also visible to the global zone are protected. Files specific to a non-global zone are not protected.

# How do I protect Azure Government instances?

To protect Azure Government instances, you have a few options:

- You can deploy Deep Security Manager using the Deep Security Manager (BYOL) VM that's listed inside Azure Government's Marketplace (see the image below). The deployment instructions for the Azure Government are the same as any other region. See "Deploy Deep Security Manager VM for Azure Marketplace" on page 506.
- You can install the Deep Security Manager on-premises software onto an Azure VM running inside Azure Government.



Make sure you deploy from Azure Government, and use the Deep Security Manager (BYOL) VM

## Protecting Azure Government instances using a manager in global Azure

Warning: Be aware that if your Deep Security Manager is outside of Azure Government, using it to manage computers in the Azure Government would break ITAR compliance.

You cannot use the **Computers > Add > Add Account** option in the Deep Security Manager console to add Azure Government instances to a manager in global Azure, and vice versa. This is because the manager can only communicate with Azure instances in its own cloud.

# How does Deep Security Agent use the Amazon Instance Metadata Service?

When running on EC2 instances in AWS, the Deep Security Agent uses the Amazon Instance Metadata Service (IMDS) to query information about the EC2 instance.

Note: Deep Security support for IMDS v2 was added in Deep Security Manager FR 2020-04-29 and Deep Security Agent FR 2020-05-19. If you are using an older version of Deep Security only IMDS v1 is supported and you must ensure that your AWS configuration allows Deep Security Agent access to host metadata using IMDS v1.

The information retrieved by the Deep Security Agent is necessary to ensure that the agent activates under the proper AWS account within Deep Security.

If the Deep Security Agent cannot successfully retrieve data from the instance using a Metadata Service Version 1 (IMDSv1) or 2 (IMDSv2), the following issues might be encountered:

| Issue | Root cause | Resolution | Additional notes |
|---|---|---|---|
| Duplicate computers appear - one under the AWS account and another outside of the AWS account. | If the Deep Security Agent does not have access to Instance Metadata Service Version 1 (IMDSv1) or 2 (IMDSv2), Deep Security cannot properly associate this activation with the desired cloud account. | Ensure that Deep Security has access to IMDS v1 or IMDS v2.<br>For more | If you determine that the creation of duplicate computers has occurred, you can use inactive agent cleanup to automatically remove these computers. |

| Issue | Root cause | Resolution | Additional notes |
|---|---|---|---|
| Smart folders or event-based tasks based on AWS metadata fail. | If the Deep Security Agent does not have access to Instance Metadata Service Version 1 (IMDSv1) or 2 (IMDSv2), Deep Security cannot access the AWS metadata needed for these operations. | details, see Configuring the Instance Metadata Service. | N/A |

# How can I minimize heartbeat alerts for offline environments in an AWS Elastic Beanstalk environment?

AWS Elastic Beanstalk allows you to create multiple environments so that you can run different versions of an application at the same time. These environments usually include a production and development environment and often the development environment is powered down at night. When the development environment is brought back online in the morning, Deep Security will generate alerts related to communication problems for the period of time that it was offline. Although these alerts are actually false from your perspective, they are legitimate alerts from the perspective of Deep Security because an alert is generated whenever a specified number of heartbeats is missed.

You can minimize these heartbeat-related alerts or even prevent them from being generated for environments that you know will be offline for a period of time every day by creating a policy with specific heartbeat settings and applying that policy to the servers in those partially offline environments.

1. Go to the **Policies** tab in the main Deep Security Manager window.
2. Create a new policy or edit an existing one.
3. Click the **Settings** tab in the **Policy editor**[1] and go to the **Computer** tab.
4. Change one or both of the **Heartbeat Interval** and **Number of Heartbeats that can be missed before an alert is raised** setting to numbers that take into account the number of hours your Elastic Beanstalk environment will be offline.
   *For example, if you know that a server will be offline for 12 hours a day and the Heartbeat Interval is set at 10 minutes, you could change the Number of Heartbeats that can be*

[1] To open the Policy editor, go to the Policies page and double-click the policy that you want to edit (or select the policy and click Details).

*missed before an alert is raised setting to unlimited to never get an alert or you could increase the Heartbeat Interval to something greater than 10 to get fewer alerts.*

5. Click **Save** and apply the policy to all relevant servers.

For more information on using Deep Security in an AWS Elastic Beanstalk environment, you can watch the Trend Micro webinar Deploying Scalable and Secure Web Apps with AWS Elastic Beanstalk and Deep Security.

# Why can't I add my Azure server using the Azure cloud connector?

If an Azure server loses connectivity to the Azure metadata service, the Deep Security Manager will no longer be able to identify it as an Azure server and you will be unable to add it using the Azure cloud connector.

This situation can happen if the server's public or private IP address is changed outside of the Azure console. The Azure server relies on DHCP to communicate with the metadata service and changing the IP outside of the console disables DHCP.

Microsoft recommends against changing the Azure VM's IP address from within its operating system, unless necessary, such as when assigning multiple IP addresses to a Windows VM. For details, see this Azure article.

To check if your Azure server is able to connect to the Azure metadata service, run the Detect Windows Azure Virtual Machine PowerShell script from the Microsoft Script Center.

# Why can't I view all of the VMs in an Azure subscription in Deep Security?

If not all of the virtual machine resources in an Azure subscription are being displayed on the Computers page of Deep Security Manager, this could be because they were deployed using the Azure deployment model Resource Manager. All resources are deployed using this model unless you select **Classic** from the **Select a deployment model** list.

Not all VMs are displayed because older versions of the Deep Security Manager use the Service Management API provided by the classic Azure deployment model (the Service Management model) to connect to Azure virtual machines so it can only enumerate VMs deployed with the Classic model.

To see both Classic or Resource Manager VMs, upgrade your cloud connector. For more information, see "Why should I upgrade to the new Azure Resource Manager connection functionality?" on page 605.

**Note:** If you are unable to upgrade your Resource Manager servers as per the article above, you can still protect them by using the deployment script on the VM and letting the activation create a new computer object outside of the connector.

# Deep Security coverage of Log4j vulnerability

On December 9, 2021, a new critical zero-day vulnerability impacting multiple versions of the popular Apache Log4j 2 logging library was publicly disclosed. If exploited, this vulnerability could result in Remote Code Execution (RCE) by logging a certain string on affected installations. This specific vulnerability has been assigned CVE-2021-44228 and is also being commonly referred to as "Log4Shell" in various blogs and reports.

Deep Security includes the Intrusion Prevention module (IPS), which protects your computers from zero-day vulnerabilities and other attacks. Intrusion Prevention rules provide "virtual patching" by intercepting traffic that's trying to exploit the vulnerability, protecting your computers until vendor's patches that fix the vulnerability are released, tested, and deployed.

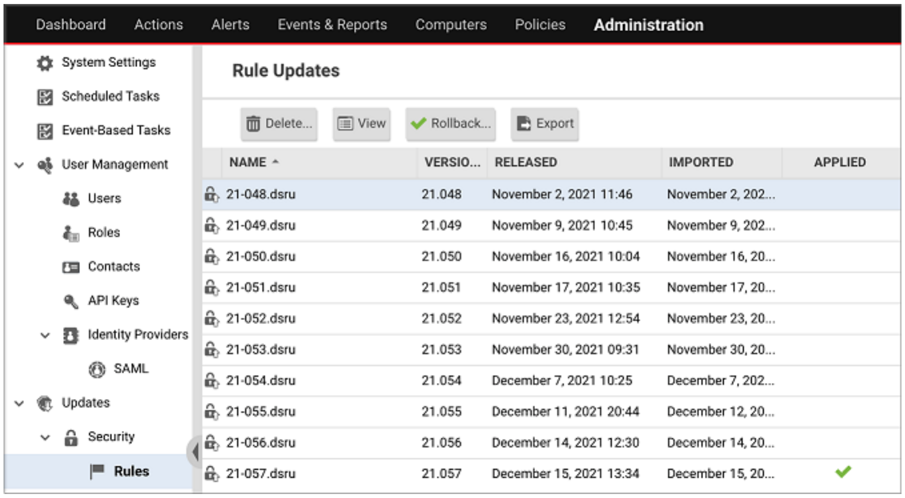
The Trend Micro Labs team has provided a new IPS rule to address this vulnerability:

**1011242 - Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)**

## Apply virtual patching for the Log4j vulnerability

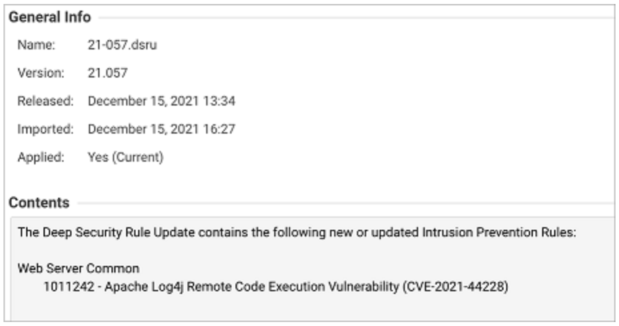
Follow the steps below to check whether the new rule is protecting your computers.

1. In Deep Security Manager, go to **Administration > Updates > Security > Rules**.
2. The new rule is included in **21-057.dsru**. Check that the rule update is shown as **Applied**.



Rule Updates

| NAME | VERSIO... | RELEASED | IMPORTED | APPLIED |
|---|---|---|---|---|
| 21-048.dsru | 21.048 | November 2, 2021 11:46 | November 2, 202... | |
| 21-049.dsru | 21.049 | November 9, 2021 10:45 | November 9, 202... | |
| 21-050.dsru | 21.050 | November 16, 2021 10:04 | November 16, 20... | |
| 21-051.dsru | 21.051 | November 17, 2021 10:35 | November 17, 20... | |
| 21-052.dsru | 21.052 | November 23, 2021 12:54 | November 23, 20... | |
| 21-053.dsru | 21.053 | November 30, 2021 09:31 | November 30, 20... | |
| 21-054.dsru | 21.054 | December 7, 2021 10:25 | December 7, 202... | |
| 21-055.dsru | 21.055 | December 11, 2021 20:44 | December 12, 20... | |
| 21-056.dsru | 21.056 | December 14, 2021 12:30 | December 14, 20... | |
| 21-057.dsru | 21.057 | December 15, 2021 13:34 | December 15, 20... | ✓ |



General Info

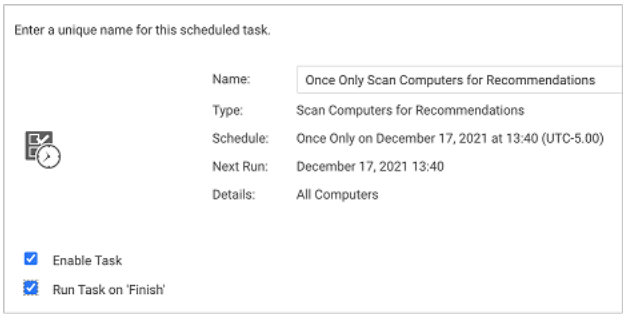
Name: 21-057.dsru
Version: 21.057
Released: December 15, 2021 13:34
Imported: December 15, 2021 16:27
Applied: Yes (Current)

Contents

The Deep Security Rule Update contains the following new or updated Intrusion Prevention Rules:

Web Server Common
1011242 - Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)

3. If the rule isn't applied, run a recommendation scan. We suggest that you create a 'run once' scheduled task and select the **Run Task on 'Finish'** option.



