TREND MICRO™

Deep Security as a Service Guide

Legal notices

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the release notes and the latest version of the applicable user documentation, which are available from the Trend Micro Web site at:

https://help.deepsecurity.trendmicro.com/software.html

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: APEM128608/190306

Publication Date: 9/16/2020 1:27 PM

Contents

About Deep Security

Deep Security Trust Center

As a global leader in security, Trend Micro develops innovative security solutions that make the world safe for businesses and consumers to exchange digital information. With more than 30 years of security expertise, we're recognized as the market leader in server security, cloud security, and small business content security.

Trend Micro Deep Security as a Service provides world-class security to cloud workloads. This offering is hosted through Amazon Web Services (AWS) and offers workload protection through the installation of Deep Security Agents.

Deep Security as a Service is committed to earning and preserving the trust of our customers. The following resources demonstrate our commitment to security, privacy, transparency, and compliance to industry-recognized standards.

 Compliance	 Privacy	 Security
"PCI DSS " below "ISO 27001 " on the next page	"GDPR" on the next page Deep Security as a Service Data Collection Notice Privacy Policy	"FAQ" on the next page

PCI DSS

Deep Security as a Service is certified as a PCI DSS level 1 service provider.

Coalfire, a Qualified PCI Auditor, has certified Deep Security as a Service according to version 3.2 of the PCI Data Security Standard. The Attestation of Compliance is available on request. AWS is also PCI certified.

For more information, see "Meet PCI DSS requirements with Deep Security" on page 1034.

ISO 27001

ISO 27001 is an internationally recognized security standard that outlines the requirements for information security management systems. Deep Security as a Service has been added to the Trend Micro ISO 27001 certification, as of December 2018. You can view the ISO 27001 certificate on the Trend Micro product certifications site.

GDPR

Trend Micro and Deep Security as a Service were ready for, and have met, all of our obligations under GDPR for May 25th 2018. One key item to note for Deep Security as a Service is that, as a data processor under GDPR, our processing of 'personal data' is limited.

- Where appropriate, we implement Technical and Organization Measures (“TOMs”) to support our processing of data under GDPR.
- Details on the data processed by Deep Security as a Service, and the controls available to you over that data, are documented in the Deep Security as a Service Data Collection Notice.

For more information, see the Trend Micro GDPR Compliance site and see "Privacy and personal data collection disclosure" on page 1040 for information about personal data collection in Deep Security as a Service.

FAQ

How are security logs monitored?

> Deep Security protection modules generate security events for the Deep Security as a Service production workloads. Security events collected from Deep Security as a Service are forwarded to a central SIEM. Security events are generated for all relevant protection modules: Anti-Malware, Firewall, Intrusion Prevention, Integrity Monitoring, Log Inspection. Additional AWS logs (CloudTrail, CloudWatch), system, and database logs are forwarded to the SIEM. Access to Deep Security event management console and SIEM is restricted based on roles.
>
> Deep Security as a Service enables automated alerts and employs 24/7 on-call staff. Security logs are reviewed for all systems on a daily basis. If a security incident is

suspected, it is immediately reported to the Trend Micro Security Operations Center (SOC). This potential incident is prioritized based on the severity of the suspected incident, and a team from the SOC, as well as technical experts, is assigned to investigate.

How are Trend Micro employees trained?

All Trend Micro employees undergo a security awareness training course upon being hired and on a yearly basis. All employees must adhere to Trend Micro's Internet, Computer, Remote Access and Mobile device acceptable use policies. Failure to comply with these policies may result in disciplinary actions which could include termination.

All new employees and contractors are required to complete a criminal background check.

What are Trend Micro's password policies and standards?

Trend Micro adheres to the following password polices and standards:

- All passwords must be changed at least on a quarterly basis.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords must not be shared or revealed to anyone.
- Passwords must be changed immediately if compromise is suspected.
- Passwords must be encrypted during transmission and stored hashed with a salt.
- Passwords must be at least eight alphanumeric characters long.
- Passwords must contain both upper and lower case characters (for example, a-z, A-Z).
- Password reuse prevention is enforced.
- Passwords must not be based on personal information, names of family, and so on.

How is access to Trend Micro's infrastructure controlled?

Remote access to Trend Micro's infrastructure is strictly controlled and monitored. All authentication methods use industry best practices and standards, and include such things as certificate based authentication and multi-factor authentication. Where appropriate, single sign-on (SSO) that leverages Trend Micro's Active Directory is used.

How does Trend Micro handle sensitive information?

In relation to the Deep Security as a Service environment, Trend Micro primarily handles data that is collected through the protection policy and security events. Each tenant's information is separated using a dedicated database schema. Access and storage of this information is strictly controlled and is used for diagnostic and support purposes only. Client contact details, such as their email address, are retained encrypted at rest for client management purposes.

What change control practices does Deep Security as a Service follow?

Application upgrades within the Deep Security as a Service environment are completed after meeting our quality objectives. Trend Micro uses best practices for changes, including full backups and approval processes. Deep Security as a Service has multiple dedicated development and testing environments.

Any changes requested are first reviewed by technical stakeholders to determine the urgency and potential impact of the changes. All changes require a documented back-out plan. These changes are tracked and recorded in a change control system.

How is communication secured?

All communication between customers, software, and infrastructure is encrypted using industry-accepted ciphers and algorithms. These ciphers and algorithms are reviewed continuously to determine whether adjustments should be made, such as the deprecation of old or insecure ciphers and cipher suites. To take advantage to these improvements, customers must ensure that their agents are updated regularly.

Encryption keys are stored in AWS KMS. Only a limited number of Deep Security as a Service team member have access to the KMS.

How does Trend Micro handle physical security?

All access to Trend Micro offices and networks is strictly controlled to authorized or accompanied individuals only. Access is given through a key card system and approval is required before entry is granted into sensitive areas. The Deep Security as a Service infrastructure is hosted in AWS.

What is the Trend Micro incident response plan?

Trend Micro has a dedicated Information Security (InfoSec) team that is responsible for ensuring compliance with Trend Micro security policies. Deep Security as a Service engineers immediately contact the InfoSec team when a security incident is discovered. In addition, InfoSec independently monitors Deep Security as a Service environment logs.

If a security incident is discovered, the incident is prioritized based on severity. A dedicated team of technical experts is assigned to investigate, advise on containment procedures, perform forensics, and manage communication.

Following an incident, the team examines the root cause, and revises the response plan accordingly.

In the event of a breach involving customer data, Trend Micro will follow its obligations under GDPR. For more information, see https://www.trendmicro.com/en_ca/business/capabilities/solutions-for/gdpr-compliance/our-journey.html.

Does Deep Security as a Service conduct vulnerability and penetration testing?

Vulnerability scans of the Deep Security as a Service production environment are performed weekly by a PCI authorized scanning vendor (ASV), Tenable.io. A PCI ASV attestation is obtained quarterly. The same vendor is used for automated weekly internal scans of the Deep Security as a Service Virtual Private Cloud (VPC).

Deep Security software and the Deep Security as a Service production environment undergo yearly penetration tests conducted by third-party security experts to detect and rectify common security issues. The scope of the third-party penetration tests includes application security tests, internal and external network scans, and network segmentation tests.

Trend Micro InfoSec conducts web application assessments of the Deep Security Manager application for any major release and at least annually using leading dynamic analysis security tools.

The Deep Security code base is scanned weekly using a leading static analysis security tool. The development team receives automated alerts if new issues are identified, and a clean scan is a requirement for each product release.

Third-party components included with Deep Security are monitored continuously using a leading software composition analysis tool. Scans are executed as part of nightly builds to automatically detect newly introduced third-party software.

Does the development team follow secure coding practices?

Deep Security software developers are trained in secure coding practices using an industry-standard curriculum based on SANS 25/OWASP Top 10/PCI 6.5. Education campaigns are conducted on an annual basis and when an employee joins the company.

The Deep Security development team employs specialized staff to handle product security.

Security testing, secure code review, and threat modeling are part of the development lifecycle.

How are vulnerabilities and patches handled?

Vulnerabilities are continuously monitored and tracked. Each vulnerability is assigned a CVSS score. Patching requirements that specify time frames for addressing a vulnerability according to CVSS-based severity are included in the Secure Development Compliance Policy. The Deep Security software in the Deep Security as a Service environment is updated weekly to use the latest available code base, including vulnerability fixes.

The Deep Security as a Service team is responsible for patching the Deep Security software and supporting AWS services. The client is responsible for updating the Deep Security Agents deployed on client workloads.

Deep Security 20 release strategy and life cycle policy

Deep Security 20 is a long-term support release (LTS).

There are a number of changes to Deep Security 20 release management and life cycle that make working this release easier for our customers and partners:

- Deep Security 20 updates will include both new content and fixes to ensure we deliver new features to our customers with increased velocity.
- To reduce the number of software releases and simplify understanding of the support policy, we are no longer releasing Feature Releases (FR).
- Standard Support and Extended Support Services are now closely aligned to provide a more consistent support experience from day 1 to the end of life of the release.

We encourage you to update your software on a regular basis. Software updates provide additional features, security updates, performance improvements, and updates to stay in sync with updates from other software in your data center or cloud ecosystem. Keeping software updated regularly also ensures that, if support is required, you have a supported upgrade path to any updates that contain necessary fixes.

Supported upgrade paths

Deep Security supports upgrades from the last 2 major releases for all Deep Security software components (Deep Security Manager, Deep Security Agent, and Deep Security Relay).

You can upgrade to Deep Security 20 from these older versions:

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

Deep Security 20 supports upgrading to new LTS Update releases, but rolling back to a previous release is not supported.

Deep Security 20 updates

Consistent with previous LTS releases, Deep Security 20 updates will be released monthly. If the need arises, typically due to critical fixes or vulnerabilities, more frequent releases will be provided.

If a software fix is required on an actively supported release of software, we will make an update available that can be applied directly to the software release within the active support period. For example, if you are running Deep Security 20 Update 2 and have an issue, when the latest update is released (for example Deep Security 20 Update 10) you can update directly from Update 2 to Update 10 to ensure that you can resolve issues quickly and easily.

LTS release support duration and upgrade best practices

A key best practice for software updates is to ensure you have a well defined, regularly scheduled, and, ideally, automated process in place that ensures all components are updated regularly.

The following table summarizes when updates are released, the support duration of that component, and considerations when designing your upgrade strategy.

Component	When are updates released?	Support	Upgrade considerations
Deep Security Agent	LTS updates are released monthly	Standard support until 3 years after GA. Extended support until 4 years after GA.	LTS agents support upgrades from the last 2 major releases (for example Deep Security Agent 11.0 to Deep Security Agent 20 LTS). Plan to upgrade regularly to ensure that you remain on a supported release and are able to upgrade to the latest software with a single upgrade.
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 "Deep Security Agent platforms" on page 80.
Deep Security Relay	LTS updates are released	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.

Component	When are updates released?	Support	Upgrade considerations
	monthly		

Support services

The following table indicates which support items are available during the life cycle of Deep Security 20.

Support item	LTS - standard support	LTS - extended support (*)	Delivery mechanism
New features	✔	✔	LTS update
Small enhancements (no change to core functionality)	✔	✔	LTS update
Linux kernel updates	✔	On request	Linux Kernel Support Package (LKP)
General bug fixes	✔	✔	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	✔	✔	LTS update

Support item	LTS - standard support	LTS - extended support (*)	Delivery mechanism
systems			

(*) Extended support is provided to all customers at no additional charge.

Agent platform support policy

Deep Security Agent software is released multiple times a year, as described above. Agent platforms (operating systems) are supported according to the policy below. We recognize that in some cases you must commit to platforms for many years. This policy is designed to provide predictability when you deploy Deep Security in these environments:

- The agent is supported on a large range of platforms, as shown in the "Agent platform support table" on page 80.
- The support duration of any individual release of agent software is described in the tables above. For example, you'll receive 3 years of standard support and 4 years of extended support for LTS releases of the agent (11.0, 12.0, and so on). In cases where you plan to use an OS platform for an extended period of time, you must also plan to upgrade the agent software on a regular basis to stay within the support life cycle for any specific Deep Security software release. In cases where an older agent is recommended for a given platform, this agent will be considered a part of the overall solution and takes on the support dates for the release in which it is contained. See the bullet below for details.
- Platforms continue to be supported until at least the OS vendor's end-of-extended-support date. Where interest dictates, Trend Micro extends support significantly beyond this date.
- To ensure that you have the latest performance and security updates from your OS vendor, Trend Micro strongly encourages you to move to the latest version of the OS for which an agent is available.
- We strive to release a new version of the Deep Security Agent for all supported platforms. However, in some cases we recommend the use of a previous release of the agent to provide coverage for older platforms. For example, with Deep Security 11.0, the latest agent for Windows 2000 is Deep Security Agent 9.6. This 9.6 agent becomes part of the overall 11.0 Deep Security solution and takes on the support dates for the release in which it is contained.

- You'll always receive advance warning if we end support for a platform, and we'll never shorten the support life cycle of a software release post-General Availability (GA).*

* *Once a platform is no longer supported by the OS vendor, there is a risk that a technical issue arises that cannot be fixed without the support of the OS vendor. If this situation occurs, Trend Micro will communicate the limitation to you immediately. Note that this situation may result in loss of functionality. We will do our best to deal with any technical issues if they arise.*

Deep Security life cycle dates

Deep Security LTS 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.

Deep Security Manager supports the use of older agent versions (see "Deep Security Agent platforms" on page 80), but we do encourage customers to upgrade agents regularly. New agent releases provide additional security features and protection, higher quality, performance improvements, and updates to stay in sync with releases from each platform vendor.

You can find more information in the "Deep Security 20 release strategy and life cycle policy" on page 60. For feature releases, see "Deep Security FR life cycle dates" on page 68

Note: Products for the Japan region are handled under a region-specific policy.

Deep Security LTS release life cycle dates

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

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 (EOL)	Extended support was introduced in Deep Security 10.0. See the Trend Micro End-of-Life Policy for terms and definitions.
Deep Security 9.5	All	All	13-Aug-2014	17-Aug-2018 (EOL)	
Deep Security 9.6	All	All	12-Aug-2015	12-Aug-2019 (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 20.0	All	All	30-Jul-2020	30-Jul-2023	30-Jul-2024

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	30-Jul-2023 *	Deep Security Windows 2000 Platform Support Update. Updated the guidance on how to use Trend Micro Deep Security to protect Windows 2003, Windows XP, and Windows 2000 based systems Support will continue as defined in the "Agent platform support policy" on page 63
Windows 2003	Agent	Deep Security 10.0	30-Jul-2023 *	Deep Security Windows 2003 Platform Support Update. Updated the guidance on how to use Trend Micro Deep Security to protect Windows 2003, Windows XP, and Windows 2000 based systems Support will continue as defined in the "Agent platform support policy" on page 63
Windows XP	Agent	Deep Security 10.0	30-Jul-2023 *	Updated the guidance on how to use Trend Micro Deep Security to protect Windows 2003, Windows XP, and Windows 2000 based systems Support will continue as defined in the "Agent platform support policy" on page 63
AIX	Agent	Deep	31-	Deep Security AIX Platform Support Update

Platform	Component	Version	Updated end of life (EOL)	More information
		Security 9.0	Dec-2020	
CloudLinux 5 (32- and 64-bit)	Agent	Deep Security 9.6	30-Jul-2023 * –	Support will continue as defined in the "Agent platform support policy" on page 63
Cloud Linux 6 (32-bit)	Agent	Deep Security 10.0	30-Jul-2023 * –	Support will continue as defined in the "Agent platform support policy" on page 63
Cloud Linux 6 (64-bit)	Agent	Deep Security 11.0	30-Jul-2023 * –	Support will continue as defined in the "Agent platform support policy" on page 63
Debian 6	Agent	Deep Security 9.6	30-Jul-2023 * –	Support will continue as defined in the "Agent platform support policy" on page 63
Oracle Linux 5	Agent	Deep Security 10.0	20-Jun-2023 * –	Support will continue as defined in the "Agent platform support policy" on page 63
Red Hat Enterprise Linux 5	Agent	Deep Security 10.0	30-Jul-2023 * –	Support will continue as defined in the "Agent platform support policy" on page 63
SUSE Linux Enterprise Server 10 SP3, SP4 (32- and 64-bit)	Agent	Deep Security 9.6	23-May-2021	Deep Security SuSE Enterprise Linux 10 Platform Support Update
Ubuntu 10, 12	Agent	Deep Security 9.6	30-Jul-2023 * –	Support will continue as defined in the "Agent platform support policy" on page 63
Ubuntu 14	Agent	Deep Security 10.0	30-Jul-2023 * –	Support will continue as defined in the "Agent platform support policy" on page 63

* At this time, there are no plans to end support for this platform. This platform is currently supported using an older version of Deep Security Agent. The EOL date will be revisited and updated for this specific agent-platform combination with each annual long-term release of Deep Security. Please see the "Agent platform support policy" on page 63 for more detail.

Archive of past support extensions

The following table lists support extensions that are now expired.

Platform	Component	Version	Updated end of life (EOL)	More information
All	Appliance	Deep Security 9.5	12-Aug-2019	The 9.5 Deep Security Virtual Appliance's embedded agent must be at version 9.6 to adopt this EOL date. If you do not upgrade the embedded agent to 9.6, then an EOL date of **August 17, 2018** applies. Upgrading the embedded agent beyond 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 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	Deep Security Solaris Platform Support Update
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

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, we are no longer releasing Feature Releases (FR) after the release of Deep Security 20. See "Deep Security 20 release strategy and life cycle policy" on page 60.

Note: Products for the Japan region are handled under a region-specific policy.

Deep Security FR release life cycle dates

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

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
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

Version	Component	Platform	Build number	GA date	End of support
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

Version	Component	Platform	Updated end of life	More information
Deep Security 11.1, 11.2, 11.3	Deep Security Agent Linux Kernel Updates	Linux	31-Dec-2020	Extending Linux kernel updates for Deep Security 11.1, 11.2, 11.3 Feature Release Agents

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 System Tray 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 " below
- "Firewall " on the next page
- "Web Reputation " on the next page
- "Integrity Monitoring " on the next page
- "Log Inspection " on the next page
- "Application Control" on page 74

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 370.

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 319.

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 409.

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 361.

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 449.

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.

For more information, see "Set up Log Inspection" on page 507.

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 549.

About billing and pricing

Topics in this section:

Billing methods

The billing methods available to you depend on your deployment type. For details, see the table below and the descriptions below the table.