Enter a unique name for this scheduled task.

Name: Once Only Scan Computers for Recommendations
Type: Scan Computers for Recommendations
Schedule: Once Only on December 17, 2021 at 13:40 (UTC-5.00)
Next Run: December 17, 2021 13:40
Details: All Computers

☑ Enable Task
☑ Run Task on 'Finish'

4. To ensure that the rule gets applied wherever it's recommended, open the policy that is assigned to the computers you just scanned, go to **Intrusion Prevention > General**, and search for rule 1011242. Select the checkbox next to the rule name to assign it to the policy. All computers protected by this policy will have the rule applied to it.

5. Intrusion Prevention operates in either Detect or Prevent mode. Detect mode generates events about rule violations but doesn't block traffic. Prevent mode generates events and blocks traffic that matches rules, to prevent attacks. To set Prevent mode, open the computer or policy editor, go to **Intrusion Prevention > General** and set **Intrusion Prevention Behavior** to **Prevent**. Click **Save**.

## Identify potentially affected hosts

If you are also using Trend Micro Vision One, you can use the following query to identify hosts that may be affected by this vulnerability:

```
eventName:DEEP_PACKET_INSPECTION_EVENT AND (ruleId:1008610 OR ruleId:1011242
OR ruleId:1005177) AND ("${" AND ("lower:" OR "upper:" OR "sys:" OR "env:"
OR "java:" OR "jndi:"))
```

## Use a custom Log Inspection rule to investigate activity

Trend Micro has provided a Log Inspection rule to help identify activity related to this vulnerability:

**1011241 - Apache Log4j Remote Code Execution Vulnerability (CVE-2021-44228)**

You can also create a custom Log Inspection rule to detect patterns that are discovered in the future. For details, see Custom Log Inspection Rules for Log4Shell Vulnerability on Trend Cloud One - Endpoint & Workload Security and Deep Security.

## More resources from Trend Micro about this vulnerability

- For up-to-date information about how Trend Micro can help, see Apache Log4j (Log4Shell) Vulnerability.
- For a video with information about this vulnerability.
- For details on this vulnerability and how Trend Micro can help protect your environment from attack, see SECURITY ALERT: Apache Log4j "Log4Shell" Remote Code Execution 0-Day Vulnerability (CVE-2021-44228).

# Troubleshooting

## Offline agent

A computer status of Offline or Managed (Offline) means that Deep Security Manager has not communicated with the Deep Security Agent's instance for some time and has exceeded the missed heartbeat threshold (see "Configure the heartbeat" on page 1374). The status change can also appear in alerts and events.

## Causes

Heartbeat connections can fail due to the following reasons:

- The agent is installed on a workstation or other computer that has been shut down. If you are using Deep Security to protect computers that sometimes get shut down, make sure the policy assigned to those computers does not raise an alert when there is a missed heartbeat. In the policy editor, go to **Settings > General > Number of Heartbeats that can be missed before an alert is raised** and change the setting to Unlimited.
- Firewall, IPS rules, or security groups block the heartbeat port number.
- Outbound (ephemeral) ports were blocked accidentally. See "Blocked port" on page 1312 for troubleshooting tips.
- Bi-directional communication is enabled, but only one direction is allowed or reliable (see "Configure communication directionality" on page 1375).
- Computer is powered off.
- Computer has left the context of the private network
  This can occur if roaming endpoints (such as a laptop) cannot connect to the manager at their current location. Guest Wi-Fi, for example, often restricts open ports, and has NAT when traffic goes across the Internet.
- Amazon WorkSpace computer is being powered off, and the heartbeat interval is fast (for example, one minute). In this case, wait until the WorkSpace is fully powered off, and at that point the status should change from Offline to VM Stopped.
- DNS was down, or could not resolve the manager's hostname.
- The manager, the agent, or both are under very high system resource load.
- The agent process might not be running.

- Certificates for mutual authentication in the SSL or TLS connection have become invalid or revoked (see "Replace the Deep Security Manager TLS certificate" on page 1494).
- The agent's or manager's system time is incorrect (required by SSL/TLS connections).
- Deep Security rule update is not yet complete, temporarily interrupting connectivity.
- On AWS EC2, ICMP traffic is required, but is blocked.
- After upgrading to agent version 20.0.0.6313 or later, if the agent is still using SHA-1 algorithm. The agent only allows newer, more secure cryptographic algorithms for communication to the manager.

Tip: If you are using manager-initiated or bi-directional communication, and are having communication issues, you should change to agent-initiated activation (see "Activate and protect agents using agent-initiated activation and communication" on page 1386).

To troubleshoot the error, verify that the agent is running and can communicate with the manager.

## Verify that the agent is running

On the computer with the agent, verify that the Trend Micro Deep Security Agent service is running. Methods depend on the operating system:

- On Windows, open the Microsoft Windows Services Console (services.msc) or Task Manager. Look for the service named ds_agent.

- On Linux, open a terminal and enter the command for a process listing. Look for the service named ds_agent or ds-agent, such as:

  ```
  sudo ps -aux | grep ds_agent
  ```

  ```
  sudo service ds_agent status
  ```

- On Solaris, open a terminal and enter the command for a process listing. Look for the service named ds_agent, such as:

  ```
  sudo ps -ef | grep ds_agent
  ```

  ```
  sudo svcs -l svc:/application/ds_agent:default
  ```

## Verify DNS

If agents connect to the manager via its domain name or hostname, not its IP address, test the DNS resolution:

```
nslookup [manager domain name]
```

DNS service must be reliable.

If the test fails, verify that the agent is using the correct DNS proxy or server (internal domain names cannot be resolved by a public DNS server such as Google or your ISP). If a name such as dsm.example.com cannot be resolved into its IP address, communication fails, even though correct routes and firewall policies exist for the IP address.

If the computer uses DHCP, in the computer or policy settings, in the **Advanced Network Engine** area, you might need to enable **Force Allow DHCP DNS** (see "Network engine settings" on page 658).

## Allow outbound ports (agent-initiated heartbeat)

Telnet to required port numbers on the manager to verify that a route exists, and the port is open:

```
telnet [manager IP]:4120
```

Telnet success proves most of the same things as a ping: a route and correct firewall policy exist, and Ethernet frame sizes are correct. Ping is disabled on computers that use the default security policy for the manager. Networks sometimes block ICMP ping and traceroute to block attackers' reconnaissance scans. Therefore typically you cannot ping the manager to test.

If telnet fails, trace the route to discover which point on the network is interrupting connectivity:

- On Linux, enter the following command:

  ```
  traceroute [agent IP]
  ```

- On Windows, enter the following command:

  ```
  tracert [agent IP]
  ```

Adjust firewall policies, routes, NAT port forwarding, or all three to correct the problem. Verify both network and host-based firewalls, such as Windows Firewall and Linux iptables. For an AWS EC2 instance, see the Amazon documentation Amazon EC2 Security Groups for Linux

Instances or Amazon EC2 Security Groups for Windows Instances. For an Azure VM instance, see the Microsoft Azure documentation Modifying a Network Security Group.

If connectivity tests from the agent to the manager succeed, then next you must test connectivity in the other direction (firewalls and routers often require policy-route pairs to allow connectivity. If only one of the two required policies or routes exist, then packets are allowed in one direction but not the other).

## Allow inbound ports (manager-initiated heartbeat)

On the manager, ping the agent and telnet to the heartbeat port number to verify that heartbeat and configuration traffic can reach the agent:

```
ping [agent IP]
```

```
telnet [agent IP]:4118
```

If the ping and telnet fail, use:

```
traceroute [agent IP]
```

to discover which point on the network is interrupting connectivity. Adjust firewall policies, routes, NAT port forwarding, or all three to correct the problem.

If IPS or firewall rules are blocking the connection between the agent and the manager, then the manager cannot connect in order to unassign the policy that is causing the problem. To solve this, enter the command on the computer to reset policies on the agent:

```
dsa_control -r
```

You must reactivate the agent after running this command.

## Allow ICMP on Amazon AWS EC2 instances

In the AWS cloud, routers require ICMP type 3 code 4. If this traffic is blocked, connectivity between agents and the manager may be interrupted.

You can force allow this traffic in Deep Security. Either create a firewall policy with a force allow, or in the computer or policy settings, in the **Advanced Network Engine** area, enable **Force Allow ICMP type3 code4** (see "Network engine settings" on page 658).

## Fix the upgrade issue on Solaris 11

A problem may occur if you previously installed Deep Security Agent 9.0 on Solaris 11, and then upgraded the agent software to 11.0 directly without first installing 9.0.0-5616 or a later 9.0 agent. In this scenario, the agent may fail to start after the upgrade and may appear as offline in Deep Security Manager. To fix this issue:

1. Uninstall the agent from the server. See "Uninstall Deep Security Agent" on page 1556.
2. Install the Deep Security Agent 11.0. See "Install the agent manually" on page 548.
3. Reactivate the agent on the manager. See "Activate the agent" on page 566.

# High CPU usage

On a computer protected by Deep Security Agent, you can use these steps to determine and resolve the cause of high CPU usage.

1. Verify that the Trend Micro Deep Security Agent process (ds_agent.exe on Windows) has unusually high CPU usage. Method varies by operating system.

   Windows: Task Manager

   Linux: `top`

   Solaris: `prstat`

   AIX: `topas`
2. Verify that the agent is updated to the latest version.
3. Apply the best practices on "Improve Anti-Malware performance" on page 763 and "Performance tips for intrusion prevention" on page 848.
4. If you have just enabled application control, wait until the initial baseline ruleset is complete. Time required varies by the number of files on the file system. The CPU usage should decrease.
5. If a recommendation scan is being performed, try running scans during a time when the computer is less busy, or (if the computer is a VM) allocating more vCPUs.
6. Temporarily disable each protection feature (anti-malware etc.), one at a time. Check CPU usage each time to determine if a specific module is the cause.
7. If high CPU usage still continues, try temporarily stopping the agent. Verify that the issue stops when the agent is stopped. If it does, collect diagnostic information and give it to your support provider.

# Diagnose problems with agent deployment (Windows)

If a Deep Security Agent on Windows fails to install or activate, look in the deployment logs to find the cause and troubleshoot it.

1. Log in to the computer where you were trying to install the agent.
2. Go to `%appdata%\Trend Micro\Deep Security Agent\installer`.
3. Examine:
   - **dsa_deploy.txt** - Log from the PowerShell script. Contains agent activation issues.
   - **dsa_install.txt** - Log from the MSI installer. Contains agent installation issues.

# Anti-Malware Windows platform update failed

If you get a `935 Software Update: Anti-Malware Windows Platform Update Failed` error, double-click the error message to display more detailed information. The “Message” in the error event may include:

- "An incompatible Anti-Malware component from another Trend Micro product" below
- "An incompatible Anti-Malware component from a third-party product" on the next page
- "The certificate is not signed by Trend Micro" on the next page
- "The signed certificate is not trusted" on the next page
- "The signed certificate is not authorized with appropriated purpose" on the next page
- "Other/Unknown Error" on page 1704

## An incompatible Anti-Malware component from another Trend Micro product

To solve this error:

1. Uninstall the incompatible Trend Micro product (for example, Office Scan or Endpoint Sensor).
2. Reinstall the Deep Security Agent.

## An incompatible Anti-Malware component from a third-party product

To solve this error:

1. Uninstall the third-party product.
2. Reinstall Deep Security Agent.
3. Add Deep Security to the third-party software's exception list. Contact Trend Micro support if you need assistance.

## The certificate is not signed by Trend Micro

To solve this error:

1. Update your Windows computer to support SHA-2 code signing. For details, see New versions of Trend Micro Deep Security agents for Windows will only be signed with SHA-2.
2. Restart Deep Security Agent.
3. If the error is not resolved, please collect an agent diagnostic package and contact Trend Micro support for assistance.

## The signed certificate is not trusted

To solve this error:

1. Follow the instructions in Updating the VeriSign, DigiCert, USERTrust RSA certificate on Deep Security to import required certificates.
2. Restart Deep Security Agent.
3. If the error is not resolved, please collect an agent diagnostic package and contact Trend Micro support for assistance.

## The signed certificate is not authorized with appropriated purpose

To solve this error:

1. Follow the instruction in Examining purpose of certificate in Deep Security to enable the purpose of the certificate.
2. Restart Deep Security Agent.

3. If the error is not resolved, please collect an agent diagnostic package and contact Trend Micro support for assistance.

## Other/Unknown Error

To solve this error:

1. Uninstall and reinstall the Deep Security Agent.
2. If the error is not resolved, please collect an agent diagnostic package and contact Trend Micro support for assistance.

**Note:** These three conditions belong to this category:

- The digital signature is not found.
- The certificate failed to be verified.
- Unexpected error occurs during certificate check.

# Security update connectivity

Verify the connectivity between the relay server and its Active Update source or proxy server.

1. To verify that both a route exists and that the relay port number is open, enter the command:

   ```
   telnet [relay IP] [port number]
   ```

   If the telnet fails, verify that a route exists and that firewall policies (if any) allow the traffic by pinging or using traceroute. Also verify that the port number is open, and doesn't have a port conflict.

2. To verify that the DNS server can resolve the domain name of the relay, enter the command:

   ```
   nslookup [relay domain name]
   ```

   If the test fails, verify that the agent is using the correct DNS proxy or server (internal domain names can't be resolved by a public DNS server such as Google or your ISP).

3. If you use a proxy server, on Deep Security, confirm that the proxy settings are correct.
4. To determine if your Deep Security settings are blocking connectivity, unassign the current policy.

# SQL Server domain authentication problems

If you experience problems connecting to the Microsoft SQL Server database when installing Deep Security Manager, follow the instructions below to troubleshoot the problem.

> **Note:** This topic's scope is limited to Windows domain authentication issues. If you are using SQL Server Authentication instead, see "Configure the database" on page 504 and review the configuration steps listed in that topic to troubleshoot any problems.

> **Tip:** 'Windows domain authentication' goes by many names: Kerberos authentication, domain authentication, Windows authentication, integrated authentication, and a few others. In this topic, the terms 'Kerberos' and 'Windows domain authentication' are used.

"Step 1: Verify the host name and domain" below

"Step 2: Verify the servicePrincipalName (SPN)" on the next page

"Step 3: Verify the krb5.conf file (Linux only)" on page 1718

"Step 4: Verify the system clock " on page 1720

"Step 5: Verify the firewall " on page 1720

"Step 6: Verify the dsm.properties file" on page 1720

## Step 1: Verify the host name and domain

You must make sure the **Host name** field is in FQDN format and resolvable by the DNS server:

1. When you run the Deep Security Manager installer and reach the database step, make sure you specify the SQL server's FQDN. Don't input an IP address or NetBIOS host name.

   Example of a valid host name: `sqlserver.example.com`

2. Make sure the FQDN is registered and resolvable by the DNS server. To check if the correct host name was configured in the DNS entry, use the `nslookup` command-line utility. This utility can be invoked from any computer on the domain. Enter the following command:

   ```
   nslookup <SQL Server FQDN>
   ```

   where `<SQL_Server_FQDN>` is replaced with the FQDN of the SQL server. If the utility can resolve the provided FQDN successfully, then the DNS entry is configured properly. If the

FQDN cannot be resolved, then configure a DNS A record and reverse record that includes the FQDN.

3. Still on the installer's database page, click **Advanced** and make sure you specify the SQL server's full domain name in the **Domain** field. The domain must include one or more dots ("."). Don't input a short domain name or NetBIOS name.

   Example of a valid domain name: `example.com`

4. Check if the domain name is in FQDN format using the `nslookup` command-line utility. Enter the following command:

   ```
   nslookup <Domain_Name>
   ```

   where `<Domain_Name>` is replaced with the full domain name of the SQL server. If the utility can resolve the provided domain name, then it is the full domain name.

   > **Note:** Database authentication using Microsoft workgroups is not supported by Deep Security Manager 10.2 and later. For Windows domain authentication, you'll need to have installed an Active Directory domain controller, configured a domain, and added the SQL server to this domain. If there is no Active Directory domain infrastructure in your environment, you must use SQL Server Authentication instead. (To use SQL Server Authentication instead of Windows domain authentication, enter the Deep Security Manager database owner's user name and password into the **User name** and **Password** fields on the **Database** page of the manager's installer. Do not input a domain. The omission of a domain name causes SQL Server Authentication to be used. )

## Step 2: Verify the servicePrincipalName (SPN)

You must make sure the servicePrincipalName (SPN) is configured correctly in Active Directory.

For Microsoft SQL Server, the SPN is in this format:

```
MSSQLSvc/<SQL_Server_Endpoint_FQDN>
```

```
MSSQLSvc/<SQL_Server_Endpoint_FQDN>:<PORT>
```

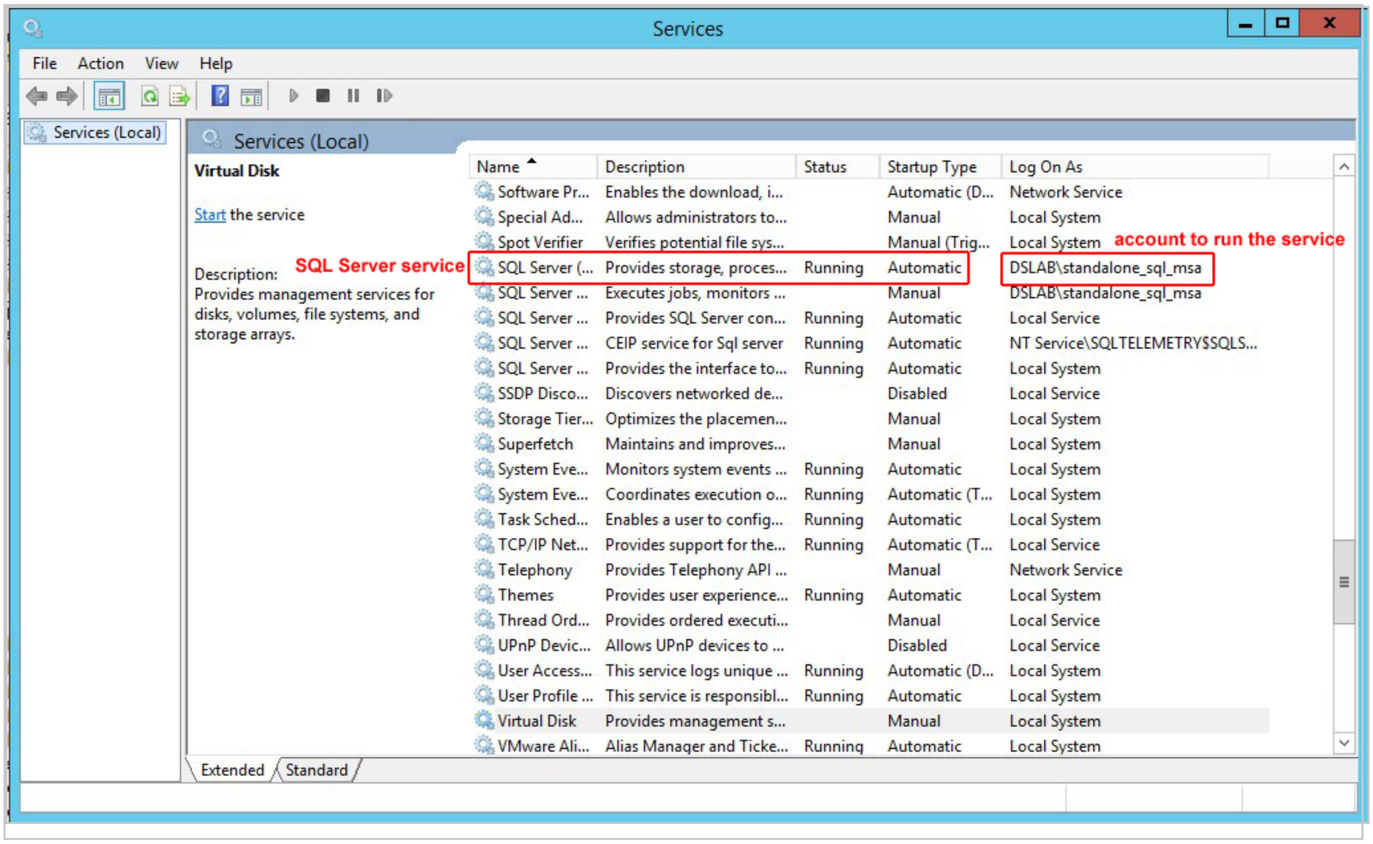
To verify that the SPN is correct, run through these tasks. At the end are some step-by-step instructions for specific use cases, references to other documentation, and debugging tips.