		Billing type							
		Metered					BYOL	Free tier	
		AWS subscription		Azure subscription	Prepaid credit	Credit card		30-day trial	5 instance unlimited
		Pay as you Go	Annual + Pay as you Go	Pay as you Go					
Deployment type	On-premise						•		
	AMI from AWS Marketplace	•					•		
	VM for Azure Marketplace						•		
	Deep Security as a Service	•	•	•	•	o	o	•	•

• = supported
o = supported for existing deployments only

Metered billing

You are billed based on the number of hours your computers are protected with Deep Security. These are known as 'protection-hours'. Pricing for metered billing depends on the type of metered billing you choose.

Bring-your-own license (BYOL)

You are billed based on a license that you pre-purchase from Trend Micro. For BYOL pricing, please contact the Deep Security Support team.

Free tier billing

There are two free options:

- A 30-day trial. You are given unlimited access to Deep Security as a Service for 30 days.
- 5 instance unlimited: You are given unlimited access to Deep Security as a Service with a 5 agent maximum. You are placed automatically in the '5 instance unlimited' category when your 30-day trial lapses, or when you cancel your metered or BYOL billing.

AWS subscription billing

Your Amazon Web Services (AWS) account is billed.

Azure subscription billing

Your Azure account is billed.

Pay as you Go billing

You are billed monthly for the protection-hours used the previous month.

The pricing for Pay as you Go is shown in the table below. The same rates apply for both AWS and Azure subscriptions.

Note: The rates below only apply if you added the computers through the manager > **Computers > Add Account**. If you used **Computers > Add Computer**, the protection-hours are billed at the highest rate (Data Center) regardless of the computer's size.

Computer size	Examples	Cost per hour (in USD) per instance
Medium or smaller	Amazon EC2: C1, M1, M3, T1, T2 Amazon WorkSpaces Azure: 1 core Google: 1 core	$0.01
Large	Amazon EC2: C3, C4, M1, M3, M4, R3, T2 Azure: 2 cores Google: 2-3 cores	$0.03

Computer size	Examples	Cost per hour (in USD) per instance
Extra-large and greater	Amazon EC2: C1, C3, C4, CC2, CG1, CR1, D2, G2, HI1, HS1, I2, M1, M2, M3, M4, R3 Azure: 4 or more cores Google: 4 or more cores	$0.06
Data Center	All computers in Deep Security Manager that are not from a cloud connector	$0.06

Annual + Pay as you Go

You are billed based on a number of seats, or 'licenses', that you pre-purchase from Trend Micro. 1 seat equals 1 agent, and can be purchased for a 1 month, 1 year, 2 year, or 3 year term. If you need to protect additional computers later, those overages are billed at the Pay as You Go rate.

To lower your costs, Trend Micro applies the Pay as You Go rate to the smallest size possible of your instances, and uses the (cheaper) seat license rate for your largest instances. For example, if you initially purchased 5 seats covering 5 medium instances, and then later added 4 more large instances, your 5 seats would cover the 4 large instances you just added plus 1 of your existing medium instances. The remaining 4 medium instances would be billed at the Pay as you Go rate.

Prepaid credit

You are billed based on a number of protection-hour credits that you pre-purchase from Trend Micro. By prepaying, you receive a discount on Pay as you Go rates. Please contact the Deep Security Support team for pricing details.

Trend Micro notifies you when an estimated 30 days of credit remain. The estimate is based on current usage. If credits run out before you renew, then existing protection remains, but you won't be able to activate Deep Security Agent on new computers, and existing agents won't receive updates.

Tip: Commit to using Deep Security as a Service for one year and save up to 30% (for largest instance sizes).

Credit card

Note: Credit card billing is no longer offered for new deployments. If you are already using credit card billing, you can continue to use it.

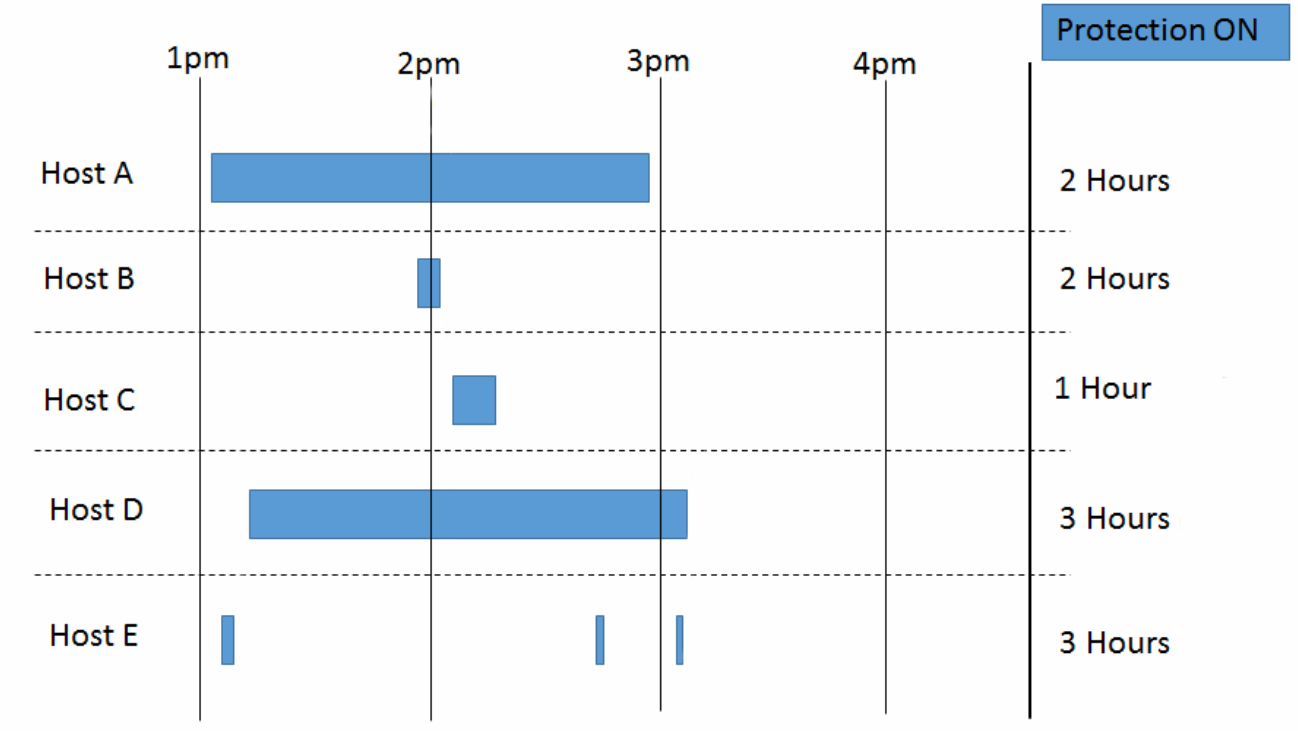
You are billed monthly for the protection-hours used the previous month. The manager tallies your hourly usage and sends the total owing that month to CleverBridge, a third-party billing service, which subsequently bills you. CleverBridge handles all credit card information so Trend Micro never sees any of it.

Credit card pricing is the same as Pay as you Go.

What Deep Security considers as a protection-hour

This section applies only to metered billing methods.

Cost is based on hours during which your computers are protected by Deep Security Agent. Partial protection within a clock-hour boundary is considered a full hour. In the example below, you can see how this is calculated in the usage scenarios below.



When protection-hours start and stop

This section applies only to metered billing methods.

How Deep Security counts protection-hours varies by how the computer was added to the manager:

- If added through **Computers > Add Account**: Protection-hours start when the instance is powered on, and *include* hours when the Deep Security Agent status is "Offline". Protection-hours stop when the instance is powered off, deleted, or the agent is uninstalled.
- If added through **Computers > Add Computer:** Same as above, but *excludes* hours when the Deep Security Agent status is "Offline".

Note: Even if an agent's status is "Offline", protection continues with the agent's last known configuration. Other features such as centralized reporting, however, require connectivity with the manager. To troubleshoot, see "Offline" agent. Alternatively, if the computer is decommissioned and will be permanently offline, you should de-activate its agent on the manager.

About this release

Deep Security as a Service release notes

Deep Security as a Service release notes have moved to What's New in Workload Security.

Scheduled maintenance

In most cases, we can perform upgrades and routine maintenance tasks without any service impact.

Periodically, we require a service-impacting maintenance window to perform specific tasks. Because these maintenance tasks are planned, we provide at least seven days notice prior to any scheduled maintenance.

If you'd like to be notified of scheduled maintenance, subscribe to our "Deep Security as a Service release notes" on the previous page RSS feed:

Subscribe via RSS

The feed notifies you for all new content as well as when scheduled maintenance is planned.

Next scheduled maintenance

There is no maintenance scheduled at this time.

Compatibility

Deep Security Agent platforms

Topics on this page:

See also "Agent platform support policy" on page 63.

Agent platform support table

Deep Security Manager supports the Deep Security Agents on the operating systems shown in the table below. If platform support was added in an update release, the minimum update version is noted next to the check mark in the table.

Deep Security Manager supports the use of older agent versions, but we do encourage customers to upgrade agents regularly. New agent releases provide additional security features and protection, higher quality, performance improvements, and updates to stay in sync with releases from each platform vendor. Each agent has an end-of-life date. For details, see "Deep Security LTS life cycle dates" on page 64 and "Deep Security FR life cycle dates" on page 68.

Note: Not all Deep Security features are available on all platforms. See "Supported features by platform" on page 90.

Note: The Deep Security Agent can be installed and is fully supported on any of the below platforms running in Amazon AWS, Google Cloud Platform (GCP), or Microsoft Azure.

Deep Security Agent Platform	Deep Security Agent Version									
	20 LTS	12 FR	12 LTS	11.3	11.2	11.1	11 LTS	10 LTS	9.6	9.0
Windows 2000, Service Pack 3 or 4 (32-bit) (See Note 5)									✔ U17	
Windows XP (32- and 64-bit) (See Note 5)								✔		
Windows Server 2003 SP1 or SP2 (32- and 64-bit) (See Note 5)								✔		
Windows Server 2003 R2 SP2 (32- and 64-bit)) (See Note 5)								✔		
Windows 7 (32- and 64-bit) (See Note 5)	✔	✔	✔	•	•	•	✔			
Windows 7 Embedded (32-bit) (See Note 2 and Note 5)	✔	✔	✔	•						
Windows Server 2008 (32- and 64-bit) (See Note 3 and Note 5)	✔	✔	✔	•	•	•	✔			
Windows Server 2008 R2 (64-bit) (See Note 3 and Note 5)	✔	✔	✔	•	•	•	✔			
Windows 8 (32- and 64-bit)	✔	✔	✔	•	•	•	✔			
Windows 8.1 (32- and 64-bit)	✔	✔	✔	•	•	•	✔			
Windows 8.1 Embedded (32-bit) (See Note 2)	✔	✔	✔	•						
Windows 10 (32- and 64-bit) (See Note 1)	✔	✔	✔	•	•	•	✔			
Windows 10 Embedded (64-bit) (See Note 2)	✔	✔	✔	•						
Windows Server 2012 (64-bit)	✔	✔	✔	•	•	•	✔			
Windows Server 2012 R2 (64-bit)	✔	✔	✔	•	•	•	✔			
Windows Server 2016 (LTSC, version 1607) (64-bit)	✔	✔	✔	•	•	•	✔			
Windows Server Core (SAC, version 1709) (64-bit) (See Note 1)	✔	✔	✔	•	•	•	✔			
Windows Server 2019 (LTSC, version 1809) (64-bit)	✔	✔	✔	•			✔ U4			

Deep Security Agent Platform	Deep Security Agent Version									
	20 LTS	12 FR	12 LTS	11.3	11.2	11.1	11 LTS	10 LTS	9.6	9.0
Red Hat Enterprise Linux 5 (32- and 64-bit)								✔		
Red Hat Enterprise Linux 6 (32- and 64-bit)	✔	✔	✔	•	•	•	✔			
Red Hat Enterprise Linux 7 (64-bit)	✔	✔	✔	•	•	•	✔			
Red Hat Enterprise Linux 8 (64-bit)	✔	✔	✔				✔ U12			
Ubuntu 10 (64-bit)									✔	
Ubuntu 12 (64-bit)									✔	
Ubuntu 14 (64-bit)								✔		
Ubuntu 16 (64-bit)	✔	✔	✔	•	•	•	✔			
Ubuntu 18 (64-bit)	✔	✔	✔	•	•		✔ U2			
Ubuntu 20.04 (64-bit)	✔	✔	✔ U10							
CentOS 5 (32- and 64-bit)								✔		
CentOS 6 (32- and 64-bit)	✔	✔	✔	•	•	•	✔			
CentOS 7 (64-bit)	✔	✔	✔	•	•	•	✔			
CentOS 8 (64-bit)	✔	✔	✔ U3				✔ U17			
Debian 6 (64-bit)									✔	
Debian 7 (64-bit)			✔	•	•	•	✔			
Debian 8 (64-bit)	✔	✔	✔	•	•	•	✔			
Debian 9 (64-bit)	✔	✔	✔	•	•	•	✔			
Debian 10 (64-bit)	✔	✔	✔ U1				✔ U14			
Amazon Linux (64-bit)	✔	✔	✔	•	•	•	✔			
Amazon Linux 2 (64-bit)	✔	✔	✔	•	•	•	✔			
Oracle Linux 5 (32- and 64-bit)								✔		
Oracle Linux 6 (32- and 64-bit)	✔	✔	✔	•	•	•	✔			
Oracle Linux 7 (64-bit)	✔	✔	✔	•	•	•	✔			
Oracle Linux 8 (64-bit)	✔	✔	✔ U2				✔ U14			
SUSE Linux Enterprise Server 10 (32- and 64-bit)									✔	
SUSE Linux Enterprise Server 11 (32- and 64-bit)			✔	•	•	•	✔	✔		
SUSE Linux Enterprise Server 12 (64-bit)	✔	✔	✔	•	•	•	✔	✔		
SUSE Linux Enterprise Server 15 (64-bit)	✔	✔	✔				✔ U13			
CloudLinux 5 (32- and 64-bit)									✔	

Deep Security Agent Platform	Deep Security Agent Version									
	20 LTS	12 FR	12 LTS	11.3	11.2	11.1	11 LTS	10 LTS	9.6	9.0
CloudLinux 6 (32-bit)								✔		
CloudLinux 6 (64-bit)							✔ U6			
CloudLinux 7 (64-bit)	✔	✔	✔	•	•	•	✔			
CloudLinux 8 (64-bit)	✔	✔ FR 2020-05-19								
Solaris 10 Updates 4-6 (64-bit, SPARC or x86)	✔		✔				✔ U6			
Solaris 10 Updates 7-10 (64-bit, SPARC or x86)	✔		✔				✔ U6			
Solaris 10 Update 11 (64-bit, SPARC or x86)	✔		✔				✔ U6			
Solaris 11.0 (1111)-11.1 (64-bit, SPARC or x86)	✔		✔				✔ U6			
Solaris 11.2-11.3 (64-bit, SPARC or x86)	✔		✔				✔ U6			
Solaris 11.4 (64-bit, SPARC or x86)	✔		✔				✔ U7			
AIX 5.3 (See Note 4)										✔
AIX 6.1, 7.1, 7.2 (See Note 4)	✔		✔ U5							

• Support for these releases is ending soon. Please upgrade to Deep Security Agent 20 as soon as possible.

If platform support was added in an update or FR release, the minimum update or FR version is noted next to the check mark in the table. Examples: ✔ U1, ✔ FR 2020-05-04.

Note 1: Microsoft releases regular, semi-annual releases for Microsoft Windows 10 and Windows Server Core. For details about which specific releases are supported, see Deep Security Support for Windows 10 and Deep Security Support for Windows Server Core.

Note 2: All Trend Micro testing on Windows Embedded platforms is performed in a virtualized environment. Because these operating systems are typically run on custom hardware (for example, on point-of-sale terminals), customers must plan to thoroughly test on their target hardware platform prior to deployment in a production environment. In addition, before raising support cases, customers should attempt to reproduce problems in a virtualized environment because this is the environment the Trend Micro support team has available. If the issue is specific to deployments on custom hardware, Trend Micro may require the customer to provide us with remote access to a suitable environment before we can fully respond to support cases.

Note 3: Deep Security Agent is supported with both Full/Desktop Experience and Server Core installations of Windows Server 2012 and later. For Windows Server 2008 and 2008 R2, only the 'Full Installation' is supported. (The 'Server Core Installation' is not.)

Note 4: If you want to use Deep Security Agent 9.0 for AIX, you'll need to use a signed agent, version 9.0.0-5624 or higher. Please be aware that the end-of-life date for this agent is 31-Dec-2020. You can download this agent from the **Earlier Versions** tab on the Deep Security SoftwareDeep Security Software page. The following AIX configurations are supported:

- AIX LPARs running on the PowerVM Hypervisor on Power Servers.
- AIX running as the bare metal OS on Power Servers.

Note 5: Microsoft has changed their signing policy to use only SHA-2. For information on compatibility and required Microsoft security updates, see:

- 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 (also available in Japanese)

Also, Deep Security 10.0 Update 26 does not support the installation or upgrade of Deep Security Agent on Windows 2003 or Windows XP. Support for these platforms will be re-introduced in a subsequent update. For more information, see Deep Security Agent version 10 update 26 cannot be used for installation or upgrade on Windows XP/2003.

Docker support

You can use Deep Security 10.0 or later to protect Docker hosts and containers running on Linux distributions. Windows is not supported.

With each Deep Security long-term support (LTS) release, Deep Security supports all Docker Enterprise Edition (EE) versions that have not reached end-of-life. (See Announcing Docker Enterprise Edition.) We do not officially support Docker Edge releases, but strive to test against Docker Edge releases to the best of our ability.

Support for new stable Docker releases is introduced with each release of Deep Security. We recommend that you refrain from upgrading to the latest stable release of Docker until Trend Micro documents the support statements for the latest Deep Security release.

Deep Security 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	17.06	18.03	18.06	18.09	19.03
10 LTS	✔	✔												
11 LTS			✔	✔	✔					✔	✔	✔	✔	✔
11.1					✔	✔				✔	✔			
11.2						✔	✔			✔	✔			
11.3							✔	✔		✔	✔			
12 LTS							✔	✔		✔	✔	✔	✔	✔
12 FR									✔	✔	✔	✔	✔	✔
20 LTS									✔	✔	✔	✔	✔	✔

Note: Deep Security support for Docker releases includes any sub-versions of those releases. For example, Deep Security 11.0 supports Docker 17.09-ce including its sub-versions: 17.09.0-ce and 17.09.1-ce.

Before deploying Deep Security into your target environment, you should ensure that Docker supports your target environment and platform configuration.

Systemd support

Some versions of the Deep Security Agent for Linux support systemd. See the table below for details.