"Step 2a: Identify the account (SID) running the SQL Server service" on the next page

## Step 2a: Identify the account (SID) running the SQL Server service

The SPN is configured inside the account running the SQL Server service.

To identify which account is running the SQL Server service, use the `services.msc` utility. You see the SQL Server service appear, along with the associated account.



**Virtual Disk**

Start the service

Description:
Provides management services for disks, volumes, file systems, and storage arrays.

SQL Server service

account to run the service

| Name | Description | Status | Startup Type | Log On As |
|---|---|---|---|---|
| Software Pr... | Enables the download, i... | | Automatic (D... | Network Service |
| Special Ad... | Allows administrators to... | | Manual | Local System |
| Spot Verifier | Verifies potential file sys... | | Manual (Trig... | Local System |
| SQL Server (... | Provides storage, proces... | Running | Automatic | DSLAB\standalone_sql_msa |
| SQL Server ... | Executes jobs, monitors ... | | Manual | DSLAB\standalone_sql_msa |
| SQL Server ... | Provides SQL Server con... | Running | Automatic | Local Service |
| SQL Server ... | CEIP service for Sql server | Running | Automatic | NT Service\SQLTELEMETRY$SQLS... |
| SQL Server ... | Provides the interface to... | Running | Automatic | Local System |
| SSDP Disco... | Discovers networked de... | | Disabled | Local Service |
| Storage Tier... | Optimizes the placemen... | | Manual | Local System |
| Superfetch | Maintains and improves... | | Manual | Local System |
| System Eve... | Monitors system events ... | Running | Automatic | Local System |
| System Eve... | Coordinates execution o... | Running | Automatic (T... | Local System |
| Task Sched... | Enables a user to config... | Running | Automatic | Local System |
| TCP/IP Net... | Provides support for the... | Running | Automatic (T... | Local Service |
| Telephony | Provides Telephony API ... | | Manual | Network Service |
| Themes | Provides user experience... | Running | Automatic | Local System |
| Thread Ord... | Provides ordered executi... | | Manual | Local Service |
| UPnP Devic... | Allows UPnP devices to ... | | Disabled | Local Service |
| User Access... | This service logs unique ... | Running | Automatic (D... | Local System |
| User Profile ... | This service is responsibl... | Running | Automatic | Local System |
| Virtual Disk | Provides management s... | | Manual | Local System |
| VMware Ali... | Alias Manager and Ticke... | Running | Automatic | Local System |

## Step 2b: Find the account in Active Directory

Once you know the name of the account running the SQL Server service, you must locate it in Active Directory. The account can be in a few possible locations depending on whether it is a local virtual account, a domain account, or a Managed Service account. The table below outlines these possible locations. You can use the ADSI Editor (`adsiedit.msc`) on the Active Directory computer to look for the different folders in Active Directory and find the account.

| Account type | Name of account | Location of account in Active Directory | Description |
|---|---|---|---|
| Local virtual account | NT SERVICE\MSSQLSERVER (default instance)<br>NT SERVICE\MSSQL$InstanceName (named instance) | CN=Computer<br>CN=<Computer_Name> | Services that run under virtual accounts access network resources by |

| Account type | Name of account | Location of account in Active Directory | Description |
|---|---|---|---|
| | | | using the credentials of the computer account. The default standalone SQL Server service uses this account to start up. |
| Domain account | A domain user name, for example, SQLServerServiceUser | CN=Users<br>CN=<User_Name> | Services started using this account access the network resources using a domain user's credentials. SQL Server failover clusters require a domain account to run the service. The standalone SQL Server service can also be configured to use a domain account to start up. |
| Managed Service account | A Managed Service account name, for example SQLServerMSA | CN=Managed Service Account<br>CN=<Account_ Name> | Introduced in Windows Server 2008 R2, the Managed |

| Account type | Name of account | Location of account in Active Directory | Description |
|---|---|---|---|
| | | | Service Account resembles the domain account, but can be used to perform interactive logons. Both the standalone SQL Server service and the SQL Server cluster services can be configured to use a Managed Service account to start up. |

## Step 2c: Identify which FQDN to use in the SPN

For naming consistency, it is recommended that you set the SPN to the FQDN of the endpoint. The endpoint is the target to which the SQL Server client (Deep Security Manager) connects, and may be an individual SQL Server or a cluster. Consult the table below for details on which FQDN to use.

| If the SQL Server installation type is... | Set the SPN to... |
|---|---|
| Standalone SQL Server | The FQDN of the host where the SQL Server is installed |
| Failover SQL Server cluster | The FQDN of the SQL Server cluster (individual SQL Server nodes are not the endpoint and should not be used in the FQDN) |

## Step 2d: Identify whether you're using a default instance or named instance

You must know whether the SQL Server was installed as a default instance or a named instance because the port number and instance name (if one was specified) need to go into the SPN.

- The default instance typically uses port 1433.
- A named instance uses a different port. To determine this port, consult this webpage.

Example: If the FQDN endpoint of the SQL Server service is `sqlserver.example.com` and it is the default instance, then the SPN will be in the format:

```
MSSQLSvc/sqlserver.example.com
```

```
MSSQLSvc/sqlserver.example.com:1433
```

Another example: If the FQDN endpoint of SQL Server service is `sqlserver.example.com` and it is a named instance using port 51635 with an instance name of `DEEPSECURITY`, then the SPN will be in the format:

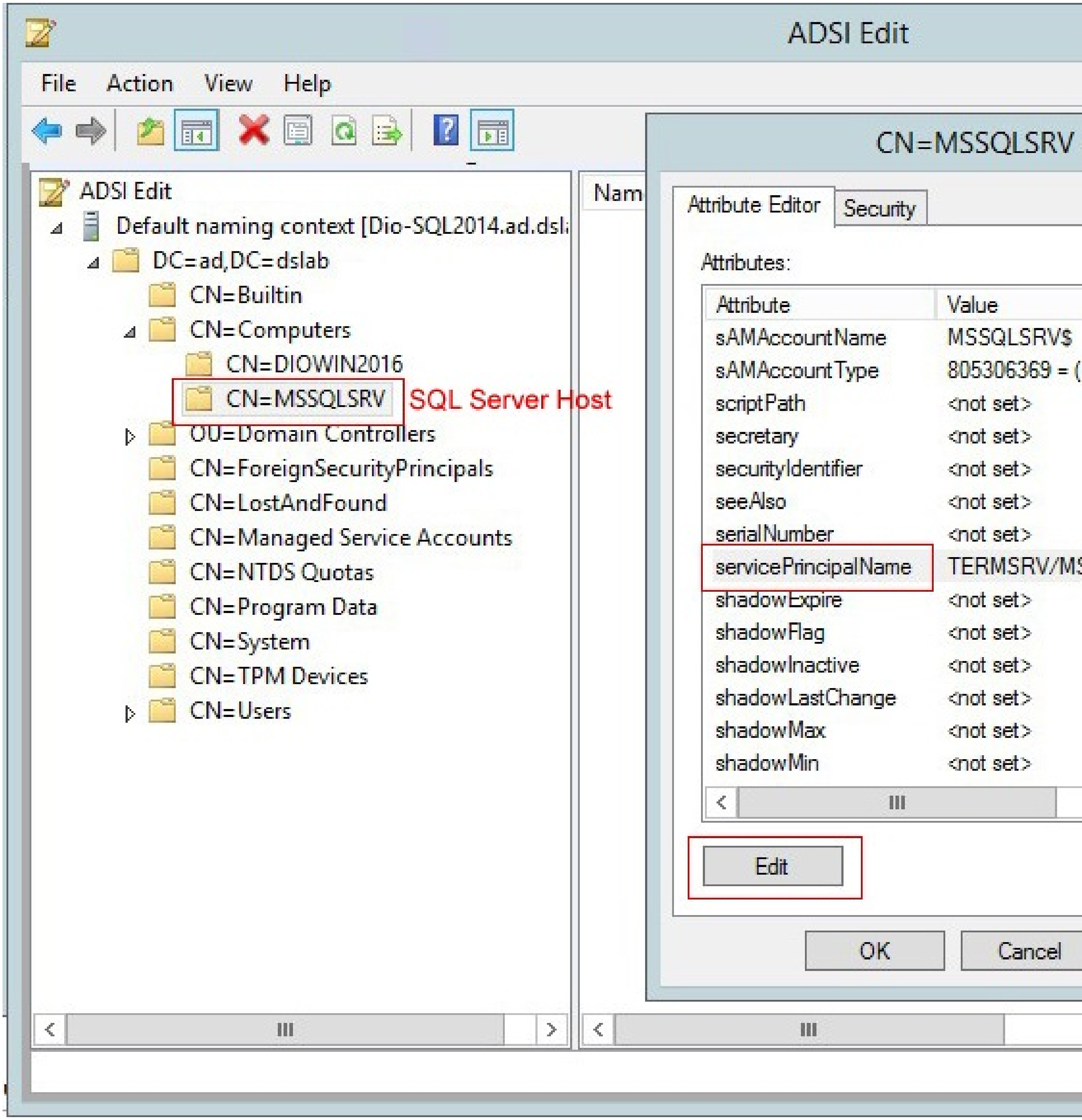
```
MSSQLSvc/sqlserver.example.com:DEEPSECURITY
```

```
MSSQLSvc/sqlserver.example.com:51635
```

## Case 1: Set the SPN under a local virtual account

To set the SPN for a standalone SQL Server that runs under a local virtual account:

1. On the Active Directory computer, open `ADSIEdit.msc`. The ADSI Editor opens.
2. Locate the SQL Server host in **CN=Computers**.
3. Right-click the SQL Server host, and select **Properties**.
4. On the **Attribute Editor** tab, scroll to **servicePrincipalNames** and click the **Edit** button.
5. If the attribute values don't exist, add each one individually using the **Add** button. Click **OK**.