Deep Security Agent Platform	Deep Security Agent Version			
	20 LTS	12 FR	12 LTS	11 LTS
Amazon Linux (64-bit)				
Amazon Linux 2 (64-bit)				
CloudLinux 6 (64-bit)				
CloudLinux 7 (64-bit)				
CloudLinux 8 (64-bit)	✔	✔ FR 2020-05-19		
Debian 8 (64-bit)				
Debian 9 (64-bit)				
Debian 10 (64-bit)	✔	✔	✔ U1	✔ U14
Oracle Linux 6 (32- and 64-bit)				
Oracle Linux 7 (64-bit)	✔	✔	✔ U1	✔ U13
Oracle Linux 8 (64-bit)	✔	✔	✔ U2	✔ U14
Red Hat Enterprise Linux 6 (32- and 64-bit)				
Red Hat Enterprise Linux 7 (64-bit)	✔	✔	✔ U1	✔ U13
Red Hat Enterprise Linux 8 (64-bit)	✔	✔	✔	✔ U12
SUSE Linux Enterprise Server 11 (32- and 64-bit)				
SUSE Linux Enterprise Server 12 (64-bit)				
SUSE Linux Enterprise Server 15 (64-bit)	✔	✔	✔	✔ U13
Ubuntu 16 (64-bit)				

Deep Security Agent Platform	Deep Security Agent Version			
Ubuntu 18 (64-bit)	✔	✔		
Ubuntu 20 (64-bit)	✔			

If systemd support was added in an update or FR release, the minimum update or FR version is noted next to the check mark in the table. Examples: ✔ U1, ✔ FR 2020-05-04

SELinux support

Security-Enhanced Linux (SELinux) enforcing mode is supported on these OS and agent combinations, using the default SELinux policies:

Deep Security Agent Platform	Deep Security Agent Version		
	20 LTS	12 FR	12 LTS
Red Hat Enterprise Linux 7 (64-bit)	✔	✔ (FR 2020-05-19 or later)	✔ (Update 9 or later)
Red Hat Enterprise Linux 8 (64-bit)	✔	✔ (FR 2020-05-19 or later)	✔ (Update 9 or later)

Warning: Anti-Malware software such as Deep Security Agent must run in an unconfined domain in order to protect the system. Any additional SELinux policy customization or configuration may cause Deep Security Agent to be blocked.

Note: If any alerts occur, see "Troubleshoot SELinux alerts" on page 1078.

Secure Boot support

Some versions of the Deep Security Agent support the Secure Boot feature. See the table below for details. For details on configuring the agent for Secure Boot, see Linux Secure Boot support for agents.

Note: Secure Boot is not available for AWS instances and Azure VMs.

	Deep Security Agent Version			
Deep Security Agent Platform	20 LTS	12 FR	12 LTS	11 LTS
Red Hat Enterprise Linux 7 (64-bit)	✔	✔	✔	✔
Red Hat Enterprise Linux 8 (64-bit)	✔	✔		
Debian 10 (64-bit)	✔	✔		
SUSE Linux Enterprise Server 12 (64-bit)	✔	✔		
SUSE Linux Enterprise Server 15 (64-bit)	✔	✔		
Ubuntu 16 (64-bit)	✔	✔		
Ubuntu 18 (64-bit)	✔	✔		
Ubuntu 20 (64-bit)	✔			

Deep Security Agent Linux kernel support

- 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 version of the complete list of the supported Linux kernels for Deep Security Agent 10.0 and higher with scripts and automated workflows.

Supported features by platform

The tables below list the features available for each OS platform of **Deep Security Agent 20** :

Note:
Older agents are compatible with other platforms (although they don't support new features). See "Deep Security Agent platforms" on page 80 for a complete list of compatible agents. To see the features available with older agents:

- Deep Security Agent 10.0 (and newer) supported features: In the drop-down menu above, select that version of Deep Security.
- Deep Security Agent 9.6 Service Pack 1 supported features

Microsoft Windows

Note: Deep Security Agent is supported with both Full/Desktop Experience and Server Core installations of Windows Server 2012 and later (any exceptions for particular features are noted in the table below). 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	Recommen-dation Scan	Relay
	Real-time		On-demand						Real-time			On-demand						
	Feature set 1	Feature set 2	Feature set 1	Feature set 2			Unencrypted Traffic	SSL Encrypted Traffic	File Scans	Directory Scans	Scans of Running Services, Processes, Listening Ports	File and Directory Scans	Registry Scans	Scans of Running Services, Processes, Listening Ports				
Windows 7 (32-bit)	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔		✔	
Windows 7 (64-bit)	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔		✔	✔
Windows 7 Embedded (32-bit) (3)	✔	✔	✔		✔	✔	✔	✔				✔	✔	✔	✔		✔	
Windows Server 2008 (32-bit)	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔		✔	
Windows Server 2008 (64-bit)	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔		✔	✔
Windows Server 2008 R2 (64-bit)	✔	✔	✔		✔	✔	✔	✔	✔ (1)	✔ (1)	✔	✔	✔	✔	✔	✔	✔	✔

	Anti-Malware				Web Reputation Service	Firewall	Intrusion Prevention System		Integrity Monitoring						Log Inspection	Application Control	Recommen-dation Scan	Relay
	Real-time		On-demand						Real-time			On-demand						
	Feature set 1	Feature set 2	Feature set 1	Feature set 2			Unencrypted Traffic	SSL Encrypted Traffic	File Scans	Directory Scans	Scans of Running Services, Processes, Listening Ports	File and Directory Scans	Registry Scans	Scans of Running Services, Processes, Listening Ports				
Windows 8 (32-bit)	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔		✔	
Windows 8 (64-bit)	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔		✔	✔
Windows 8.1 (32-bit)	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔		✔	
Windows 8.1 (64-bit)	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔		✔	✔
Windows 8.1 Embedded (32-bit) (3)	✔	✔	✔		✔	✔	✔	✔				✔	✔	✔	✔		✔	
Windows 10 (32-bit) (2)	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔		✔	
Windows 10 (64-bit) (2)	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔		✔	✔
Windows 10 Embedded (64-bit) (3)	✔	✔	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔		✔	✔

	Anti-Malware				Web Reputation Service	Firewall	Intrusion Prevention System		Integrity Monitoring						Log Inspection	Application Control	Recommen-dation Scan	Relay
	Real-time		On-demand						Real-time			On-demand						
	Feature set 1	Feature set 2	Feature set 1	Feature set 2			Unencrypted Traffic	SSL Encrypted Traffic	File Scans	Directory Scans	Scans of Running Services, Processes, Listening Ports	File and Directory Scans	Registry Scans	Scans of Running Services, Processes, Listening Ports				
Windows Server 2012 (64-bit)	✔	✔	✔		✔	✔	✔	✔	✔ (1) (5)	✔ (1)(5)	✔	✔	✔	✔	✔	✔ (5)	✔	✔
Windows Server 2012 R2 (64-bit)	✔	✔	✔		✔	✔	✔	✔	✔ (1)	✔ (1)	✔	✔	✔	✔	✔	✔	✔	✔
Windows Server 2016 (LTSC, version 1607) (64-bit)	✔	✔	✔		✔	✔	✔	✔	✔ (1)	✔ (1)	✔	✔	✔	✔	✔	✔	✔	✔
Windows Server Core (SAC, version 1709) (64-bit)(2)	✔	✔	✔		✔	✔	✔	✔	✔ (1)	✔ (1)	✔	✔	✔	✔	✔	✔	✔	✔
Windows Server 2019 (LTSC, version 1809) (64-bit)	✔	✔	✔		✔	✔	✔	✔	✔ (1)	✔ (1)	✔	✔	✔	✔	✔	✔	✔	✔

Red Hat Enterprise Linux

	Anti-Malware				Web Reputation Service	Firewall	Intrusion Prevention System		Integrity Monitoring						Log Inspection	Application Control	Recommen-dation Scan	Relay
	Real-time		On-demand						Real-time			On-demand						
	Feature set 1	Feature set 2	Feature set 1	Feature set 2			Unencrypted Traffic	SSL Encrypted Traffic	File Scans	Directory Scans	Scans of Running Processes, Listening Ports	File and Directory Scans	Registry Scans	Scans of Running Processes, Listening Ports				
Red Hat Enterprise Linux 6 (32-bit)	✔ (4)		✔			✔	✔	✔			✔	✔		✔	✔		✔	
Red Hat Enterprise Linux 6 (64-bit)	✔ (4)		✔		✔	✔	✔	✔	✔ (1)		✔	✔		✔	✔	✔	✔	✔
Red Hat Enterprise Linux 7 (64-bit)	✔ (4)		✔		✔	✔	✔	✔	✔ (1)		✔	✔		✔	✔	✔	✔	✔
Red Hat Enterprise Linux 8 (64-bit)	✔ (4)		✔		✔	✔	✔	✔	✔ (1)		✔	✔		✔	✔	✔	✔	✔

CentOS Linux

	Anti-Malware				Web Reputation Service	Firewall	Intrusion Prevention System		Integrity Monitoring						Log Inspection	Application Control	Recommen-dation Scan	Relay
	Real-time		On-demand						Real-time			On-demand						
	Feature set 1	Feature set 2	Feature set 1	Feature set 2			Unencrypted Traffic	SSL Encrypted Traffic	File Scans	Directory Scans	Scans of Running Processes, Listening Ports	File and Directory Scans	Registry Scans	Scans of Running Processes, Listening Ports				
CentOS 6 (32-bit)	✔ (4)		✔			✔	✔	✔			✔	✔		✔	✔		✔	
CentOS 6 (64-bit)	✔ (4)		✔		✔	✔	✔	✔	✔ (1)		✔	✔		✔	✔	✔	✔	✔
CentOS 7 (64-bit)	✔ (4)		✔		✔	✔	✔	✔	✔ (1)		✔	✔		✔	✔	✔	✔	✔
CentOS 8 (64-bit)	✔ (4)		✔		✔	✔	✔	✔	✔ (1)		✔	✔		✔	✔	✔	✔	✔

Oracle Linux

	Anti-Malware				Web Reputation Service	Firewall	Intrusion Prevention System		Integrity Monitoring						Log Inspection	Application Control	Recommen-dation Scan	Relay
	Real-time		On-demand						Real-time			On-demand						
	Feature set 1	Feature set 2	Feature set 1	Feature set 2			Unencrypted Traffic	SSL Encrypted Traffic	File Scans	Directory Scans	Scans of Running Processes, Listening Ports	File and Directory Scans	Registry Scans	Scans of Running Processes, Listening Ports				
Oracle Linux 6 (32-bit)			✔			✔	✔	✔			✔	✔		✔	✔		✔	
Oracle Linux 6 (64-bit)	✔(4)		✔		✔	✔	✔	✔	✔ (1)		✔	✔		✔	✔	✔	✔	✔
Oracle Linux 7 (64-bit)	✔(4)		✔		✔	✔	✔	✔	✔ (1)		✔	✔		✔	✔	✔	✔	✔
Oracle Linux 8 (64-bit)	✔(4)		✔		✔	✔	✔	✔	✔ (1)		✔	✔		✔	✔	✔	✔	✔

SUSE Linux

	Anti-Malware				Web Reputation Service	Firewall	Intrusion Prevention System		Integrity Monitoring						Log Inspection	Application Control	Recommen-dation Scan	Relay
	Real-time		On-demand						Real-time			On-demand						
	Feature set 1	Feature set 2	Feature set 1	Feature set 2			Unencrypted Traffic	SSL Encrypted Traffic	File Scans	Directory Scans	Scans of Running Processes, Listening Ports	File and Directory Scans	Registry Scans	Scans of Running Processes, Listening Ports				
SUSE Linux Enterprise Server 12 SP1, SP2, SP3 (64-bit)	✔(4)		✔		✔	✔	✔	✔	✔(1)		✔	✔		✔	✔	✔	✔	✔
SUSE Linux Enterprise Server 15 (64-bit)	✔(4)		✔		✔	✔	✔	✔	✔(1)		✔	✔		✔	✔	✔	✔	✔

Ubuntu Linux

	Anti-Malware				Web Reputation Service	Firewall	Intrusion Prevention System		Integrity Monitoring						Log Inspection	Application Control	Recommen-dation Scan	Relay
	Real-time		On-demand						Real-time			On-demand						
	Feature set 1	Feature set 2	Feature set 1	Feature set 2			Unencrypted Traffic	SSL Encrypted Traffic	File Scans	Directory Scans	Scans of Running Processes, Listening Ports	File and Directory Scans	Registry Scans	Scans of Running Processes, Listening Ports				
Ubuntu 16 (64-bit)	✔ (4)		✔		✔	✔	✔	✔	✔ (1)		✔	✔		✔	✔	✔	✔	✔
Ubuntu 18 (64-bit)	✔ (4)		✔		✔	✔	✔	✔	✔ (1)		✔	✔		✔	✔	✔	✔	✔
Ubuntu 20.04 (64-bit)	✔ (4)		✔		✔	✔	✔	✔	✔ (1)		✔	✔		✔	✔	✔	✔	✔

Debian Linux

	Anti-Malware				Web Reputation Service	Firewall	Intrusion Prevention System		Integrity Monitoring						Log Inspection	Application Control	Recommen-dation Scan	Relay
	Real-time		On-demand						Real-time			On-demand						
	Feature set 1	Feature set 2	Feature set 1	Feature set 2			Unencrypted Traffic	SSL Encrypted Traffic	File Scans	Directory Scans	Scans of Running Processes, Listening Ports	File and Directory Scans	Registry Scans	Scans of Running Processes, Listening Ports				
Debian 8 (64-bit)	✔(4)		✔		✔	✔	✔	✔	✔(1)		✔	✔		✔	✔	✔	✔	✔
Debian 9 (64-bit)	✔(4)		✔		✔	✔	✔	✔	✔(1)		✔	✔		✔	✔	✔	✔	✔
Debian Linux 10 (64-bit)	✔(4)		✔		✔	✔	✔	✔	✔(1)		✔	✔		✔	✔	✔	✔	✔

CloudLinux

	Anti-Malware				Web Reputation Service	Firewall	Intrusion Prevention System		Integrity Monitoring						Log Inspection	Application Control	Recommen-dation Scan	Relay
	Real-time		On-demand						Real-time			On-demand						
	Feature set 1	Feature set 2	Feature set 1	Feature set 2			Unencrypted Traffic	SSL Encrypted Traffic	File Scans	Directory Scans	Scans of Running Processes, Listening Ports	File and Directory Scans	Registry Scans	Scans of Running Processes, Listening Ports				
CloudLinux 7, 8 (64-bit)	✔(4)		✔		✔	✔	✔	✔	✔ (1)		✔	✔		✔	✔	✔	✔	✔

Amazon Linux

	Anti-Malware				Web Reputation Service	Firewall	Intrusion Prevention System		Integrity Monitoring						Log Inspection	Application Control	Recommen-dation Scan	Relay
	Real-time		On-demand						Real-time			On-demand						
	Feature set 1	Feature set 2	Feature set 1	Feature set 2			Unencrypted Traffic	SSL Encrypted Traffic	File Scans	Directory Scans	Scans of Running Processes, Listening Ports	File and Directory Scans	Registry Scans	Scans of Running Processes, Listening Ports				
Amazon Linux (64-bit)	✔(4)		✔		✔	✔	✔	✔	✔ (1)		✔	✔		✔	✔	✔	✔	✔

	Anti-Malware				Web Reputation Service	Firewall	Intrusion Prevention System		Integrity Monitoring						Log Inspection	Application Control	Recommen-dation Scan	Relay
	Real-time		On-demand						Real-time			On-demand						
	Feature set 1	Feature set 2	Feature set 1	Feature set 2			Unencrypted Traffic	SSL Encrypted Traffic	File Scans	Directory Scans	Scans of Running Processes, Listening Ports	File and Directory Scans	Registry Scans	Scans of Running Processes, Listening Ports				
Amazon Linux 2 (64-bit)	✔(4)		✔		✔	✔	✔	✔	✔(1)		✔	✔		✔	✔	✔	✔	✔

Solaris

Note: See "How does agent protection work for Solaris zones?" on page 1057 for more on how protection works between Solaris zones. For a list of supported Solaris versions, see "Deep Security Agent platforms" on page 80.

	Anti-Malware				Web Reputation Service	Firewall	Intrusion Prevention System		Integrity Monitoring						Log Inspection	Application Control	Recommen-dation Scan	Relay	Scanner	FIPS mode
	Real-time		On-demand						Real-time			On-demand								
	Feature set 1	Feature set 2	Feature set 1	Feature set 2			Unencrypted Traffic	SSL Encrypted Traffic	File Scans	Directory Scans	Scans of Running Processes, Listening Ports	File and Directory Scans	Registry Scans	Scans of Running Processes, Listening Ports						
Solaris			✔		✔	✔	✔	✔	✔		✔	✔		✔	✔		✔			

AIX

Note: For a list of supported AIX versions, see "Deep Security Agent platforms" on page 80.

	Anti-Malware				Web Reputation Service	Firewall	Intrusion Prevention System		Integrity Monitoring						Log Inspection	Application Control	Recommen-dation Scan	Relay	Scanner	FIPS mode
	Real-time		On-demand						Real-time			On-demand								
	Feature set 1	Feature set 2	Feature set 1	Feature set 2			Unencrypted Traffic	SSL Encrypted Traffic	FileScans	Directory Scans	Scans of Running Processes, Listening Ports	File and Directory Scans	Registry Scans	Scans of Running Processes, Listening Ports						
AIX 6.1, 7.1, 7.2						✔	✔	✔			✔	✔		✔	✔		✔			

Feature set 1 includes signature-based file scanning, spyware scanning, and document exploit protection.

Feature set 2 includes behavior monitoring, process memory scanning, and registry scanning.

(1) This platform supports enhanced real-time integrity monitoring. It uses the application control driver to provide file monitoring and captures information about *who* made changes to a monitored file.

(2) Microsoft releases regular, semi-annual releases for Microsoft Windows 10 and Windows Server Core. For details about which specific releases are supported, see Deep Security Support for Windows 10 and Deep Security Support for Windows Server Core.

(3) All Trend Micro testing on Windows Embedded platforms is performed in a virtualized environment. Because these operating systems are typically run on custom hardware (for example, on point-of-sale terminals), customers must plan to thoroughly test on their target hardware platform prior to deployment in a production environment. In addition, before raising support cases, customers should attempt to reproduce problems in a virtualized environment because this is the environment the Trend Micro support team has available. If the issue is specific to deployments on custom hardware, Trend Micro may require the customer to provide us with remote access to a suitable environment before we can fully respond to support cases.