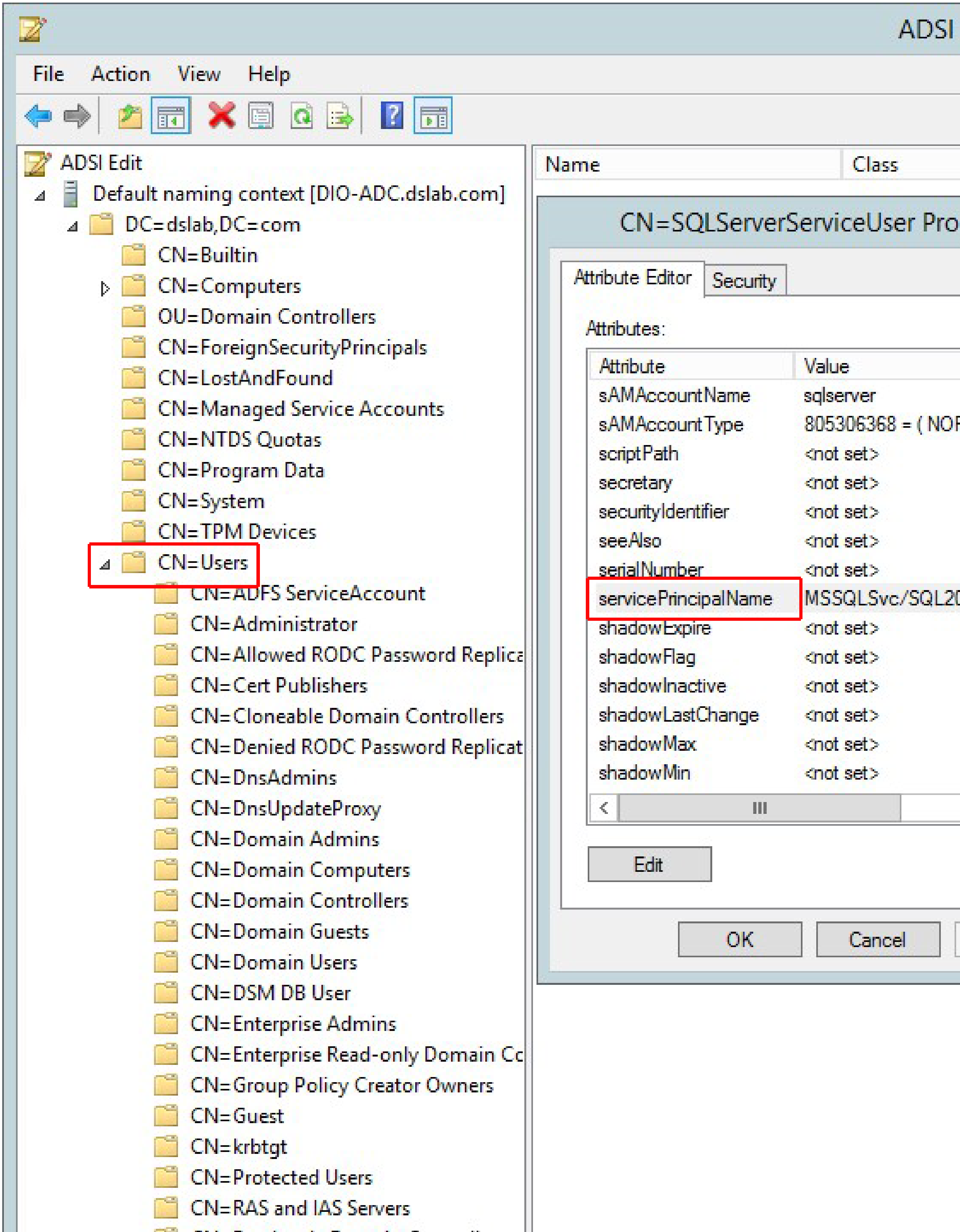


Attributes:

| Attribute | Value |
|---|---|
| sAMAccountName | MSSQLSRV$ |
| sAMAccountType | 805306369 = ( |
| scriptPath | <not set> |
| secretary | <not set> |
| securityIdentifier | <not set> |
| seeAlso | <not set> |
| serialNumber | <not set> |
| servicePrincipalName | TERMSRV/MS |
| shadowExpire | <not set> |
| shadowFlag | <not set> |
| shadowInactive | <not set> |
| shadowLastChange | <not set> |
| shadowMax | <not set> |
| shadowMin | <not set> |

## Case 2: Set the SPN under a domain account

The SPN configuration is similar to the local virtual account configuration except that the SPN is set in domain account (**CN=Users**) running the SQL Server service.



ADSI Edit
- Default naming context [DIO-ADC.dslab.com]
  - DC=dslab,DC=com
    - CN=Builtin
    - CN=Computers
    - OU=Domain Controllers
    - CN=ForeignSecurityPrincipals
    - CN=LostAndFound
    - CN=Managed Service Accounts
    - CN=NTDS Quotas
    - CN=Program Data
    - CN=System
    - CN=TPM Devices
    - CN=Users
      - CN=ADFS ServiceAccount
      - CN=Administrator
      - CN=Allowed RODC Password Replica
      - CN=Cert Publishers
      - CN=Cloneable Domain Controllers
      - CN=Denied RODC Password Replicat
      - CN=DnsAdmins
      - CN=DnsUpdateProxy
      - CN=Domain Admins
      - CN=Domain Computers
      - CN=Domain Controllers
      - CN=Domain Guests
      - CN=Domain Users
      - CN=DSM DB User
      - CN=Enterprise Admins
      - CN=Enterprise Read-only Domain Cc
      - CN=Group Policy Creator Owners
      - CN=Guest
      - CN=krbtgt
      - CN=Protected Users
      - CN=RAS and IAS Servers

| Name | Class |
|---|---|

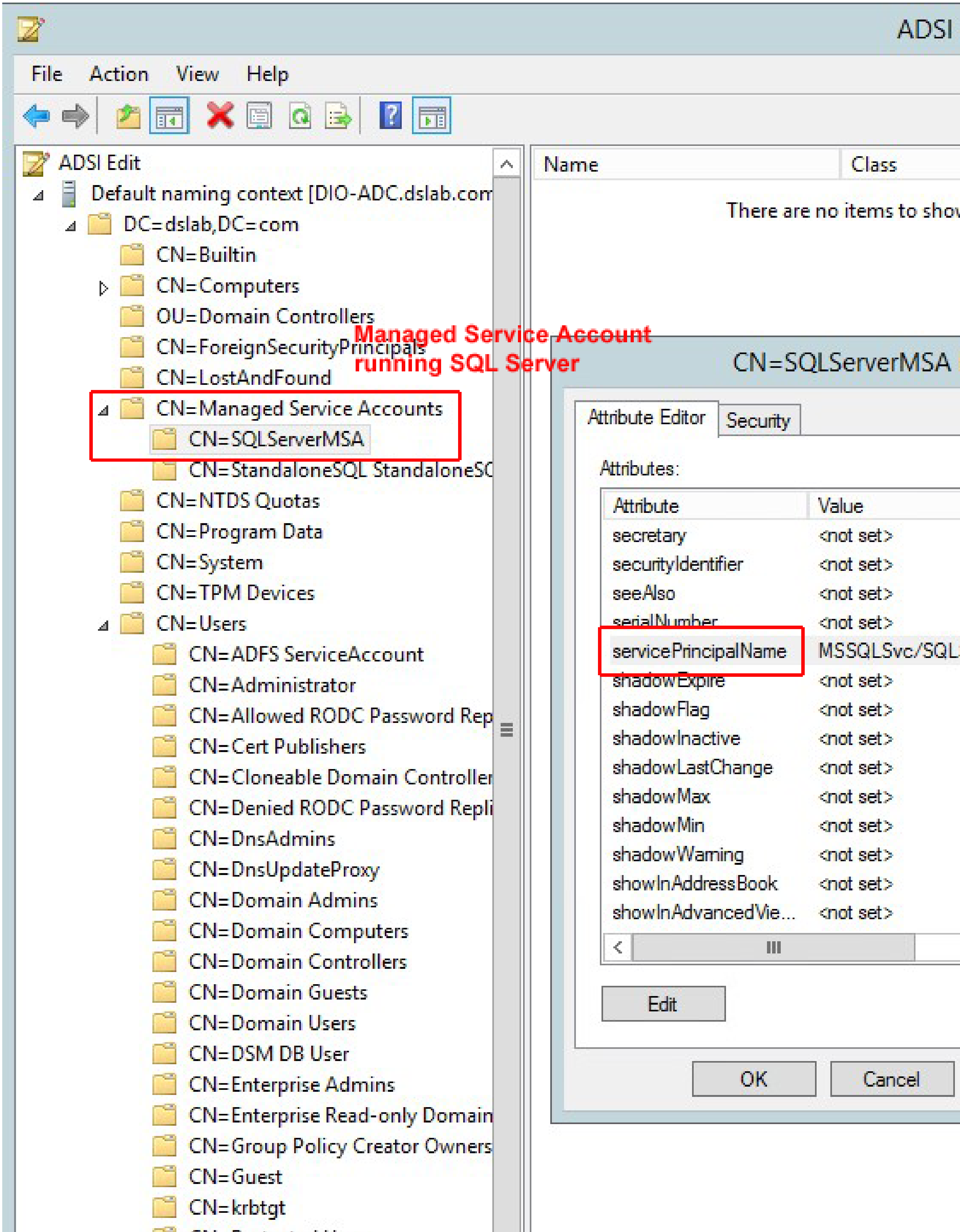
CN=SQLServerServiceUser Pro

Attributes:

| Attribute | Value |
|---|---|
| sAMAccountName | sqlserver |
| sAMAccountType | 805306368 = ( NOF |
| scriptPath | <not set> |
| secretary | <not set> |
| securityIdentifier | <not set> |
| seeAlso | <not set> |
| serialNumber | <not set> |
| servicePrincipalName | MSSQLSvc/SQL20 |
| shadowExpire | <not set> |
| shadowFlag | <not set> |
| shadowInactive | <not set> |
| shadowLastChange | <not set> |
| shadowMax | <not set> |
| shadowMin | <not set> |

## Case 3: Set the SPN under a Managed Service account

The SPN is set in the Managed Service account (**CN=Managed Service Account**) running the SQL Server service.