(4) **Real-time Anti-Malware support on Linux:** Real-time Anti-Malware scanning is highly dependent on the file system hooking implementation, so file system incompatibility can cause issues with this feature. The following table shows which file systems are compatible with the feature:

File system type		Deep Security 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	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔

File system type		Deep Security 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
Special file systems	tmpfs	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	aufs	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	
	OverlayFS	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
Network file systems (see Note, below)	NFSv3	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	NFSv4	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	SMB	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	CIFS	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔
	FTP	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔

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 332.

(5) This feature is available only with Full/Desktop Experience installations. It is not supported with Server Core installations.

System requirements

Requirements vary by version. For older versions of agents, or relays, see their documentation.

Deep Security Agent requirements

- Minimum RAM and disk space: See "Deep Security Agent and Relay sizing" below
- Supported platforms (operating systems): See "Deep Security Agent platforms" on page 80.
- Supported features: Supported Deep Security features vary by platform.

Note: 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 a few constraints:

- Relays are only supported on 64-bit operating systems.
- Relays are not supported on Solaris or AIX.

Sizing

Sizing guidelines for Deep Security deployments vary by the scale of your network, hardware, and software.

Deep Security Agent and Relay sizing

Platform	Features enabled	Minimum RAM	Recommended RAM	Minimum disk space
Windows	All protection	2 GB	4 GB	1 GB
Windows	Relay only	2 GB	4 GB	900 GB

Platform	Features enabled	Minimum RAM	Recommended RAM	Minimum disk space
Linux	All protection	2 GB	5 GB	1 GB
Linux	Relay only	2 GB	4 GB	900 GB
Solaris	All protection. Relay not supported	4 GB	4 GB	2 GB
AIX	All protection. Relay not supported	4 GB	4 GB	2 GB

Less RAM is required for some OS versions, or if you do not enable all Deep Security features.

Relays require more disk space if you install Deep Security Agent on many different platforms. (Relays store update packages for each platform.) For details, see "Get Deep Security Agent software" on page 144.

Note: Relays are already provided as part of Deep Security as a Service. Do not create more relays unless required. For details, see "Deploy additional relays" on page 816.

Port numbers, URLs, and IP addresses

Deep Security default port numbers, URLs, IP addresses, and protocols are listed in the sections below. If a port, URL or IP address is configurable, a link is provided to the relevant configuration page.

- "Deep Security port numbers" on the next page
- "Deep Security URLs" on page 111
- "Deep Security as a Service IP addresses" on page 113

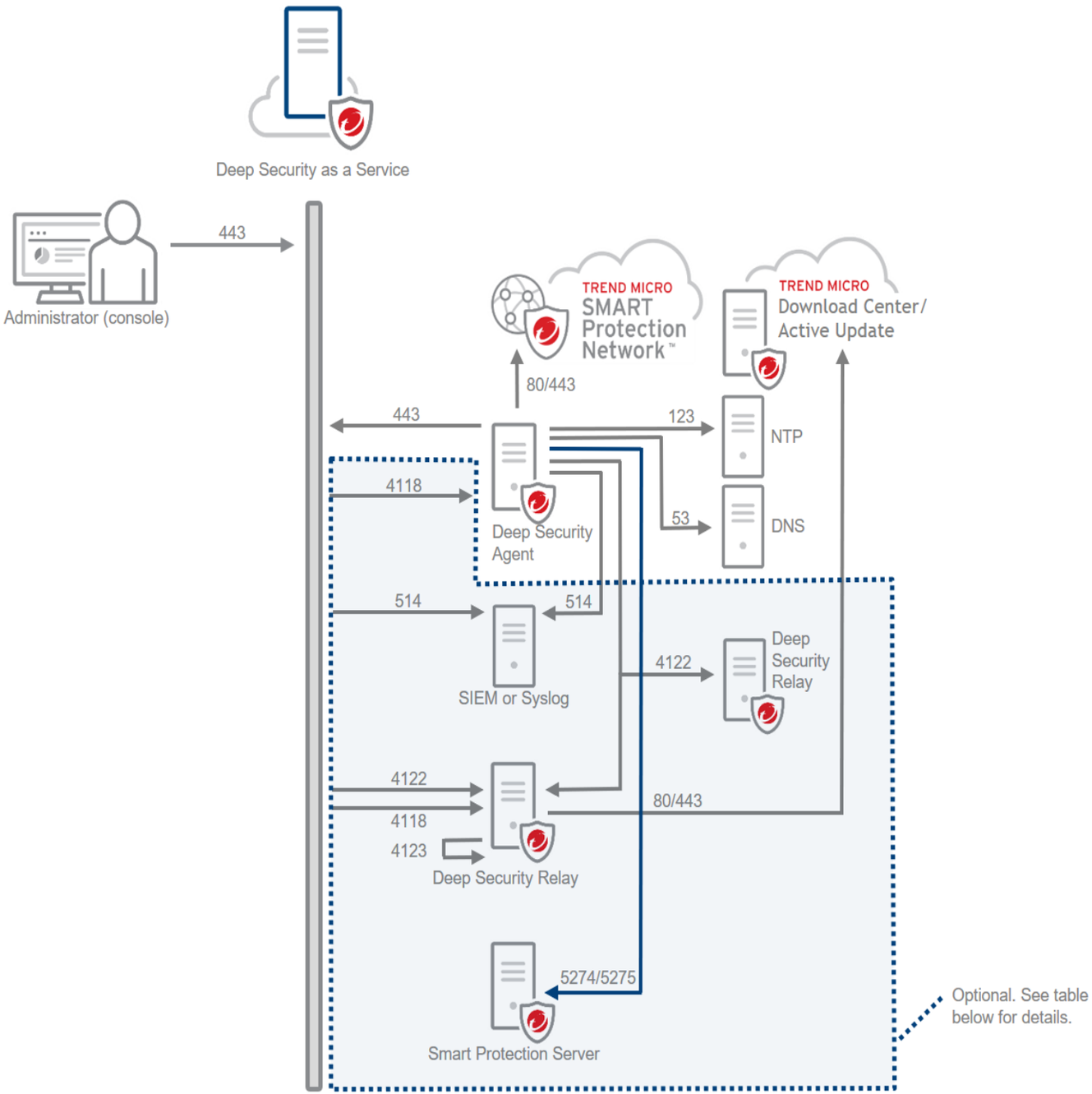
Note: If your network uses a proxy, you can configure Deep Security to connect to it instead of directly to the components listed on this page. For details, see "Configure proxies" on page 807.

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 "Activation Failed - Blocked port" on page 789.

Deep Security port numbers

The following diagram shows the default ports in a Deep Security system. For details, see the table below the diagram.

Trend Micro Deep Security as a Service



Note: In the table below:

- 'Mandatory ports' refer to ports that must be opened to ensure the proper functioning of the Deep Security system.
- 'Optional ports' refer to ports that may be opened depending on the feature or component you want to deploy.
- 'Port' is used in place of 'port number' for brevity.

Port type	Default port number and protocol
Deep Security Agent listening (inbound) port	Optional port: • 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, agent-initiated communication is used, which is why 4118/HTTPS is listed here as 'optional'. See "Agent-manager communication" on page 842 for details.
Deep Security Agent outbound ports	Mandatory ports: • 53/DNS over TCP or UDP – DNS server port • 80/HTTP, 443/HTTPS – Smart Protection Network port, Deep Security as a Service port • 123/NTP over UDP – NTP server port Optional ports: • 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 Deep Security as a Service. • 5274/HTTP, 5275/HTTPS – Smart Protection Server ports. 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, or "Integrate with Smart Protection Server" on page 1049.

Port type	Default port number and protocol
	• 4122/HTTPS – Deep Security Relay port. Allow 4122/HTTPS if you want to host relays in your local network. Local relays are typically not required. See "Deploy Deep Security Relay" on page 144 for details.
Deep Security Relay listening (inbound) ports	Relays are typically not required. For details, see "Deploy Deep Security Relay" on page 144. If you do decide to deploy relays, then make sure they can listen on the following ports. • Allow the agent listening port, since it applies to the relay too • 4122/HTTPS – Deep Security Replay port • 4123 – This port is for communication between the agent and its own internal relay **Note:** Port 4123 should not be listening to connections from other computers, and you don't need to configure it in network firewall policies. But if you have firewall software (such as Windows Firewall or iptables) on the relay itself, verify that it does not block this connection to itself. Also verify that other applications do not use the same port (a port conflict).
Deep Security Relay outbound ports	Relays are typically not required. For details, see "Deploy Deep Security Relay" on page 144. If you do decide to deploy relays, then make sure they can connect outbound to the following ports. • 80/HTTP, 443/HTTPS – Trend Micro Update Server/Active Update and Download Center ports • 4122 – port of other Deep Security Relays
Ports of components receiving traffic from Deep Security as a Service	Optional ports: • 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 Deep Security as a Service. • 4118/HTTPS – Deep Security Agent port. Leave 4118/HTTPS closed if you plan on using agent-initiated communication. Only open it if

Port type	Default port number and protocol
	you plan on using bidirectional or manager-initiated communication. By default, agent-initiated communication is used, which is why 4118/HTTPS is listed here as 'optional'. See "Agent-manager communication" on page 842 for details. • 4122/HTTPS – Deep Security Relay port. Allow 4122/HTTPS if you want to host relays in your local network. Local relays are typically not required. See "Deploy Deep Security Relay" on page 144 for details.

Deep Security URLs

If you need to restrict the URLs that are allowed in your environment, read this section.

You'll need to make sure your firewall allows traffic from the 'Source' to the 'Destinations' listed in the table below. For each FQDN, make sure you 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)
Deep Security Agent, Deep Security Relay	Deep Security as a Service	• app.deepsecurity.trendmicro.com • agents.deepsecurity.trendmicro.com • dsmim.deepsecurity.trendmicro.com • relay.deepsecurity.trendmicro.com In the list above, app.deepsecurity[...] is the Deep Security as a Service FQDN, agents.deepsecurity[...] and dsmim.deepsecurity[...] are the Deep Security as a Service heartbeat server FQDNs, and relay.deepsecurity[...] is the FQDN of the relays hosted by Deep Security as a Service.
API clients	Deep Security APIs	• app.deepsecurity.trendmicro.com/webservice/Manager?WSDL

Source	Destination server or service name	Destination fully-qualified domain name (FQDN)
		• app.deepsecurity.trendmicro.com/api • app.deepsecurity.trendmicro.com/rest
Deep Security Agent, Deep Security Relay	Download Center or web server Hosts software.	• files.trendmicro.com
Deep Security Agent	Smart Protection Network - Global Census Service Used for behavior monitoring, and predictive machine learning.	• dsaas1100-en-census.trendmicro.com
Deep Security Agent	Smart Protection Network - Good File Reputation Service Used for behavior monitoring, predictive machine learning, and process memory scans.	• deepsecaas11-en.gfrbridge.trendmicro.com
Deep Security Agent	Smart Protection Network - Smart Scan Service	• dsaas.icrc.trendmicro.com
Deep Security Agent	Smart Protection Network - predictive machine learning	• dsaas-en-f.trx.trendmicro.com • dsaas-en-b.trx.trendmicro.com
Deep Security	Smart Protection Network -	• dsaas.url.trendmicro.com

Source	Destination server or service name	Destination fully-qualified domain name (FQDN)
Agent	Web Reputation Service	

Deep Security as a Service IP addresses

If you need to restrict the IP addresses that are allowed in your environment, read this section to determine which ones must be allowed inbound and outbound.

Inbound IP addresses

If a firewall or AWS security group restricts which IP addresses are allowed *inbound* to your network, make sure to allow traffic inbound from the Deep Security as a Service subnet to the destination components listed below.

Source	Destination component, port, and protocol (on your network)	Notes
Deep Security as a Service Subnet 34.205.5.0/27	SIEM or syslog server Default port: 514 Protocol: syslog over UDP	Only allow this traffic if you configured a SIEM or syslog server.
	Deep Security Agent Default port: 4118 Protocol: HTTPS over TCP	Only allow this traffic if you configured your agents to use bidirectional or manager-initiated communication. (By default, agents use agent-initiated communication.)
	Deep Security Relay	Only allow this traffic if you deployed relays in your local network. (Under normal circumstances, you don't need local relays.)

Source	Destination component, port, and protocol (on your network)	Notes
	Default port: 4120 Protocol: HTTPS over TCP	

Outbound IP addresses

If a firewall or AWS security group restricts which IP addresses are allowed *outbound* from your network, make sure to allow HTTPS traffic outbound on port 443 to the Trend Micro destination IPv4 addresses listed in the table below.

Source (on your network)	Destination component, port, and protocol	Destination IP addresses
Deep Security Agents, administrator's computer	Deep Security as a Service GUI Port: 443 Protocol: HTTPS over TCP	34.196.38.94 34.198.27.224 34.198.6.142 34.205.210.199 34.205.219.175 34.205.239.162 34.226.116.82 34.233.153.57 35.153.222.175

Source (on your network)	Destination component, port, and protocol	Destination IP addresses
		35.169.254.68 35.169.43.208 35.172.176.62 50.17.162.194 52.0.124.201 52.0.33.128 52.202.124.22 52.207.138.122 52.22.162.229 52.3.171.31 52.72.111.249 52.72.211.36 52.87.46.150 54.175.211.84 54.80.120.113
Deep Security Agents, Deep	Trend Micro Update Server (also called	34.194.74.60

Source (on your network)	Destination component, port, and protocol	Destination IP addresses
Security Relays	Active Update) and Download Center Port: 443 Protocol: HTTPS over TCP	34.196.197.189 34.204.219.38 34.205.83.195 52.2.63.133 52.21.149.243 52.44.144.238 52.55.188.35 52.201.199.128 52.206.54.30 54.86.152.157 54.87.173.241
Deep Security Agents	Deep Security as a Service heartbeat servers Port: 443 Protocol: HTTPS over TCP	34.192.67.219 34.196.25.105 34.199.44.254 34.204.244.61 34.206.23.113

Source (on your network)	Destination component, port, and protocol	Destination IP addresses
		34.206.95.140 34.206.146.6 34.206.215.233 52.23.102.52 52.54.141.100 52.54.240.176 54.86.2.200
Deep Security Agents	Component: Deep Security as a Service fast heartbeat Port: 443 Protocol: HTTPS over TCP	34.192.145.157 34.199.111.255 34.204.221.63 34.206.179.241 52.44.129.132 52.45.95.227 52.55.183.116 52.73.88.81 52.202.143.169

Source (on your network)	Destination component, port, and protocol	Destination IP addresses
		52.206.208.21 54.208.106.230 54.152.108.196 54.85.86.247 18.204.77.2 54.84.198.181 52.0.58.66 52.6.19.160 18.233.125.165 34.227.134.223 52.73.122.26 34.233.252.54 34.236.163.142 52.44.40.85 3.209.15.127 52.70.113.18 3.210.118.160

Source (on your network)	Destination component, port, and protocol	Destination IP addresses
		54.175.77.19 3.225.117.164 54.224.63.108 52.72.213.26 18.235.177.174 34.203.45.194 54.165.185.17
Deep Security Agents	Smart Protection Network Ports: 80 and 443 Protocols: HTTP and HTTPS, over TCP	Trend Micro's cloud-based Smart Protection Network does not have static IP addresses. If you want to use the Smart Protection Network but need to restrict your outbound communication, we suggest you deploy a Smart Protection Server in your environment. For information on how to do this, see "Integrate with Smart Protection Server" on page 1049.

Get Started

Buy Deep Security as a Service

Sign up for a 30-day free trial

You can sign up for a free 30 day trial account with Deep Security as a Service to try out the service. If you'd like, you can "Try the Deep Security demo" on page 127. When you're ready to upgrade to a paid version, read the instructions at "Sign up for Deep Security as a Service" below.

Sign up for Deep Security as a Service

You can sign up using any one of the following methods:

- "Sign up with AWS - Pay as you Go billing" below
- "Sign up with AWS - Annual + Pay as you Go billing" on the next page
- "Sign up with Azure - Pay as you Go billing" on page 122
- "Sign up with prepaid credit billing" on page 126
- "Sign up with BYOL billing" on page 127

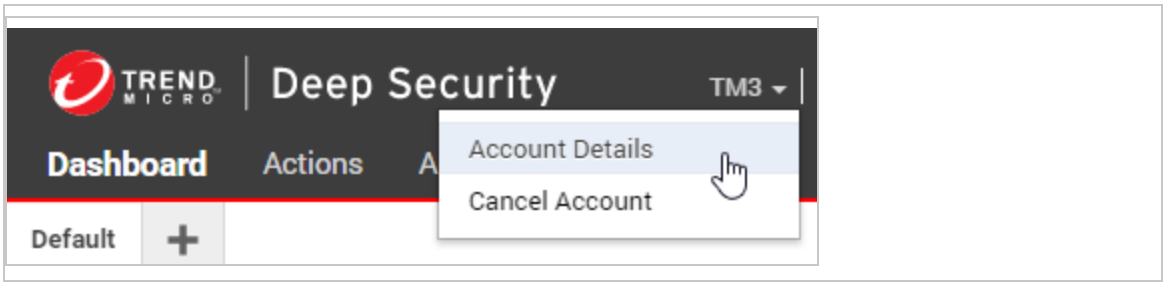
For details on the above billing methods and pricing, see "About billing and pricing" on page 74.

Sign up with AWS - Pay as you Go billing

If you already have a Deep Security as a Service account

1. Log in to Deep Security as a Service.

2. At the top of the page, click your account name (as shown below) and select **Account Details**.



3. Click **Upgrade to Paid**.
4. Click **Subscribe through AWS Marketplace**.

   Note: By default, you are brought to the AWS Marketplace page for a Pay as you Go subscription.

5. Click **Continue** > **Subscribe** > **Set Up Your Account**.

   You are brought to the Deep Security Dashboard. Your subscription is now active.

If you do not have a Deep Security as a Service account

1. Go to the Trend Micro Deep Security as a Service - Pay as You Go Marketplace page.
2. Click **Continue** > **Subscribe** > **Set Up Your Account**.
3. You are brought to the Deep Security as a Service account creation page. Fill out the form and click **Sign Up**.
4. You will receive an account confirmation email. Click the account activation link in the email.
5. Sign in to Deep Security as a Service using the company or account name and user name specified in the account confirmation email.

   Your subscription is now active.

Sign up with AWS - Annual + Pay as you Go billing

If you already have a Deep Security as a Service account

1. Go to the Trend Micro Deep Security as a Service | Annual + Pay as You Go

---

Marketplace page.
2. Click **Continue**.
3. Enter the number of instances to protect.
4. Select the contract term to protect your instances for and whether to automatically renew the contract at term end.
5. Click **Create Contract**.

   You are brought to the Deep Security Dashboard. Your subscription is now active.

If you do not have a Deep Security as a Service account

1. Go to the Trend Micro Deep Security as a Service | Annual + Pay as You Go Marketplace page.
2. Click **Continue**.
3. Enter the number of instances to protect.
4. Select the contract term to protect your instances for and whether to automatically renew the contract at term end.
5. Click **Create Contract**.
6. You will be brought to the Deep Security as a Service account creation page.
7. You will receive an account confirmation email. Click the account activation link in the email.
8. Sign in to Deep Security as a Service using the company or account name and user name specified in the account confirmation email.

   Your subscription is now active.

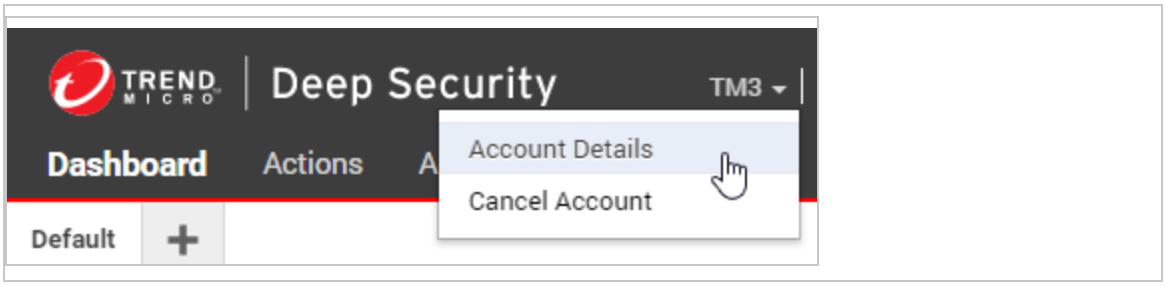
Sign up with Azure - Pay as you Go billing

If you already have a Deep Security as a Service account

1. Log in to Deep Security as a Service.

---

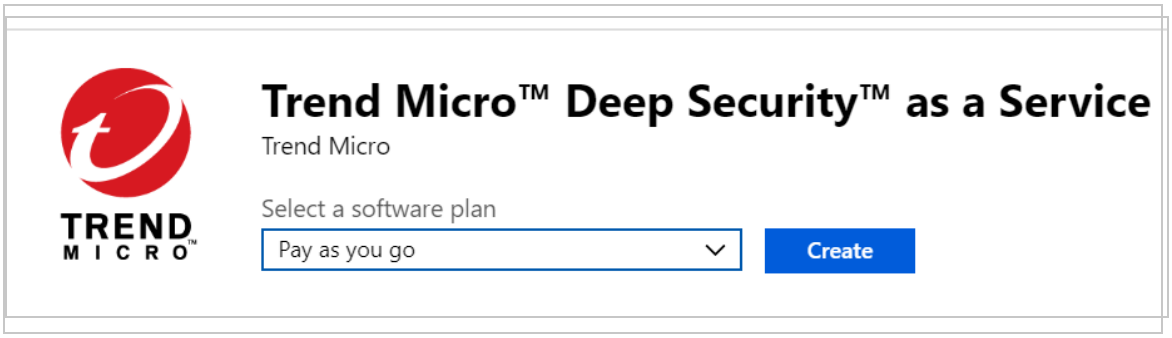
2. At the top of the page, click your account name (as shown below) and select **Account Details**.



3. Click **Upgrade to Paid**.
4. Click **Subscribe through Azure Marketplace**.

> **Note:** You are brought to the Azure Marketplace page for a Pay as you Go subscription.

5. Click **GET IT NOW**.
6. If prompted, log in to your Microsoft Azure account. This is the account that will be billed.
7. On the **One more thing** page, enable the **I give Microsoft permission to use or share my account information [...]** check box, and click **Continue**.
8. You are brought to the Deep Security as a Service page in Azure.
9. Select **Pay as you go** as your software plan and click **Create**.

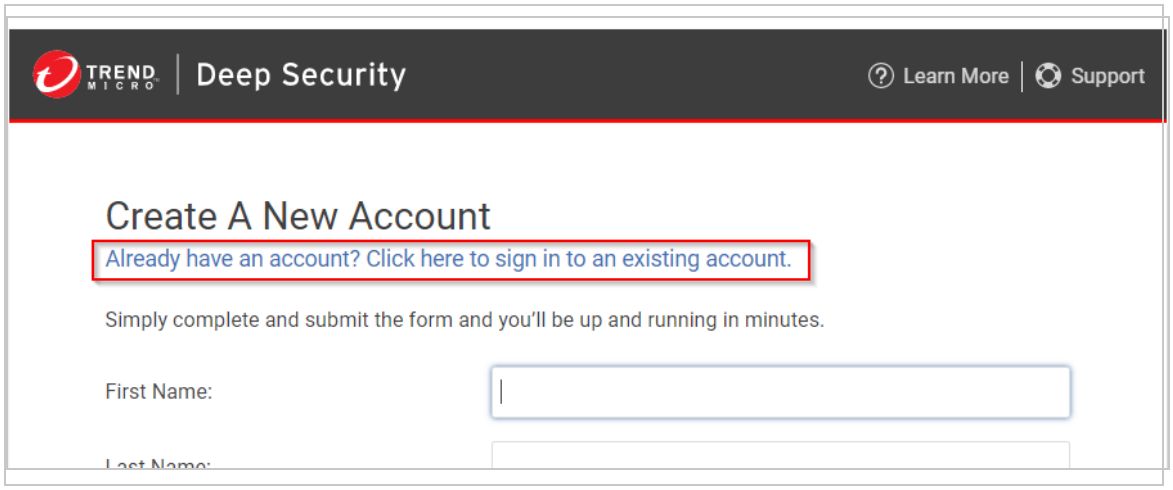


10. In the **Name** field, enter a Deep Security as a ServiceAzure account name. For example: `Example Inc - Deep Security as a Service`.
11. For the **Subscription**, select an Azure subscription.
12. For the **Plan**, make sure it is set to **Pay as you go**. (Pay as you go is the only supported option.)
13. For **Billing term**, make sure it is set to **Monthly**. (Monthly is the only supported option.)

14. Read and agree to the terms of use, then enter your preferred e-mail address and phone number.
15. Click **Subscribe**. It might take a few minutes to deploy your Security as a Service resource.
16. Use the top search bar to navigate to the **Software as a Service (SaaS)** page. If your account name hasn't appeared, click **Refresh**.
17. Click your account name (`Example Inc - Deep Security as a Service`) then **Configure Account**.

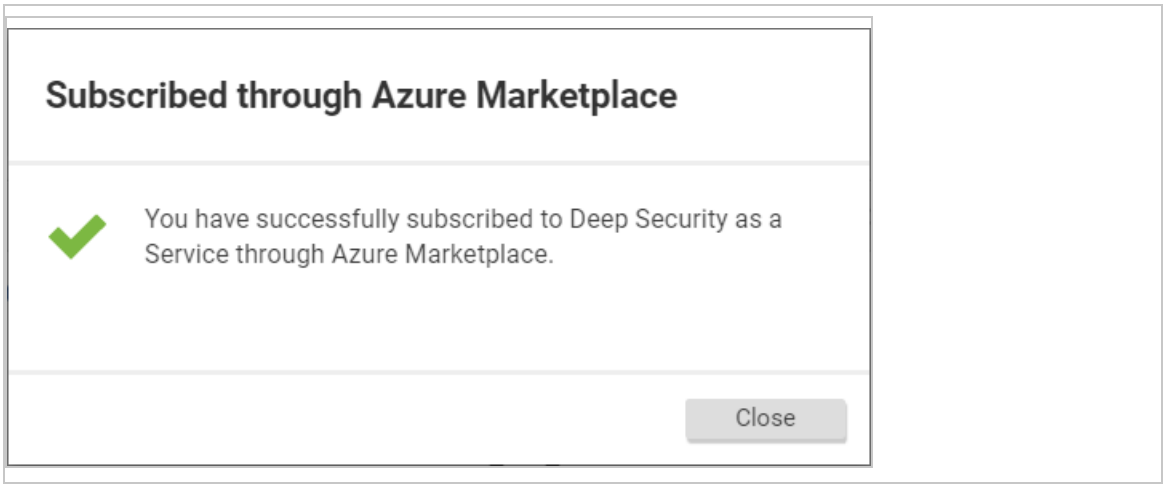
You are redirected to a **Create A New Account** page in Deep Security as a Service.

18. Click the **Already have an account?** link.



19. Sign in to your Deep Security as a Service account.

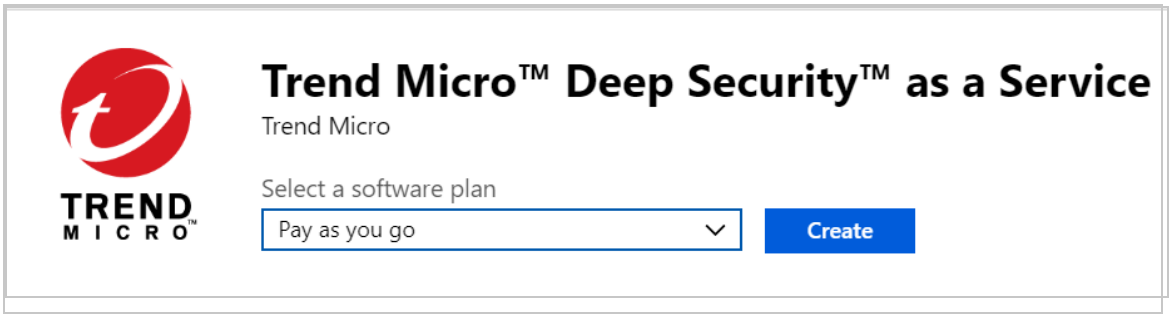
The following success message appears.



Your subscription is now active.

If you do not have a Deep Security as a Service account

1. Go to the Trend Micro Deep Security as a Service page on Azure Marketplace, and click **GET IT NOW**. You are navigated to the Microsoft Azure portal.
2. Select **Pay as you go** as your software plan and click **Create**.



3. Enter a name for your Deep Security as a Service Azure account. For example: `Example Inc - Deep Security as a Service`
4. Read and agree to the terms of use, then enter your preferred e-mail address and phone number.
5. Click **Subscribe**. It might take a few minutes to deploy your Security as a Service resource.
6. Navigate to the **Software as a Service (SaaS)** page. If your account name hasn't appeared, click **Refresh**.

---

7. Click your account name (`Example Inc - Deep Security as a Service`) then **Configure Account**, which redirects you to Deep Security as a Service to create a new account.

   You are redirected to a **Create A New Account** page in Deep Security as a Service.

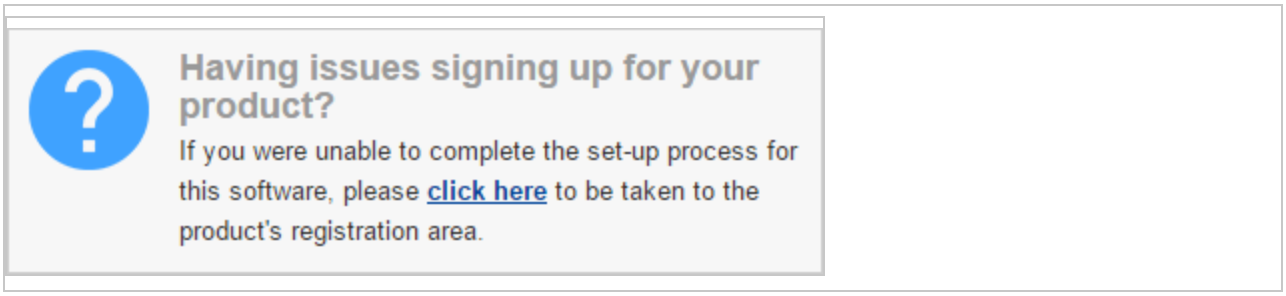
8. Enter your account information and click **Sign Up**.
9. Within a few minutes you will receive an email from Deep Security as a Service. Click the activation link in the email to activate your newly created Deep Security as a Service account.

Your subscription is now active.

Troubleshooting the sign-up on AWS

If you successfully subscribed to Trend Micro Deep Security as a Service with an AWS subscription but were unable to complete the Deep Security as a Service software setup process, follow the steps below:

1. Log in to your AWS Marketplace account.
2. Click **Your Software**.
3. Under the Trend Micro Deep Security as a Service product, click **Configure Software**.
4. Click **click here**.



Sign up with prepaid credit billing

1. Contact aws@trendmicro.com and a Trend Micro representative will connect you to someone in your region who can help you purchase prepaid credit and give you an activation code.

2. In Deep Security as a Service, click your account name and select **Account Details**.
3. Click **Upgrade to Paid**.
4. Enter your activation code and then click **Enter Activation Code**.

Sign up with BYOL billing

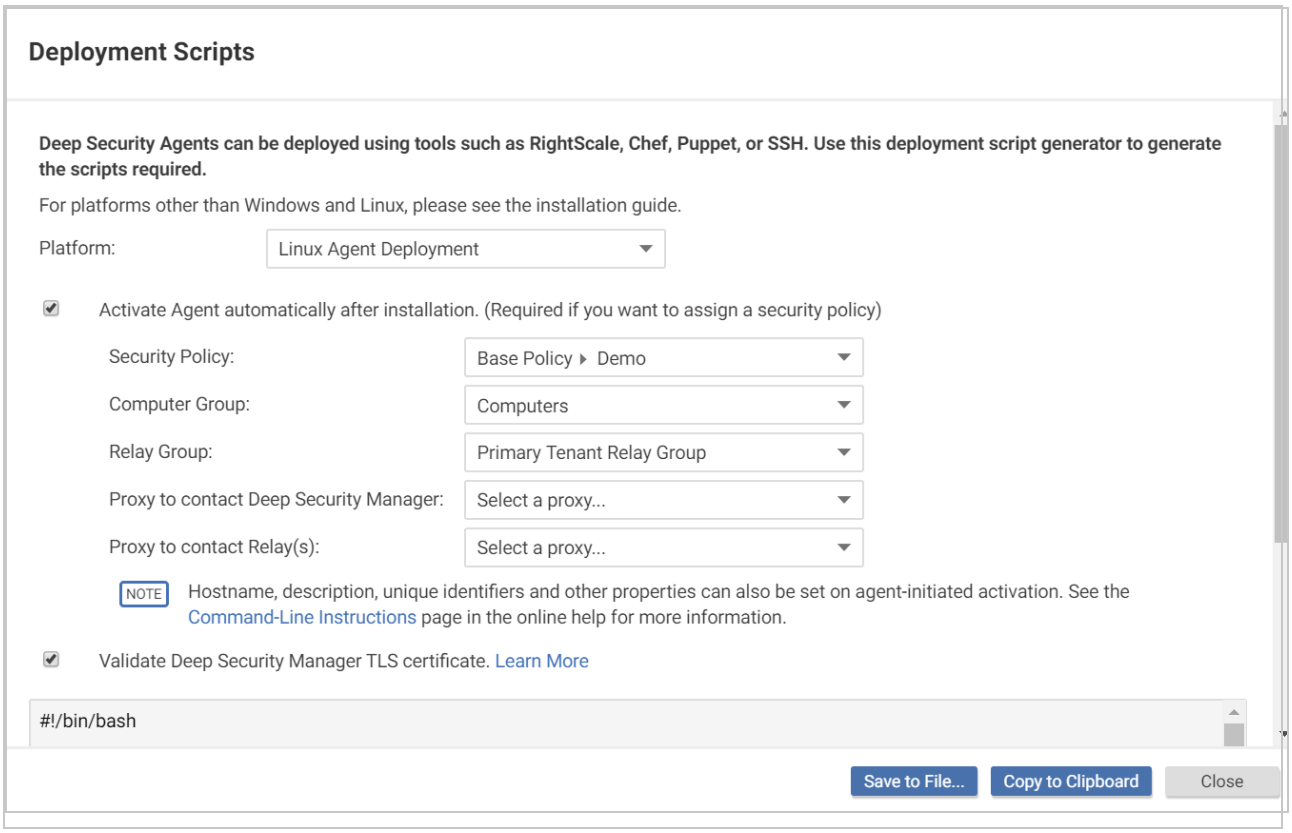
1. Contact aws@trendmicro.com and a Trend Micro representative will connect you to someone in your region who can help you purchase a bring-your-own-license (BYOL) license and give you an activation code.
2. In Deep Security as a Service, click your account name and select **Account Details**.
3. Click **Upgrade to Paid**.
4. Enter your activation code and then click **Enter Activation Code**.

Try the Deep Security demo

Note: If you'd prefer, you can watch Try the Deep Security as a Service demo application on Youtube.

You can try out the Deep Security demo application to learn how to add a protected computer and explore the various protection modules.

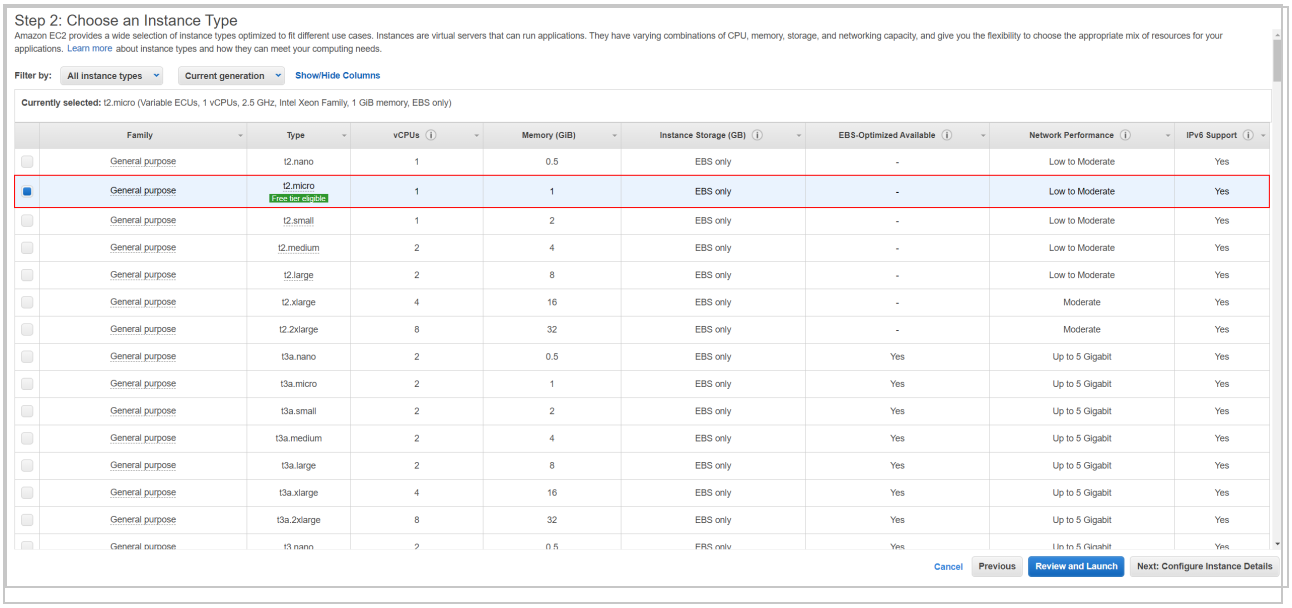
1. In Deep Security Manager, go to **Support > Deployment Scripts**. For more information about deployment scripts, see "Use deployment scripts to add and protect computers" on page 1013.
2. Set the **Platform** to **Linux Agent Deployment** and the **Security Policy** to **Base Policy > Demo**.
3. Copy the deployment script to your clipboard.