ADSI Edit
Default naming context [DIO-ADC.dslab.com
DC=dslab,DC=com
CN=Builtin
CN=Computers
OU=Domain Controllers
CN=ForeignSecurityPrincipals
CN=LostAndFound
CN=Managed Service Accounts
CN=SQLServerMSA
CN=StandaloneSQL StandaloneSC
CN=NTDS Quotas
CN=Program Data
CN=System
CN=TPM Devices
CN=Users
CN=ADFS ServiceAccount
CN=Administrator
CN=Allowed RODC Password Rep
CN=Cert Publishers
CN=Cloneable Domain Controller
CN=Denied RODC Password Repli
CN=DnsAdmins
CN=DnsUpdateProxy
CN=Domain Admins
CN=Domain Computers
CN=Domain Controllers
CN=Domain Guests
CN=Domain Users
CN=DSM DB User
CN=Enterprise Admins
CN=Enterprise Read-only Domain
CN=Group Policy Creator Owners
CN=Guest
CN=krbtgt

| Name | Class |
|---|---|

There are no items to show

Managed Service Account running SQL Server

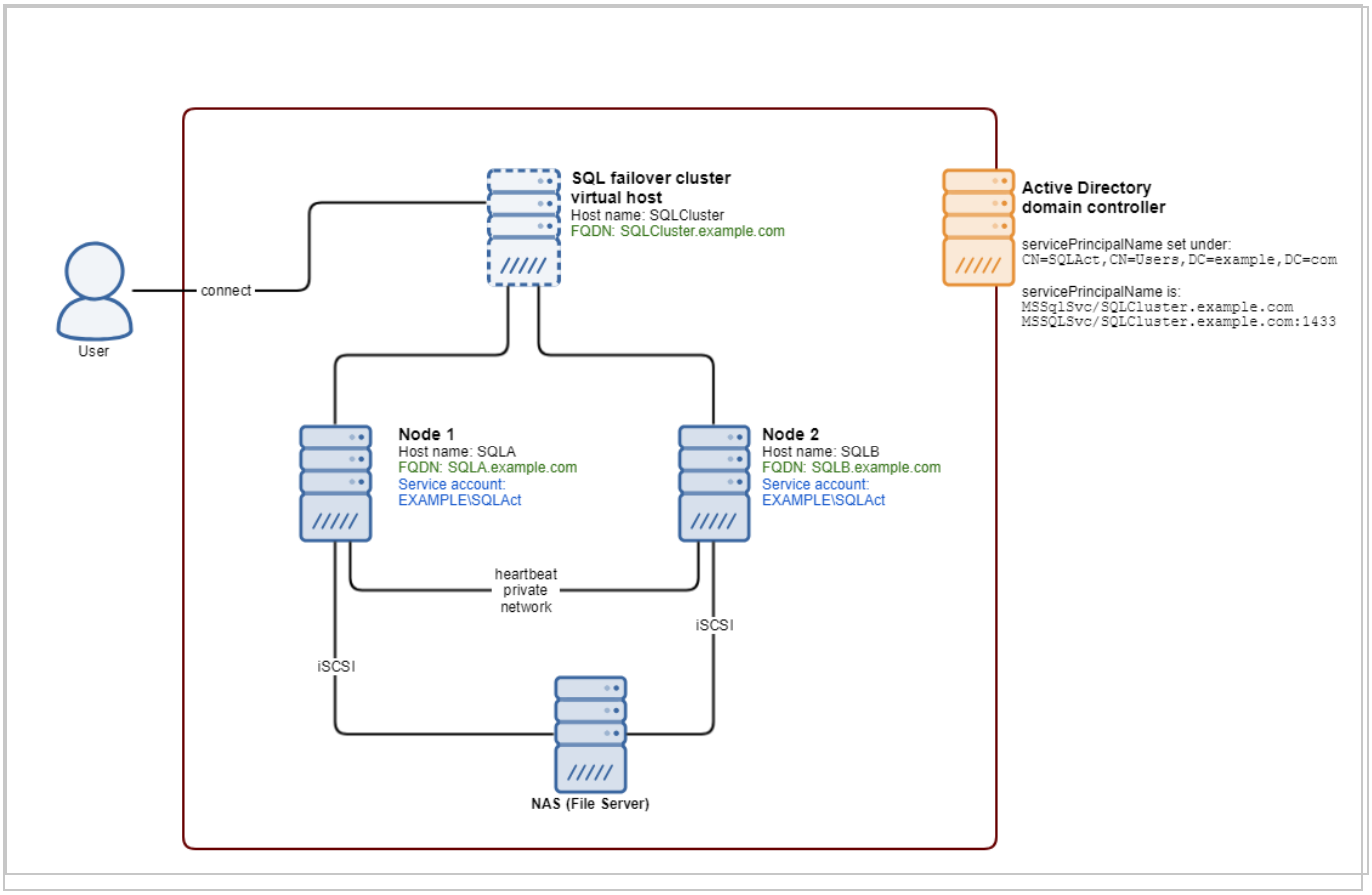
CN=SQLServerMSA

Attributes:

| Attribute | Value |
|---|---|
| secretary | <not set> |
| securityIdentifier | <not set> |
| seeAlso | <not set> |
| serialNumber | <not set> |
| servicePrincipalName | MSSQLSvc/SQL |
| shadowExpire | <not set> |
| shadowFlag | <not set> |
| shadowInactive | <not set> |
| shadowLastChange | <not set> |
| shadowMax | <not set> |
| shadowMin | <not set> |
| shadowWarning | <not set> |
| showInAddressBook | <not set> |
| showInAdvancedVie... | <not set> |

## Case 4: Set the SPN for a failover cluster

An SQL Server failover cluster can run under a domain account or a Managed Service account. Refer to "Case 2: Set the SPN under a domain account" on page 1713 or "Case 3: Set the SPN under a Managed Service account" on page 1715 for instructions. Make sure to set the SPN to the FQDN of the SQL *cluster* endpoint, not an individual SQL node.



## SPN references

Below are links to Microsoft's official documents about SPN configurations:

Register a Service Principal Name for Kerberos Connections

How to: Enable Kerberos Authentication on a SQL Server Failover Cluster

## SPN debugging tips

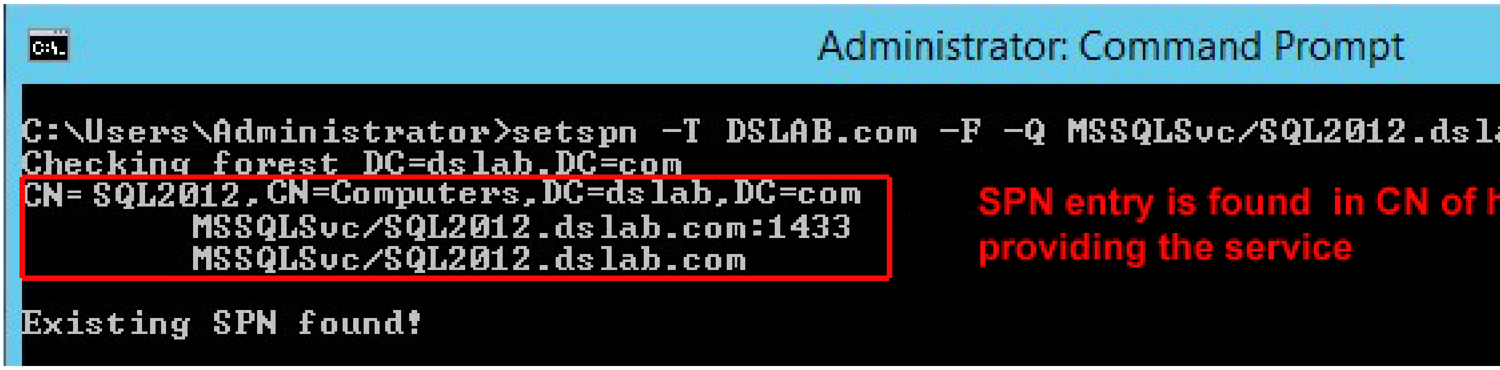
To verify that the correct SPN configuration was set, use the command line tool `setspn` to query for registered SPN entries. The command syntax is:

```
setspn -T <Full_Domain_Name> -F -Q MSSQLSvc/<SQL_Server_Endpoint_FQDN>*
```

where:

- `<Full_Domain_Name>` is replaced with the domain name of your environment.
- `<SQL_Server_Endpoint_FQDN>` is replaced with the FQDN of SQL Server.

For example: Assume that a standalone SQL Server resides at `SQL2012.dslab.com`, and runs under a local virtual account in the domain `dslab.com`. You can use command below to query all registered SPNs that have a prefix of `MSSQLSvc/SQL2012.dslab.com` and see if it is correctly configured.



```
C:\Users\Administrator>setspn -T DSLAB.com -F -Q MSSQLSvc/SQL2012.dsla
Checking forest DC=dslab,DC=com
CN= SQL2012,CN=Computers,DC=dslab,DC=com
        MSSQLSvc/SQL2012.dslab.com:1433
        MSSQLSvc/SQL2012.dslab.com

Existing SPN found!
```

SPN entry is found in CN of h
providing the service

From the command result, you can then verify that the SPN has been set and registered in correct LDAP path, and in the account that is running the SQL Server service (in this case, it is the computer account).

## Step 3: Verify the krb5.conf file (Linux only)

If you're installing the manager on Linux, you must make sure the `/etc/krb5.conf` exists and contains the correct domain and realm information:

1. Open or create the `/etc/krb5.conf` file in a text editor to configure Kerberos.
2. Provide the following information:

```
[libdefaults]
```

```
    ...
    default_realm = <DOMAIN>
    ...
[realms]
    <DOMAIN> = {
        kdc = <ACTIVE_DIRECTORY_CONTROLLER_FQDN>
        admin_server = <ACTIVE_DIRECTORY_CONTROLLER_FQDN>
    }
[domain_realm]
    .<DOMAIN FQDN> = <DOMAIN>
    <DOMAIN FQDN> = <DOMAIN>
```

where `<DOMAIN>`, `<ACTIVE_DIRECTORY_CONTROLLER_FQDN>` and `<DOMAIN_FQDN>` are replaced with your own values.

Example file:

```
[libdefaults]
    default_realm = EXAMPLE.COM
    default_tkt_enctypes = des3-hmac-sha1 des-cbc-crc
    default_tgs_enctypes = des3-hmac-sha1 des-cbc-crc
    dns_lookup_kdc = true
    dns_lookup_realm = false

[realms]
    EXAMPLE.COM = {
        kdc = kerberos.example.com
        kdc = kerberos-1.example.com
        admin_server = kerberos.example.com
    }

```

```
[domain_realm]
    .example.com = EXAMPLE.COM
    example.com = EXAMPLE.COM

[logging]
    kdc = SYSLOG:INFO
    admin_server = FILE=/var/kadm5.log
```

3. Save and close the file.

## Step 4: Verify the system clock

You must make sure the system clocks on the domain controller, SQL Server, and Deep Security Manager computer are synchronized. With Kerberos, the maximum allowable clock skew is five minutes by default.

## Step 5: Verify the firewall

You must make sure the firewall is not blocking the SQL connection. A default SQL Server instance allows connections through port 1433, while a named SQL Server instance uses a port that is selected at random. To find out which port to connect to, the SQL client (Deep Security Manager in this case) queries the available named instances and finds the mapping port by issuing a lookup request to the SQL Server browser service. The SQL Server browser service runs on port 1434 (UDP). Verify that your firewall configuration allows port 1433 (if you're using a default instance), or 1434 (if you're using a named instance).

## Step 6: Verify the dsm.properties file

Make sure the `dsm.properties` file is configured correctly.

1. Open the `dsm.properties` file in a text editor. On Windows, the file is typically located in `C:\Program Files\Trend Micro\Deep Security Manager\webclient\webapps\ROOT\WEB-INF`.