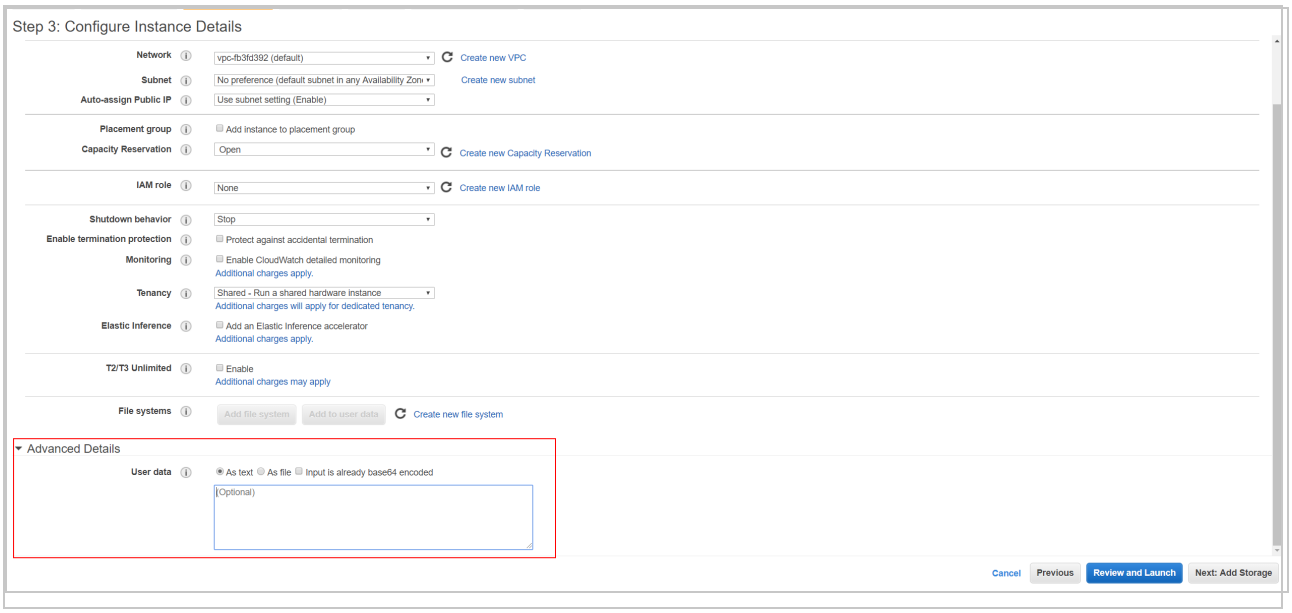
4. Navigate to your AWS console and go to **Services > Compute > EC2**.
5. Select **Instances** from the side-menu. Click **Launch Instance**.

6. Select **Ubuntu Server 18.04** from the list.

7. In **Choose an Instance Type**, select **t2.micro**. Click **Next: Configure Instance Details**.



8. In **Configure Instance Details**, choose a **Network** and **Subnet** that have public internet access.
9. Open the **Advanced Details** pane and paste the deployment script.

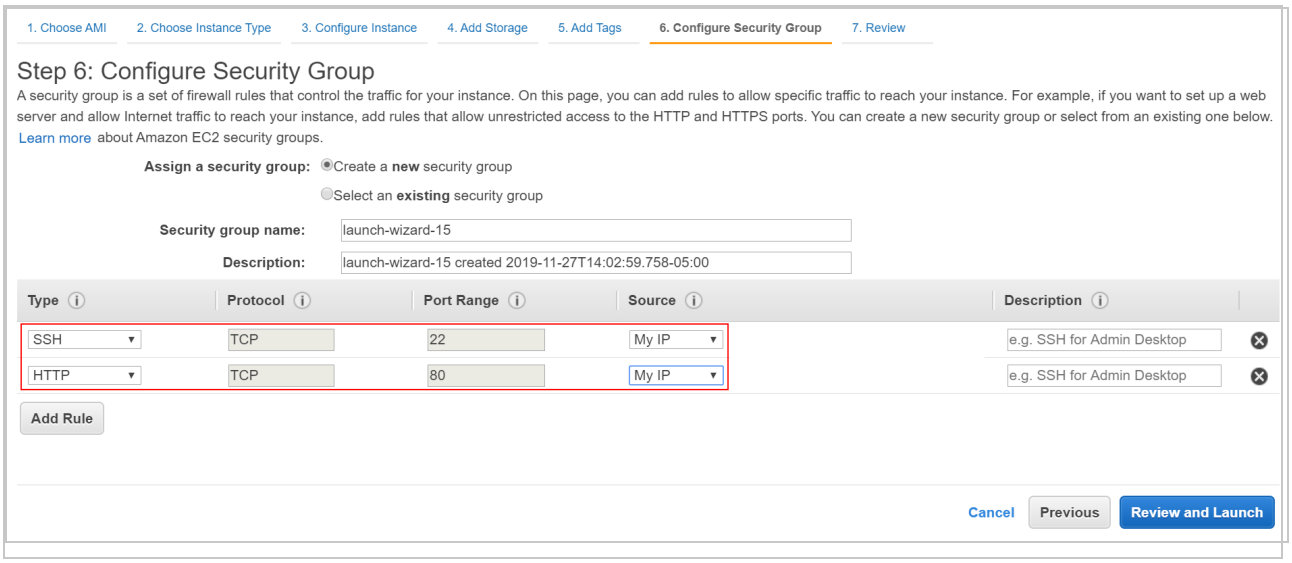


10. Under the deployment script, paste the following command:

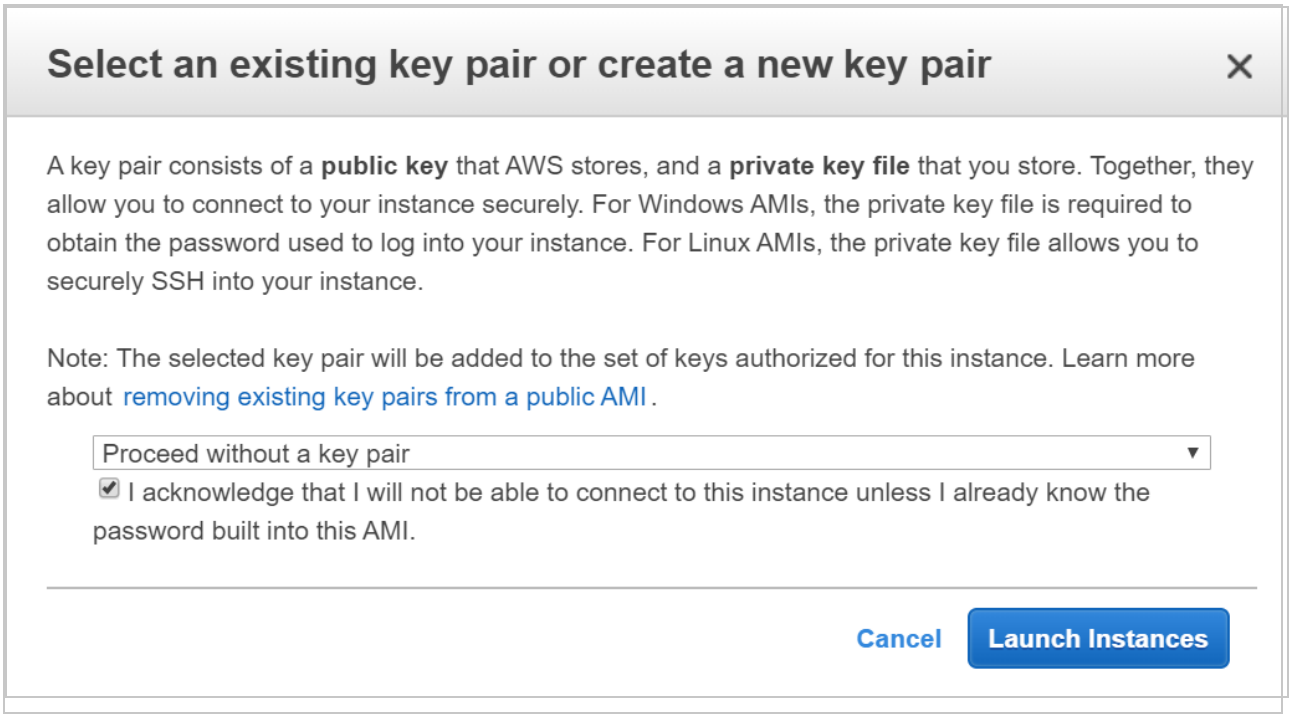
    ```
    curl https://raw.githubusercontent.com/deep-security/demo-app/master/demo-app.sh | sudo bash
    ```

    This will install and configure tomcat.

11. It is not necessary to add storage or tags, so click through to the **Configure Security Group** page.
12. Add an **SSH rule** and an **HTTP rule** and set the **Source** to **My IP**. This security group is the only thing blocking outside access to your instance until the Deep Security Agent is installed, which is why we highly recommend you only allow access from your IP address.



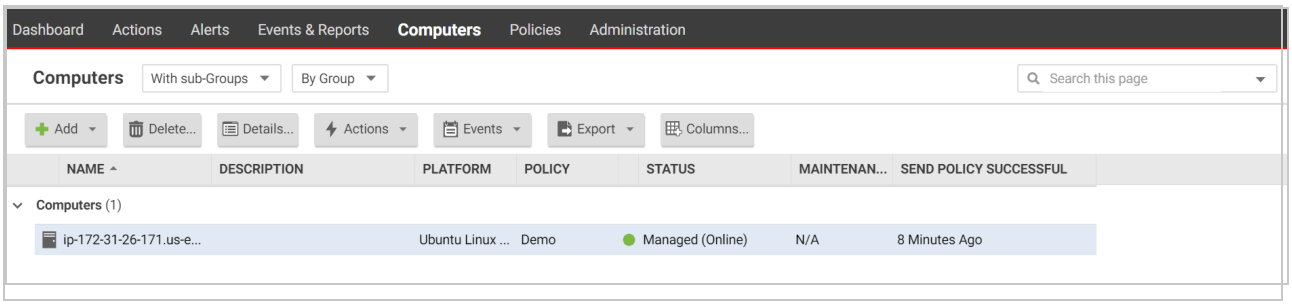
13. Click **Review and Launch**.
14. In the pop-up window, select **Proceed without a key pair**. Click **Launch Instance**.



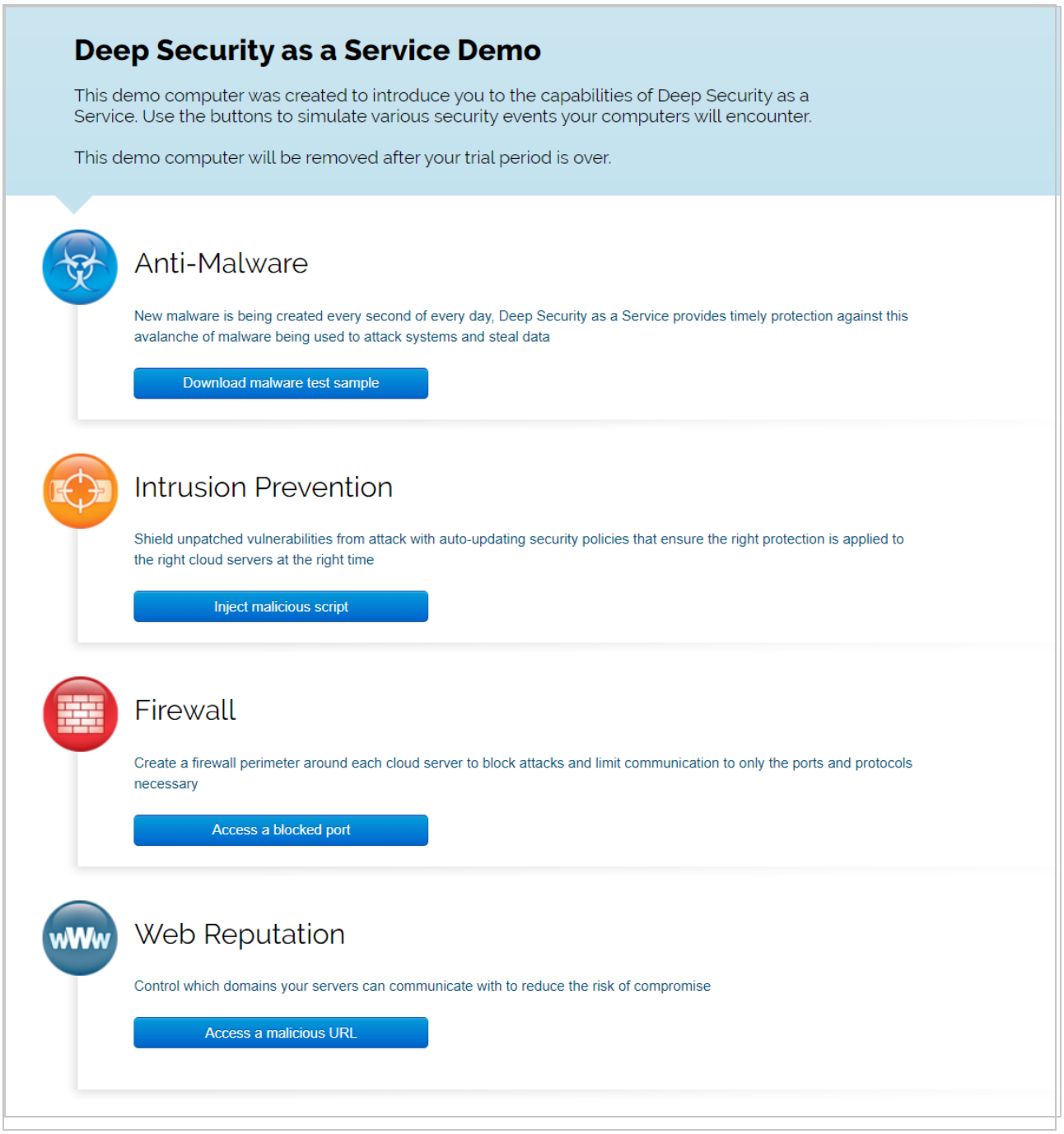
15. Click on the instance ID to navigate to the AWS console. Your instance and demo app will take about five minutes to launch and install.

    Once the instance is running and all the necessary checks are complete, you're ready to explore Deep Security Manager and Deep Security Agent!

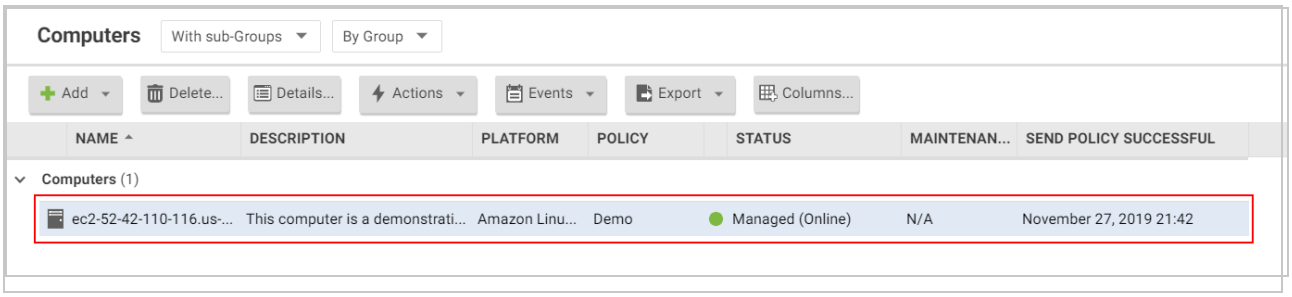
16. To view your new instance, go to **Deep Security Manager > Computers**. Your new instance should be displayed.



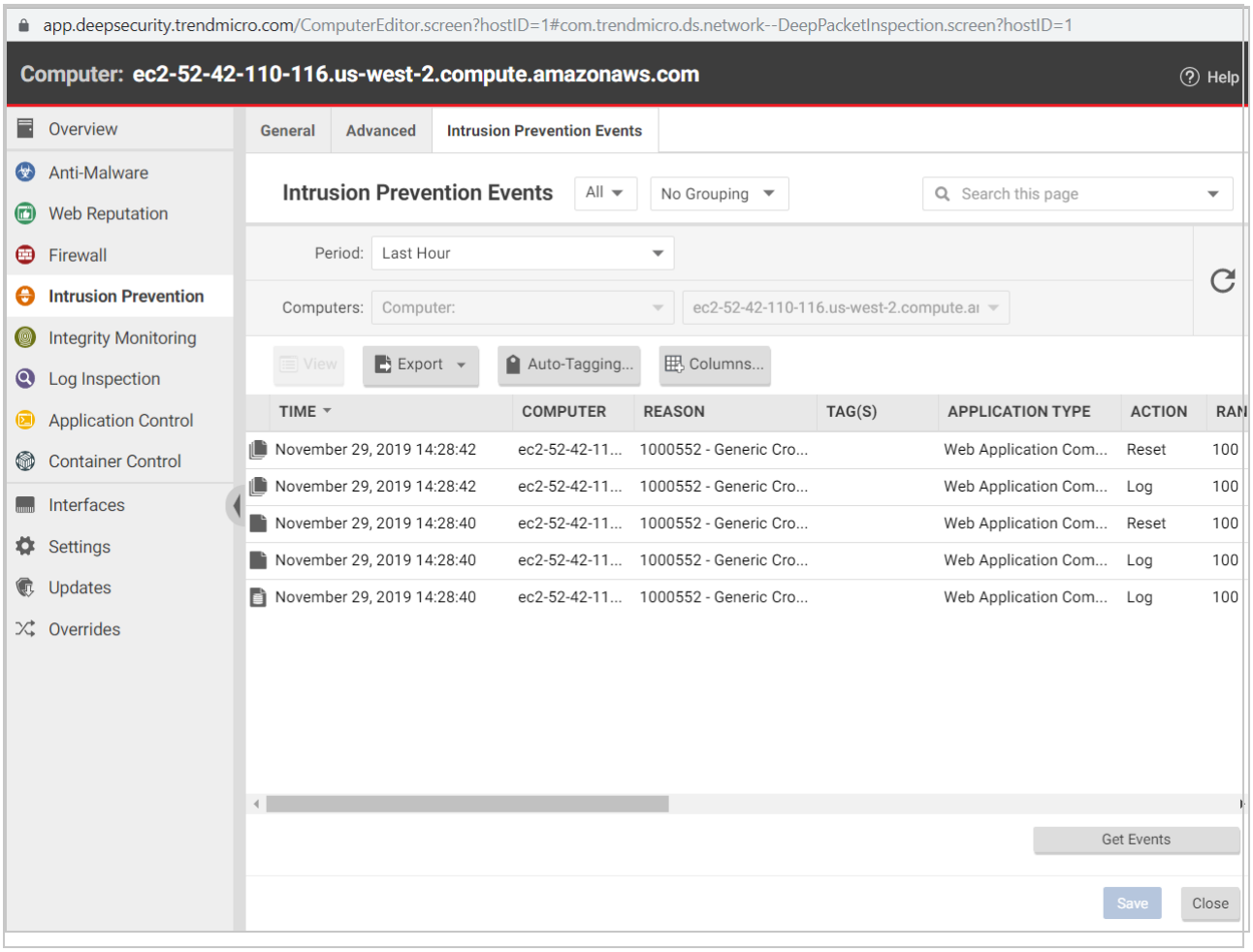
17. To access the demo application, go back to the AWS Instance page, copy your **Public DNS** and enter the URL into a browser with */demo-app* at the end.
18. Trigger the security module of your choice.



19. To view the security event, go to **Deep Security Manager > Computers** and double-click the demo computer.



20. In the pop-up window, select the security module that you triggered, then navigate to the **Events** page of that module.
21. If the event hasn't appeared, click **Get Events**. Double-click the event for more information.



Now you're ready to add an account of your own! For your next steps, see "Start protecting computers" on the next page.

Start protecting computers

If you haven't registered for a Deep Security as a Service account yet, you can sign up for a free 30 day trial account. Once your account is registered, you will need to:

1. "Add AWS EC2 instances to Deep Security" below, if they exist.
2. "Add Azure virtual machines to Deep Security" on the next page, if they exist.
3. "Add Google Cloud Platform (GCP) virtual machines to Deep Security" on the next page, if they exist.
4. "Deploy Deep Security agents to your AWS EC2 instances or Azure virtual machines" on the next page.
5. "Protect your instances with policies" on the next page

Tip: You can "Try the Deep Security demo" on page 127 to get familiar with the features of Deep Security before you start deploying.

Add AWS EC2 instances to Deep Security

Modify your AWS security group to allow outbound traffic over port 443

If you have AWS security groups that restrict outbound traffic, you need to allow outbound communication over port 443. To do so:

1. Log in to your Amazon Web Services Console and click **EC2**.
2. In the navigation pane, go to **Network & Security** > **Security Groups**.
3. On the Security Group page, select the security group associated with your instances and edit the outbound rules for the group to allow traffic to all IPs over port 443.

Note: You can also further restrict outbound traffic to only allow access to the "Deep Security as a Service IP addresses" on page 113 used by Deep Security Agents.

Add AWS EC2 instances

For details on how to add your AWS EC2 instances to Deep Security, see "About adding AWS accounts" on page 171.

Add Azure virtual machines to Deep Security

For instructions on how to add your Azure virtual machines to Deep Security, see "Add a Microsoft Azure account to Deep Security" on page 187.

Add Google Cloud Platform (GCP) virtual machines to Deep Security

For instructions on how to add your GCP virtual machines to Deep Security, see "Add a Google Cloud Platform account" on page 199.

Deploy Deep Security agents to your AWS EC2 instances or Azure virtual machines

Once you've added your AWS EC2 instances or Azure virtual machines to Deep Security, you need to install the Deep Security Agent on each instance to start protecting it. You can either "Use deployment scripts to add and protect computers" on page 1013 (recommended) or "Install the agent" on page 146.

Protect your instances with policies

Once you've installed the Deep Security Agent on your instances, you need to create policies and assign them to your instances to start protecting them.

Check digital signatures on software packages

Before you install Deep Security, you should 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 hasn't been corrupted or tampered with.

You should:

- "Check the signature on software ZIP packages" on the next page
- "Check the signature on installer files (EXE, MSI, RPM or DEB files)" on page 139

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 952 and Linux Secure Boot support for agents.

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:

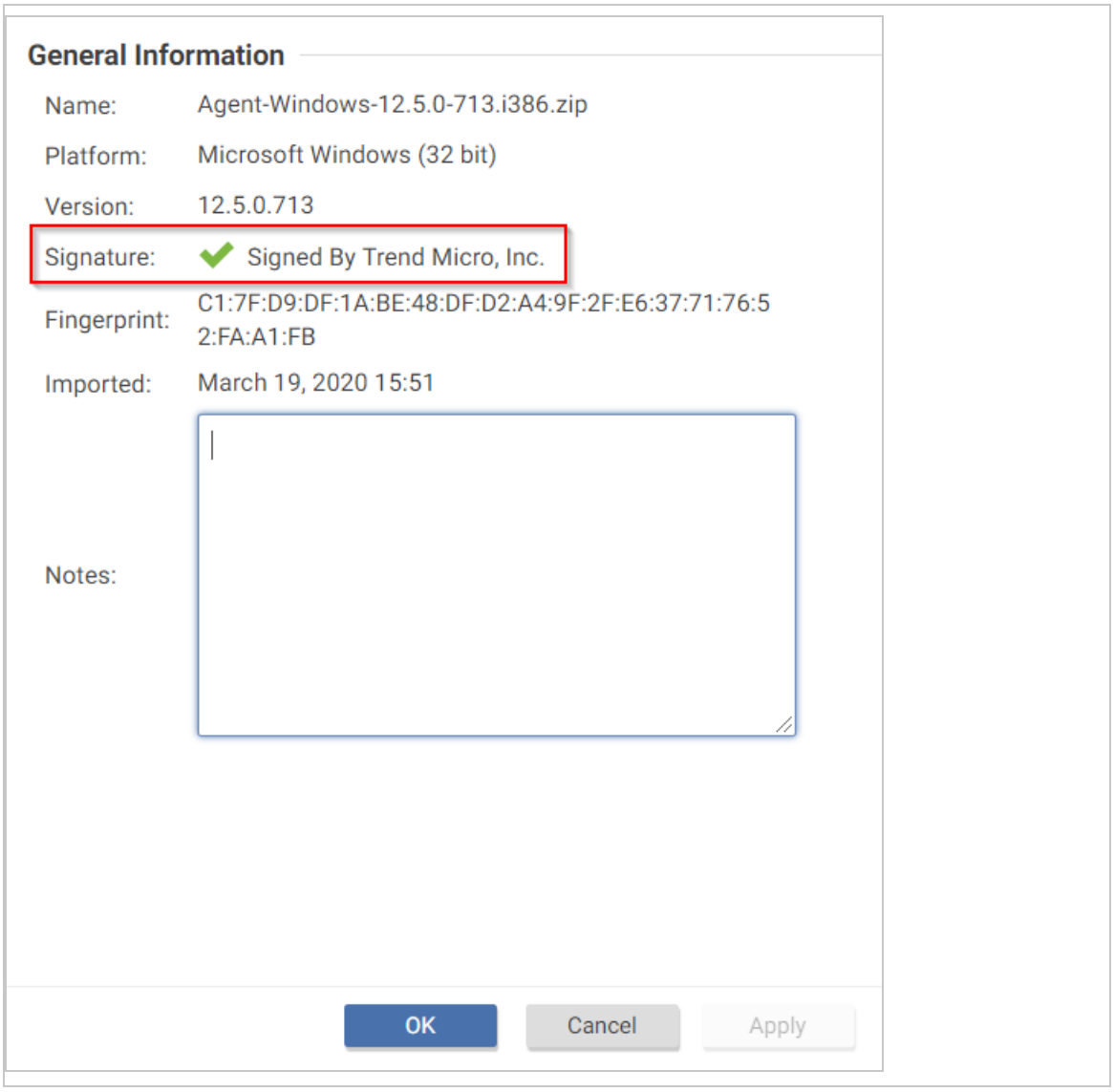
By exporting the ZIP from the manager

Export a ZIP file following the instructions in "Export the agent installer" on page 145.

On export, the manager checks the digital signature on the ZIP file. If the signature is good, the manager allows the export to proceed. If the signature is bad, or doesn't exist, 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 as a Service.
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.
5. The **Properties** page for the ZIP file opens, and the manager checks the digital signature. If the signature is good, you'll see a green check mark in the **Signature** field. (See image below.) If the signature is bad, or doesn't exist, the manager deletes the ZIP and logs an event.



By using jarsigner

Use the jarsigner Java utility to check a signature on a ZIP when you can't check it through the manager. For example, let's say 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'd 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 1013.

Follow the instructions that correspond to the type of installer file you want to check.

- "Check the signature on an EXE or MSI file" below
- "Check the signature on an RPM file" on the next page
- "Check the signature on a DEB file" on page 142

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

Install GnuPG 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'll need in order to import the signing key and check the digital signature.

Note: 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. (Optional) Verify the SHA-256 hash digest of the **ASC** file using any hashing utility. The hash is:

   ```
   c59caa810a9dc9f4ecdf5dc44e3d1c8a6342932ca1c9573745ec9f1a82c118d7
   ```

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 one is:

   ```
   gpg-pubkey-e1051cbd-5b59ac99
   ```

   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

> **Tip:** Instead of checking the signature on the RPM file manually, as described below, you can have a deployment script do it. See "Use deployment scripts to add and protect computers" on page 1013 for details.

Use this command:

```
rpm -K Agent-PGPCore-<OS agent version>.rpm
```

Example:

```
rpm -K Agent-PGPCore-RedHat_EL7-11.0.0-950.x86_64.rpm
```

Make sure you run the above command on the `Agent-PGPCore-<...>.rpm` file. (Running it on `Agent-Core-<...>.rpm` does not work.) If you cannot find the `Agent-PGPCore-<...>.rpm` file in the agent ZIP, you'll need to 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'll 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. (Optional) Verify the SHA-256 hash digest of the **ASC** file using any hashing utility. The hash is:

   ```
   c59caa810a9dc9f4ecdf5dc44e3d1c8a6342932ca1c9573745ec9f1a82c118d7
   ```

3. On the agent computer where you intend to check the signature, import the ASC file to the GPG keyring. Use this 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. (Optional) Display the Trend Micro key information. Use this 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

> **Tip:** Instead of verifying the signature on the DEB file manually, as described below, you can have a deployment script do it. See "Use deployment scripts to add and protect computers" on page 1013 for details.

Enter this 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 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.

Relays are already deployed inside the Deep Security as a Service environment, ready for use. To begin using these relays, simply verify that your computers can connect to the Deep Security as a Service listening port number.

Note: Under special circumstances, you may need to deploy additional relays in your own environment. For details, see "Deploy additional relays" on page 816.

Deploy Deep Security Agent

Get Deep Security Agent software

In this topic:

View a list of available agent software

To view a list of all available software:

1. In Deep Security as a Service, go to **Administration > Updates > Software > Local**. All available software appears.
2. (Optional) Organize the list of software by version or platform (OS) by selecting **Version** or **Platform** from the drop-down list at the top.

Export the agent installer

You can download the agent installer from Deep Security Manager.

1. In Deep Security Manager, go to **Administration > Updates > Software > Local**.
2. Select your agent from the list.

   Note: If you're looking for a Solaris agent, see "Solaris-version-to-agent-package mapping table" below 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 good, the export proceeds.

4. Save the agent installer. If you will install the agent manually, save it on the computer where you want to install Deep Security Agent.

Tip: To install Deep Security Agent, only use the exported agent installer (the .msi, .rpm, .pkg, .p5p, or .bff file depending on the platform) *not* 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 haven't 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*.)

Tip: 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 1013.

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.

Solaris-version-to-agent-package mapping table

If you're not sure which agent package to pick when exporting the agent, review the mapping table below.

Solaris-version-to-agent-package mapping table

If you're installing the agent on...	Choose this agent package...
Solaris 10 Updates 4-6 (64-bit, SPARC or x86)	Agent-Solaris_5.10_U5-xx.x.x-xxx.<sparc|.x86_64>.zip
Solaris 10 Updates 7-11 (64-bit, SPARC or x86)	Agent-Solaris_5.10_U7-xx.x.x-xxx.<sparc|.x86_64>.zip
Solaris 11.0 (1111)-11.3 (64-bit, SPARC or x86)	Agent-Solaris_5.11-xx.x.x-xxx.<sparc|.x86_64>.zip
Solaris 11.4 (64-bit, SPARC or x86)	Agent-Solaris_5.11_U4-xx.x.x-xxx.<sparc|.x86_64>.zip

- `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`. 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`. Example: `Agent-AIX_5.3-9.0.0-5625.powerpc.bff.gz.zip`.

For details on which agent you'll need for the version of AIX you're using, see "Deep Security Agent platforms" on page 80.

Install the agent

Topics:

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 105.
2. Allowed inbound and outbound communication to and from the agent on the appropriate port numbers. See "Deep Security port numbers" on page 107.
3. Exported the agent software from the manager. See "Export the agent installer" on page 145.

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, SUSE, Oracle Linux, 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 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 1013
- **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 158 and "Install the agent on Azure VMs" on page 161.

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 164
- "Assign a policy to a computer" on page 215

Install the agent on Amazon EC2 and WorkSpaces

Note: The Deep Security Agent only supports Amazon WorkSpaces Windows desktops–it does not support Linux desktops.

Read this page if you want to protect *existing* Amazon EC2 instances and Amazon WorkSpaces with Deep Security.

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 158.
- protect Amazon WorkSpaces after already protecting your Amazon EC2 instances, see instead "Protect Amazon WorkSpaces if you already added your AWS account" on page 178.

To protect your existing Amazon EC2 instances and Amazon WorkSpaces with Deep Security, follow these steps:

1. "Add your AWS accounts to Deep Security Manager" below
2. "Configure the activation type" on the next page
3. "Open ports" on page 155
4. "Deploy agents to your Amazon EC2 instances and WorkSpaces" on page 155
5. "Verify that the agent was installed and activated properly" on page 156
6. "Assign a policy" on page 157

Add your AWS accounts to Deep Security Manager

You'll 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 171 for details.

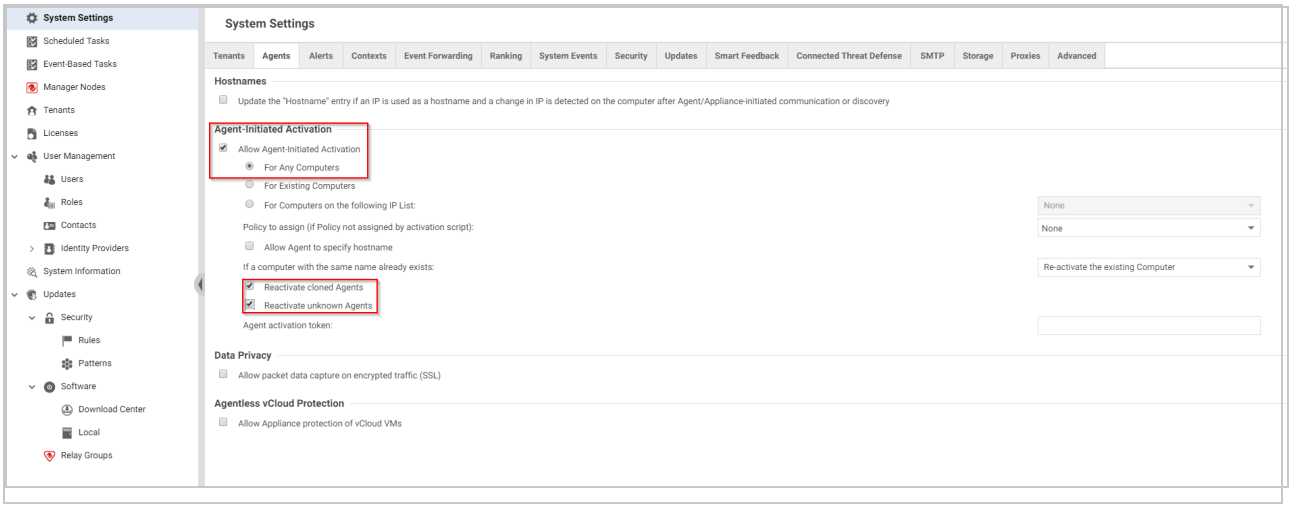
After adding your AWS accounts:

- 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.

Configure the activation type

'Activation' is the process of registering an agent with a manager. You'll need to indicate whether you'll 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. In the main pane, make sure the **Agents** tab is selected.
5. Select or deselect **Allow Agent-Initiated Activation**, noting that:
   - 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.
6. If you selected **Allow Agent-Initiated Activation**, also select **Reactivate cloned Agents**, and **Enable Reactivate unknown Agents**. See "Agent settings" on page 863 for more information.
7. Click **Save**.
8. If you're using Amazon WorkSpaces, and you *didn't* allow agent-initiated activation, manually assign an elastic IP address to each WorkSpace now, before proceeding with further steps on this page. 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.



Open ports

You'll need to make sure that the necessary ports are open to your Amazon EC2 instances or Amazon WorkSpaces.

To open ports:

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. See "Which ports should be opened?" below 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 listed above.

You have now opened the necessary ports so that Deep Security Agent and Deep Security Manager can communicate.

Which ports should be opened?

Generally-speaking:

- 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).

More specifically:

- If you enabled **Allow Agent-Initiated Activation**, you'll need to open the *outbound* TCP port (443 or 80, by default)
- If you disabled **Allow Agent-Initiated Activation**, you'll need to open the *inbound* TCP port of 4118.

Deploy agents to your Amazon EC2 instances and WorkSpaces

You'll need to deploy agents onto your Amazon EC2 instances and Amazon WorkSpaces. Below are a couple of options.

- **Option 1: Use a deployment script to install, activate, and assign a policy**

  Use Option 1 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 1013 for details.

  OR

- **Option 2: Manually install and activate**

  Use Option 2 if you only need to deploy agents to a few EC2 instances and Amazon WorkSpaces.

  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 144, and "Install the agent" on page 146.

  b. Activate the agent. You can do so on the agent (if agent-initiated activation was enabled) or on the Deep Security Manager. For details, see "Activate the agent" on page 164

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 Option 1 (you used a deployment script), a policy was assigned to the agent during activation. If you chose Option 2 (you manually installed and activated the agent), then no policy has been assigned, and you will need to assign one following the instructions further down on this page.

Verify that the agent was installed and activated properly

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 navigation pane 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. 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 215.