2. Ensure that the file contains these lines:

   `database.SqlServer.server=YOUR-SERVER.EXAMPLE.COM` //Include the domain name, which must use capital letters.

   `database.SqlServer.trustServerCertificate=true` //This line is required when SQL server enables force encrypt.

   `database.SqlServer.domain=EXAMPLE.COM` //Domain name must use capital characters.

   `database.SqlServer.user=sqlUser@EXAMPLE.COM` //The username must include the domain name, and the domain name must use capital letters.

   `database.SqlServer.integratedSecurity=true`

   `database.SqlServer.authenticationScheme=JavaKerberos`

   `database.directory=null`

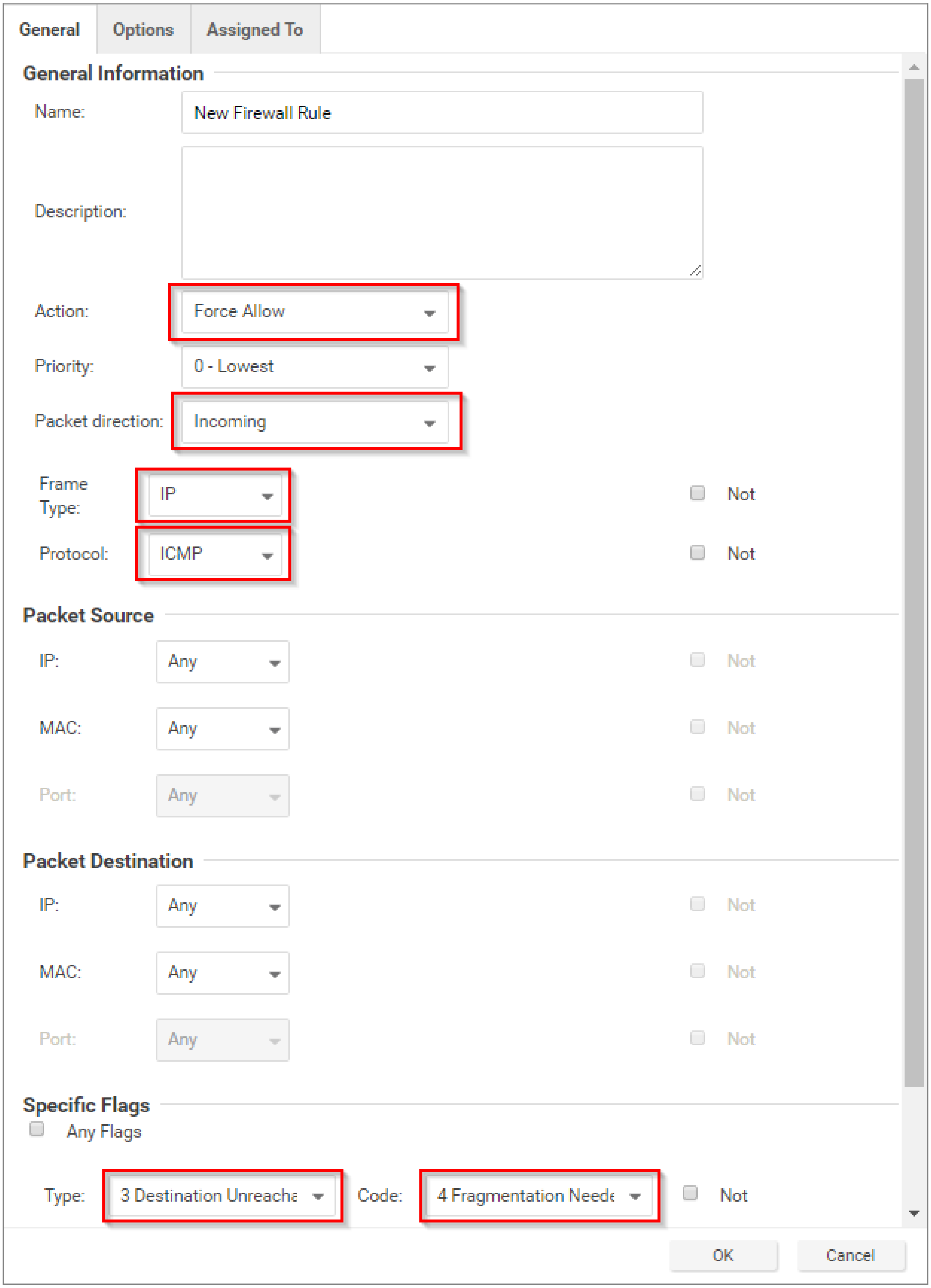
   `database.SqlServer.namedPipe=false`

3. Make any changes required and save the file.

# Prevent MTU-related agent communication issues across Amazon Virtual Private Clouds (VPC)

Agents in different VPCs might experience problems when trying to communicate with Deep Security Manager. This could be because the network maximum transmission unit (MTU) supported by Amazon Web Services is 1500 and Deep Security Agent communication traffic can exceed this, which results in fragmented and dropped packets.

You can prevent this MTU-related communication issue from happening by adding a new firewall rule to all firewall policies. The key settings for this new firewall rule are shown in the image below.



General Information

Name: New Firewall Rule

Description:

Action: Force Allow

Priority: 0 - Lowest

Packet direction: Incoming

Frame Type: IP □ Not

Protocol: ICMP □ Not

Packet Source

IP: Any □ Not

MAC: Any □ Not

Port: Any □ Not

Packet Destination

IP: Any □ Not

MAC: Any □ Not

Port: Any □ Not

Specific Flags

□ Any Flags

Type: 3 Destination Unreacha Code: 4 Fragmentation Neede □ Not

# Create a diagnostic package

To diagnose an issue, your support provider may ask you to send a diagnostic package containing debug information for Deep Security Manager, Deep Security Agent, or both.

## Deep Security Manager diagnostics

The Deep Security Manager (DSM) diagnostics are provided through a diagnostic package, which may include logs, system information, and Java Flight Recorder (JFR) recording.

### Enable debug logs for Deep Security Manager

In addition to a diagnostic package, your support provider may ask you to enable diagnostic logging.

1. Go to **Administration** > **System Information.**
2. Click **Diagnostic Logging**.
3. In the dialog that appears, select the options requested by your support provider.

   If you have a multi-tenant Deep Security Manager, and the issue that you want to diagnose only occurs with a specific tenant, select that tenant's name in the option that appears. This focuses the debug logs and minimizes performance impacts while debug logging is enabled.

   Some functional areas need more time and disk space to collect enough debug logs. For example, you might need to increase **Maximum log file size** to 25 MB and the time period to 24 hours for **Database-related Issues** and **Cloud Account Synchronization - AWS**.

   If you decrease **Maximum number of log files**, Deep Security Manager does not automatically delete existing log files that now exceed the maximum. For example, if you reduce from 10 to 5 log files, `server5.log` to `server9.log` would all still exist. To reclaim disk space, manually delete those files from the file system.

   While diagnostic logging is running, Deep Security Manager displays the message **Diagnostic Logging enabled** on the status bar. If you changed the default options, the status bar displays the message **Non default logging enabled** upon diagnostic logging completion.

4. To find diagnostic logging files, go to the root directory of the Deep Security Manager and look for file names with the pattern `server#.log`, such as `server0.log`.

**Warning:** Do not enable diagnostic logging unless recommended by your support provider. Diagnostic logging can consume large amounts of disk space and increase CPU usage.

## Enable Java Flight Recorder for Deep Security Manager

Java Flight Recorder (JFR) collects information related to the Java Virtual Machine (JVM) internal events. JFR can be used for monitoring and troubleshooting DSM issues. You should enable JFR only when requested by your support provider.

1. Go to **Administration > System Information**.
2. Click **Diagnostic Logging**.
3. In the dialog that appears, select **Enable Java Flight Recorder** and then select the amount of time after which the recording terminates.
4. Optionally, use **Maximum recording file size** to select the upper limit (in megabytes) for the recording file. If the recording data exceeds the allowed size, JFR discards older data.
5. Click **Save** to start recording.

The recording data is saved in a file called **dsm.jfr** located in the DSM installation directory. When the recording is in progress, the **dsm.jfr** file size is 0 MB. Data is only added to the file after the recording is finished. By default, the **dsm.jfr** file is included in the DSM diagnostic package and kept for 7 days. After that the file is removed.

## Create a diagnostic package for Deep Security Manager

1. Go to **Administration > System Information**.

2. Click **Create Diagnostic Package**.

   The package takes several minutes to create. After the package has been generated, a summary is displayed and your browser downloads a ZIP file containing diagnostic information.

# Deep Security Agent diagnostics

For an agent, you can create a diagnostic package in one of the following ways:

- Via the Deep Security Manager
- Using the CLI on a protected computer (if the Deep Security Manager cannot reach the agent remotely)

For Linux-specific information on increasing or decreasing the anti-malware debug logging for the diagnostic package, see "Increase debug logging for anti-malware in protected Linux instances" on page 794.

Your support provider may also ask you collect the following:

- A screenshot of Task Manager (Windows) or output from `top`(Linux) or `prstat` (Solaris) or `topas` (AIX)
- Debug logs
- Perfmon log (Windows) or Syslog
- Memory dumps (Windows) or core dumps (Linux, Solaris, AIX)

## Create an agent diagnostic package via Deep Security Manager

Deep Security Manager must be able to connect to an agent remotely to create a diagnostic package for it. If Deep Security Manager cannot reach the agent remotely, or if the agent is using agent-initiated activation, you must create the diagnostic package directly from the agent.

You can create a diagnostic package using a Deep Security Manager as follows:

1. Go to **Computers**.
2. Double-click the name of the computer for which you want to generate the diagnostic package.
3. Select the **Actions** tab.
4. Under **Support**, click **Create Diagnostics Package**.
5. Click **Next**.

   The package takes several minutes to create. When finished, a summary is displayed and your browser downloads a ZIP file containing diagnostic information.

Note that if **System Information** is enabled, it might create an extremely large diagnostic package that could have a negative impact on performance. The **System Information** option is grayed out if you are not a primary tenant or do not have the required rights.

## Create an agent diagnostic package via CLI on a protected computer

On Linux, AIX, or Solaris:

1. Connect to the server for which you want to generate the diagnostic package.
2. Enter the following command:

   ```
   sudo /opt/ds_agent/dsa_control -d
   ```

   The output shows the name and location of the diagnostic package: `/var/opt/ds_agent/diag`

On Windows:

1. Connect to the computer for which you want to generate the diagnostic package.

2. Open a command prompt as an administrator and enter the command.

   In PowerShell:

   ```
   & "\Program Files\Trend Micro\Deep Security Agent\dsa_control" -d
   ```

   In cmd.exe:

   ```
   cd C:\Program Files\Trend Micro\Deep Security Agent
   ```

   ```
   dsa_control.cmd -d
   ```

   The output shows the name and location of the diagnostic package: `C:\ProgramData\Trend Micro\Deep Security Agent\diag`

## Collect debug logs with DebugView

On Windows computers, you can collect debug logs using DebugView software.

> **Warning:** Only collect debug logs if your support provider asks for them. During debug logging, CPU usage increases, making the high CPU usage issues worse.

1. Download the DebugView utility.
2. If self-protection is enabled, disable it.
3. Stop the Trend Micro Deep Security Agent service.
4. In the `C:\Windows` directory, create a plain text file named `ds_agent.ini`.

5. In the `ds_agent.ini` file, add the following line:

```
trace=*
```

6. Launch `DebugView.exe`.
7. Go to **Menu > Capture**.
8. Enable these settings:
   - **Capture Win32**
   - **Capture Kernel**
   - **Capture Events**
9. Start the Trend Micro Deep Security Agent service.
10. Export the information in DebugView to a CSV file.
11. Re-enable self-protection if you disabled it at the beginning of this procedure.

# Increase verbose diagnostic package process memory

In environments with a large number of hosts (for example, 10,000 hosts or more,) the verbose diagnostic package process (`dsm_c.exe`) may run out of memory while creating the diagnostic package. To prevent this, you can increase the memory allocated to the verbose diagnostic package JVM process to 2 GB.

1. Go to the Deep Security Manager installation directory.
2. Create a new file with the name "dsm_c.vmoptions".
3. Open the file and add the line `-Xmx2g`.

   > **Note:** If 2 GB of memory is not enough, you can further increase the allocated memory by changing the value in the above line (for example, `-Xmx4g` for 4 GB or `-Xmx6g` for 6 GB).

4. Save the file and run `dsm_c.exe`.

# Removal of older software versions

In certain situations, we may determine that it's in the best interest of our customers to remove access to a previously released version of software. We only remove software when there is a significant known issue with that release. This is done to limit customer exposure to known problems.

When access to an old software version has been removed, the download link is replaced with a link to a Knowledge Base article detailing the issue that caused us to remove the software.

If you require access to an older version that has been removed, contact support with the software version and Knowledge Base number.

# Troubleshoot Azure code signing

Since Microsoft Windows Agent components are now signed with Azure Code Signing (ACS), computers running earlier versions of Windows need to be updated with the Microsoft KB5022661 patch to be able to identify Azure Code Signing certificates. If this patch has not been applied, the Deep Security Agent installation or upgrade is expected to fail and the Deep Security Manager will display a warning to that effect.

The following is a part of the Deep Security Agent log produced during a failed upgrade:

```
MSI (s) (E8:24) [01:16:53:747]: Executing op: ActionStart(Name=_ACSVerification,,)
MSI (s) (E8:24) [01:16:53:747]: Executing op:
CustomActionSchedule(Action=_ACSVerification,ActionType=1025,Source=BinaryData,Targ
Verification,CustomActionData=C:\Program Files\Trend Micro\Deep Security Agent\)
MSI (s) (E8:B0) [01:16:53:747]: Invoking remote custom action. DLL: C:\Windows\Inst
\MSIFC3A.tmp, Entrypoint: ACSVerification
ds_agent [01:16:53:763]: Azure Code Sign Verification Begin ...
ds_agent [01:16:53:763]: Installation property TARGETDIR is C:\Program Files\Trend
Micro\Deep Security Agent\
ds_agent [01:17:05:616]: Azure Code Sign (ACS) Verification Failed (error: 0x577).
for ACS is probably required.
CustomAction _ACSVerification returned actual error code 1603 (note this may not be
accurate if translation happened inside sandbox)
Action ended 1:17:05: InstallFinalize. Return value 3.
```

The following is a part of the Deep Security Manager system event log produced during a failed upgrade:

```
After 2023/2/18, agent components on Windows will use Azure Code Signing. If you us
older Windows version, then you must apply the patch in Microsoft KB5022661 so that
Windows can validate the certificate. Agent installations and upgrades will fail if
do not apply the update. Consult the install log for the running process:
```

For more information, see Trend Micro Server and Endpoint Protection Agent minimum Windows version requirements for updated binaries after February 2023.

# Troubleshoot IoT event overloaded alert

The IoT event Fully overloaded alert (Error: Activation Failed) appears in Deep Security when Deep Security Manager is taking longer than usual to process IoT events.

To resolve this issue, check for Deep Security Agent(s) unexpectedly producing a large number of security events:

- Check the security events in **Events & Reports** to see if any computers are generating a lot of events.
- Check those computers for misconfigured rules.

If the problem is still unresolved, contact support.

# Troubleshoot SELinux alerts

To check if SELinux is enabled, use the `sestatus` command.

## SELinux blocks the Deep Security Agent service

When the SELinux policy is set to enable and it blocks the Deep Security Agent service, the following alert sample might appear in the system audit log `/var/log/audit/audit.log` or SELinux log `/var/log/audit.log`:

```
[TIMESTAMP] [HOSTNAME] python: SELinux is preventing [/PATH/BINARY] from 'read, write' accesses on the file /var/opt/ds_agent/dsa_core/ds_agent.db-shm.

***** Plugin leaks (86.2 confidence) suggests *****************************

If you want to ignore [BINARY] trying to read write access the ds_agent.db-shm file because you believe it should not need this access. Then you should report this as a bug.

You can generate a local policy module to dontaudit this access.

Do

ausearch -x [/PATH/BINARY] --raw | audit2allow -D -M [POLICYNAME]
```

```
semodule -i POLICYNAME.pp
```

To resolve the issue, create a custom SELinux policy with Audit2allow, as follows:

1. Connect to the Deep Security Agent system as a root user.
2. Run the following commands to create a custom policy that will allow access to Deep Security Agent files:

   ```
   cd /tmp

   grep ds_agent /var/log/audit/audit* | audit2allow -M ds_agent

   semodule -i ds_agent.pp
   ```

3. Restart the `ds_agent` service.
4. Execute the following command to check the system messages and confirm that there are no alerts related to `ds_agent`.

   ```
   cat /var/log/messages | grep ds_agent
   ```

5. If alerts still occur, rerun the commands from step 2 to update and reapply the existing policy.

To remove the SELinux policy, use the following command:

`semodule -r ds_agent`.

## Berkeley Packet Filter (BPF) operations blocked

This issue can occur under the following conditions:

- The agent OS is Red Hat Enterprise Linux 7 (64-bit).
- SELinux is enabled in enforcing mode.
- The Advanced TLS Traffic Inspection feature is enabled on the agent.

An alert similar to the following might appear in the system audit log `/var/log/audit/audit.log` or SELinux log `/var/log/audit.log`:

```
type=AVC msg=audit(1682773485.952:1080): avc: denied { map_create } for pid=12807 comm="ds_nuagent" scontext=system_u:system_r:unconfined_service_t:s0 tcontext=system_u:system_r:unconfined_service_t:s0 tclass=bpf permissive=0
```

```
type=SYSCALL msg=audit(1682773485.952:1080): arch=c000003e syscall=321 success=no exit=-13
a0=0 a1=c000a25800 a2=2c a3=0 items=0 ppid=12802 pid=12807 auid=4294967295 uid=0 gid=0
euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=(none) ses=4294967295 comm="ds_nuagent"
exe="/opt/ds_agent/nuagent/ds_nuagent" subj=system_u:system_r:unconfined_service_t:s0 key=(null)
```

To resolve the issue, follow these steps to create a custom SELinux policy:

1. Connect to the Deep Security Agent system as a root user.
2. Create a Type Enforcement file named `nuagent.te`:

   ```
   module nuagent 1.0;

   require {

   type unconfined_service_t;

   class bpf { map_create map_read map_write prog_load prog_run };

   }

   #============= unconfined_service_t ==============

   allow unconfined_service_t self:bpf { map_create map_read map_write prog_load prog_run };
   ```

3. Run the following commands to create a custom policy that allows bpf access for `ds_nuagent`:

   ```
   checkmodule -M -m -o nuagent.mod nuagent.te

   semodule_package -o nuagent.pp -m nuagent.mod

   semodule -i nuagent.pp
   ```

4. Restart the `ds_agent` service.

Note that Deep Security Agent version 20.0.0-8137+ added support for a new process called `tm_netagent`. The `ds_nuagent` process is still supported and the process names can be used interchangeably.

# Network Engine Status (Windows OS)

## Network Engine Status warnings

Network Engine Status warnings are a collection of warnings and errors that might appear in the Status area of a computer when the agent raises an event about the Trend Micro LightWeight Filter Driver and the Network Engine Status Check is enabled.

If you receive one of the following warnings, the network functionality might be disabled or impaired on the agent:

- Web Reputation Engine Disabled
- Firewall Engine Disabled
- Intrusion Prevention Engine Disabled
- Web Reputation Engine Working With Limited Functionality
- Firewall Engine Working With Limited Functionality
- Intrusion Prevention Engine Working With Limited Functionality

Agents display more security events for each affected network interface. See Driver-Related Events for more information.

## Verify the driver status

You can verify the driver status as follows:

1. Open **Control Panel > Network and Internet > Network and Sharing Center**.
2. Select **Change adapter settings** on the left to open **Network Connections**.
3. Right-click each active network adapter and select **Properties**.
4. Verify that **Trend Micro LightWeight Filter Driver** is selected.

## Disable Network Engine Status warnings

You can disable Network Engine Status warnings as follows:

1. On Deep Security Manager, navigate to **Computers**.
2. Select the computer for which you want to disable the warning, and then click **Details**.
3. In the computer details, navigate to **Settings > Advanced > Network Engine Settings**.
4. For **Network Engine Status Check**, select **Disabled**.

# PDFs

## Deep Security Administration Guide

The Deep Security Administration Guide is a PDF version of the Deep Security Help Center:

Open the Deep Security Administration Guide

## Deep Security Best Practice Guide

The Deep Security Best Practice Guide is intended to help you get the best productivity out of the product. It contains a collection of best practices that are based on knowledge gathered from previous enterprise deployments, lab validations, and lessons learned in the field. Examples and considerations in this document serve only as a guide and not a representation of strict design requirements. These guidelines do not apply in every environment but will help guide you through the decisions that you need in configuring Deep Security for optimum performance.

The Deep Security 20 Best Practice Guide is currently available in PDF format and includes the following:

- Deployment considerations and recommendations
- Upgrade guidelines and scenarios
- Sizing considerations and recommendations
- Recommended configurations to maximize system performance and reduce administrative overhead
- Best practice tips for VDI, private, and public cloud environments