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 152.
- protect Amazon WorkSpaces after already protecting your Amazon EC2 instances, see instead "Protect Amazon WorkSpaces if you already added your AWS account" on page 178.

'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. "Configure the activation type" on the next page
3. "Launch a 'master' Amazon EC2 instance or Amazon WorkSpace" on the next page
4. "Deploy an agent on the master" on the next page
5. "Verify that the agent was installed and activated properly" on the next page
6. "(Recommended) Set up policy auto-assignment" on page 160
7. "Create an AMI or custom WorkSpace bundle based on the master" on page 161
8. "Use the AMI" on page 161

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 171 for details.

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 152 > "Configure the activation type" on page 154 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 152 > "Deploy agents to your Amazon EC2 instances and WorkSpaces" on page 155 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 853.

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 152 > "Verify that the agent was installed and activated properly" on page 156 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 by AWS instance tags" on page 1024.

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 164
   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

- 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 1013.
- 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**.

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 as a Service. For instructions, see "Add a Google Cloud Platform account" on page 199.
2. Configure agent-initiated activation (AIA). For instructions, see "Activate and protect agents using agent-initiated activation and communication" on page 852.
3. 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 106. For instructions on how to open ports, see this GCP webpage.
4. 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: Use a deployment script to	You need to deploy many agents to your GCP VMs.	See "Use deployment scripts to add

Option	Use if...	Instructions
install, activate, and assign a policy to the agent		and protect computers" on page 1013 for instructions.
Option 2: 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 144 b. Activate the agent. You can do so on the agent or on the Deep Security Manager. For details, see

Option	Use if...	Instructions
		"Activate the agent" below

5. 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.
6. Assign a policy if you installed and activated the agent manually. For instructions, see "Assign a policy to a computer" on page 215. 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 1013 or "Install the agent" on page 146 for instructions.

Before the installed agent can protect its computer or be converted to a relay, you must activate the agent with Deep Security as a Service. Activation registers the agent with Deep Security as a Service during an initial communication.

To do this, you can either:

- Activate the agent through a deployment script. See "Use deployment scripts to add and protect computers" on page 1013 for details.
- Activate the agent from the computer where the agent is installed. Run this command:
  `dsa_control -a dsm://agents.deepsecurity.trendmicro.com:443/ "tenantID:<tenant ID>" "token:<token>"`
  To find the appropriate values for `<tenant ID>` and `<token>`, in the Deep Security as a

Service console, go to **Support > Deployment Scripts**, scroll to the end of the script that is generated, and copy the `tenantID` and `token` values.
For details on this command, including additional parameters, see "Command-line basics" on page 973.

- 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 993.

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`

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`

---

[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).

Using systemd commands:

- Start: `systemctl start ds_agent`
- Stop: `systemctl stop ds_agent`

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 922.

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 973.

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 987.
- **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 AWS instances

About adding AWS accounts

Topics:

Overview of methods for adding AWS accounts

There a few ways to add AWS accounts to Deep Security as a Service:

- "Add an AWS account using the quick setup" on page 173. Use this method to add one or more AWS accounts quickly.
- "Add an AWS account using a cross-account role" on page 174. Use this method if you want to add multiple AWS accounts, or if you don't want to use the quick setup.

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 as a Serviceand 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.

Note: 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.

What are the benefits of adding an AWS account?

The 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**), are:

- 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.
- Your EC2 and WorkSpace instances are billed at the appropriate rate.

What AWS regions are supported?

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 whether your region uses the global service, see this table.

At the time or writing, the following regions do **not** use the global IAM service (`iam.amazonaws.com`):

- China (Beijing)
- China (Ningxia)
- AWS GovCloud (US-East)
- AWS GovCloud (US)

For the regions listed above, and any others that might not use the global IAM service, you can still load your EC2 and WorkSpace instances into the manager using the Deep Security REST API. Trend Micro has provided this sample script for your use.

Add an AWS account using the quick setup

Quick setup is the easiest way to add an AWS account because it uses an AWS CloudFormation template to automate the setup. You can run through the quick setup several times to add multiple AWS accounts.

To add an AWS account:

1. In the Deep Security Manager, go to **Computers** and click **Add > Add AWS Account**.
2. Select **Quick**.
3. Click **Next**. A page appears that describes what happens during the setup process with a URL. The URL is valid for one hour.
4. Click **Next**.
5. If you have not already signed into your AWS account you are prompted to do so.
6. Click **Next** on the **Select Template** page to accept the defaults.
7. If your organization uses tags, you can add them on the **Options** page.
8. Click **Next**.
9. On the **Review** page, select the check box next to **I acknowledge that this template might cause AWS CloudFormation to create IAM resources**.
10. Click **Create**.When AWS CloudFormation finishes setting up a cross-account role, the Deep Security Manager wizard displays a success message. You can close the screen before the success message is displayed. The account is added to Deep Security

immediately after the cross-account role is set up. For more information on how this is done, see "What does the Cloud Formation template do when I add an AWS account?" on page 184

11. If your AWS account includes Amazon WorkSpaces, and you want to protect them with Deep Security, go to Deep Security Manager, right-click your AWS account on the left, and select **Properties**. Enable **Include Amazon WorkSpaces** and click **Save**. 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.

Tip: If your account does not appear as a sub-folder under the **Computers** folder on the left within 10 minutes, or if an error message appears saying that the account could not be added, refer to "Issues adding your AWS account to Deep Security" on page 1072 for troubleshooting tips.

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, or if you want to add a single account but don't want to use the quick setup method.

The instructions below assume you want to add an AWS account with this name:

- 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 178 for details.

First, note the Deep Security as a Service account ID

Deep Security as a Service Account ID: `147995105371`

You'll need this ID later, when creating the cross-account role.

Next, configure the manager instance role

---

1. In Deep Security as a Service, click **Administration** at the top.
2. Click **System Settings** on the left.
3. Click the **Advanced** tab in the main pane.
4. Scroll to the bottom and look for the **Manager AWS Identity** section.
5. Make sure **Use Manager Instance Role** is selected.
6. Click **Save**.

Next, retrieve the external ID

1. Log in to Deep Security as a Service.
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 181
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

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 Deep Security as a Service account ID. It is: `147995105371`
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 of the AWS Primary Account.

Next, add AWS Account A to the manager

1. Log in to Deep Security as a Service.
2. Click **Computers** at the top.
3. Click **Add > Add AWS Account**.
4. Select **Advanced** and click **Next**.
5. Select **Use Cross Account Role**.
6. 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`
7. 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.
8. 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 181
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 https://success.trendmicro.com/solution/000241973 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.
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 152 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 158 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 174. 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 152
- 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 158.

Manage an AWS account

Topics:

- "Synchronize an AWS account" below

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 as a Service 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 as a Service, 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?

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 174 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 as a Service.
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 as a Service, 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 174 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.

Warning: Disabling retrieval of the external ID also disables the quick setup method of adding AWS accounts.

To disable retrieval:

1. Log in to Deep Security as a Service.
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 874.

Protect an account running in AWS Outposts

Deep Security supports AWS accounts running on AWS Outposts.

To protect your AWS accounts in Outposts:

1. . "Add an AWS account using the quick setup" on page 173.

   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 152.
3. "Activate the agent" on page 164.
4. "Create policies" on page 212.

What does the Cloud Formation template do when I add an AWS account?

The AWS Cloud Formation template creates a cross-account role that has both a unique external ID and a policy that allows Deep Security to access your AWS resources.

To accomplish this, the template first creates a temporary role with the necessary Deep Security permissions. Using this role, it starts Lambda functions that perform the following actions:

1. Creates the cross-account role for Deep Security.
2. Obtains the Amazon Resource Name (ARN) of the cross-account role.
3. Sends the ARN to the Deep Security API.

Note: The Lambda functions cannot delete the original temporary role: after your AWS account has been added to Deep Security, you must remove it by deleting the Cloud Formation stack.

For more details, you can view the content of the Cloud Formation template directly in AWS by editing it during the template selection process.

Add Azure instances

Create an Azure app 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 the Azure Active Directory and the Subscription Owner role for the Azure subscription. As an alternative, you can create an Azure app for the Deep Security Manager that provides read-only access to Azure resources.

Tip: If you have multiple Azure subscriptions, you can create a single Deep Security Azure app for all of them, as long as the subscriptions all connect to the same Active Directory. Details are provided within the set of instructions below.

To create an Azure app, you will need to:

1. "Assign the correct roles" below.
2. "Create the Azure app" on the next page.
3. "Record the Azure app ID, Active Directory ID, and password" on the next page.
4. "Record the Subscription ID(s)" on the next page.
5. "Assign the Azure app a role and connector" on page 187.

Assign the correct roles

To create an Azure app, your account must have the User Administrator role for the Azure Active Directory and the User Access Administrator role for the Azure subscription. Assign these roles to your Azure account before proceeding.

Create the Azure app

1. In the **Azure Active Directory** 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 app appears in the **App registrations** list with the **Name** you chose in Step 3 (above).

Record the Azure app ID, Active Directory ID, and password

1. In the **App registrations** list, click the Azure app.

   Note: The Azure app will display with the **Name** you chose for it in Step 3 of the "Create the Azure app" above procedure.

2. Record the **Application (client) ID**.
3. Record the **Active Directory ID**
4. Click **Certificates & secrets**.
5. Click **New client secret**.
6. Enter a **Description** for the client secret.
7. Select an appropriate **Duration**. The client secret expires after this time.
8. Click **Add**.

   The client secret **Value** appears.

9. Record the client secret **Value**. This will be used as the Application Password when registering the Azure app with Deep Security.

   Warning: The client secret **Value** only appears once, so record it now. If you do not, you must regenerate it to obtain a new **Value**.

   Note: If the client secret **Value** expires, you must regenerate it and update it in the associated Azure accounts.

Record the Subscription ID(s)

1. On the left, go to **All Services** and click **Subscriptions**.

   A list of subscriptions appears.

2. Record the **Subscription ID** of each subscription you want to associate with the Azure app. You will need the ID(s) later, when adding the Azure account(s) to Deep Security.

Assign the Azure app a role and connector

1. Under **All Services > Subscriptions**, click a subscription that you want to associate with the Azure app.

   Note: You can associate another subscription with the Azure app 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 drop-down menu.
4. Under **Role**, enter `Reader` and then click the **Reader** role that appears.
5. Under **Assign access to**, select **Azure AD user, user group, or service principal**.
6. Under **Select**, enter the Azure app **Name** (for example, `Deep Security Azure Connector`).

   The Azure app appears with the **Name** you chose for it in Step 3 of the "Create the Azure app" on the previous page procedure.

7. Click **Save**.
8. If you want to associate the Azure app to another subscription, repeat this procedure ("Assign the Azure app 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" below.

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?

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**.

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:
   - **Active Directory ID**
   - **Subscription ID**
   - **Application ID**
   - **Application Password**

   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. Click **Next**.
5. Review the summary information, and then click **Finish**.
6. 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 922 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 as a Service (DSaaS) and 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 1064

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 200.

Topics:

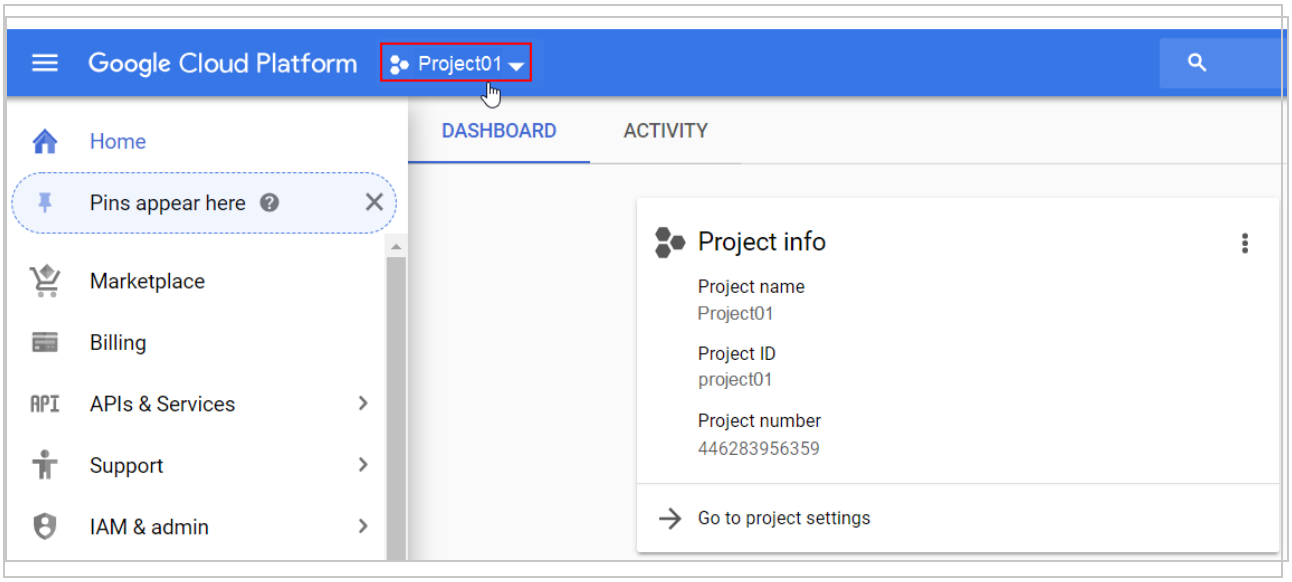
Prerequisite: Enable the Google APIs

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`



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

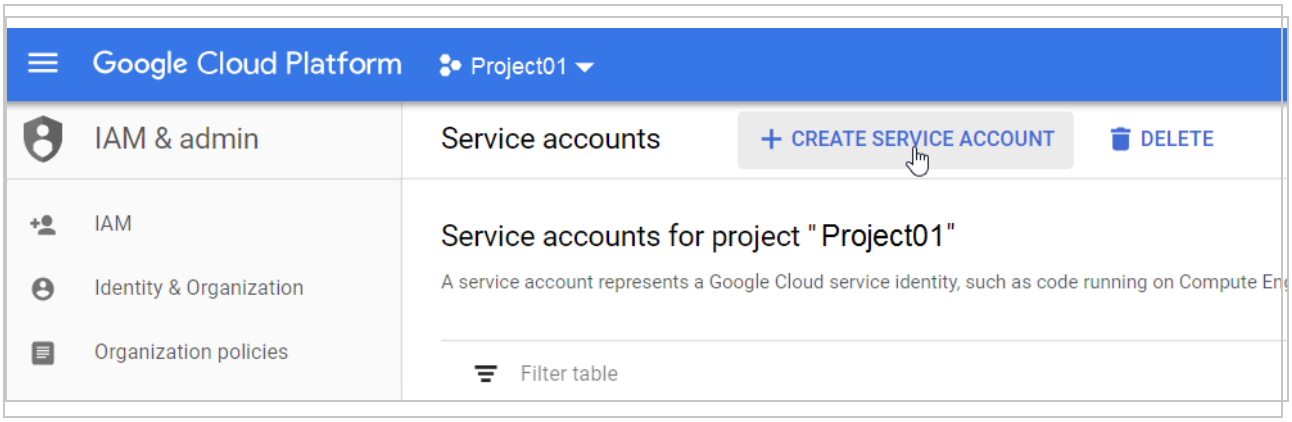
Create a GCP service account

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.

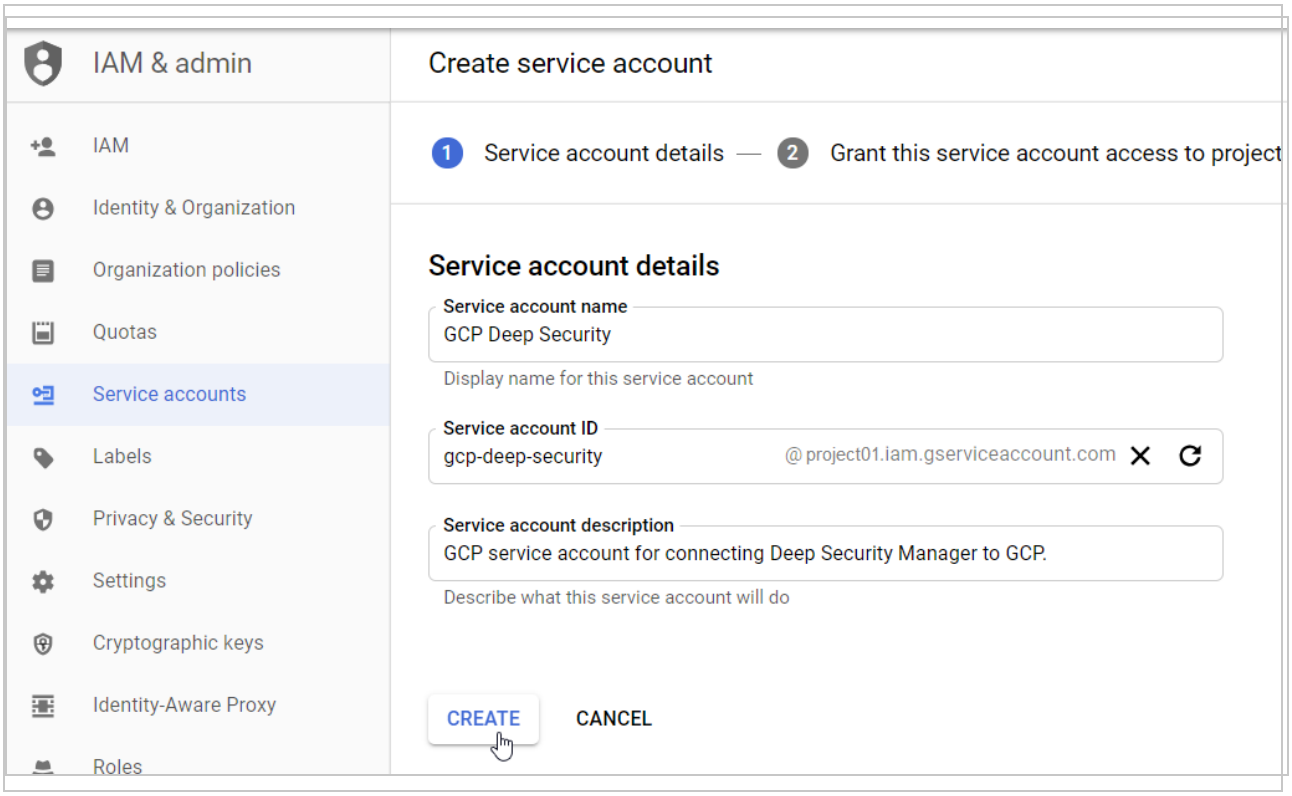
Follow the procedure below to create a service account for Deep Security Manager:

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**.



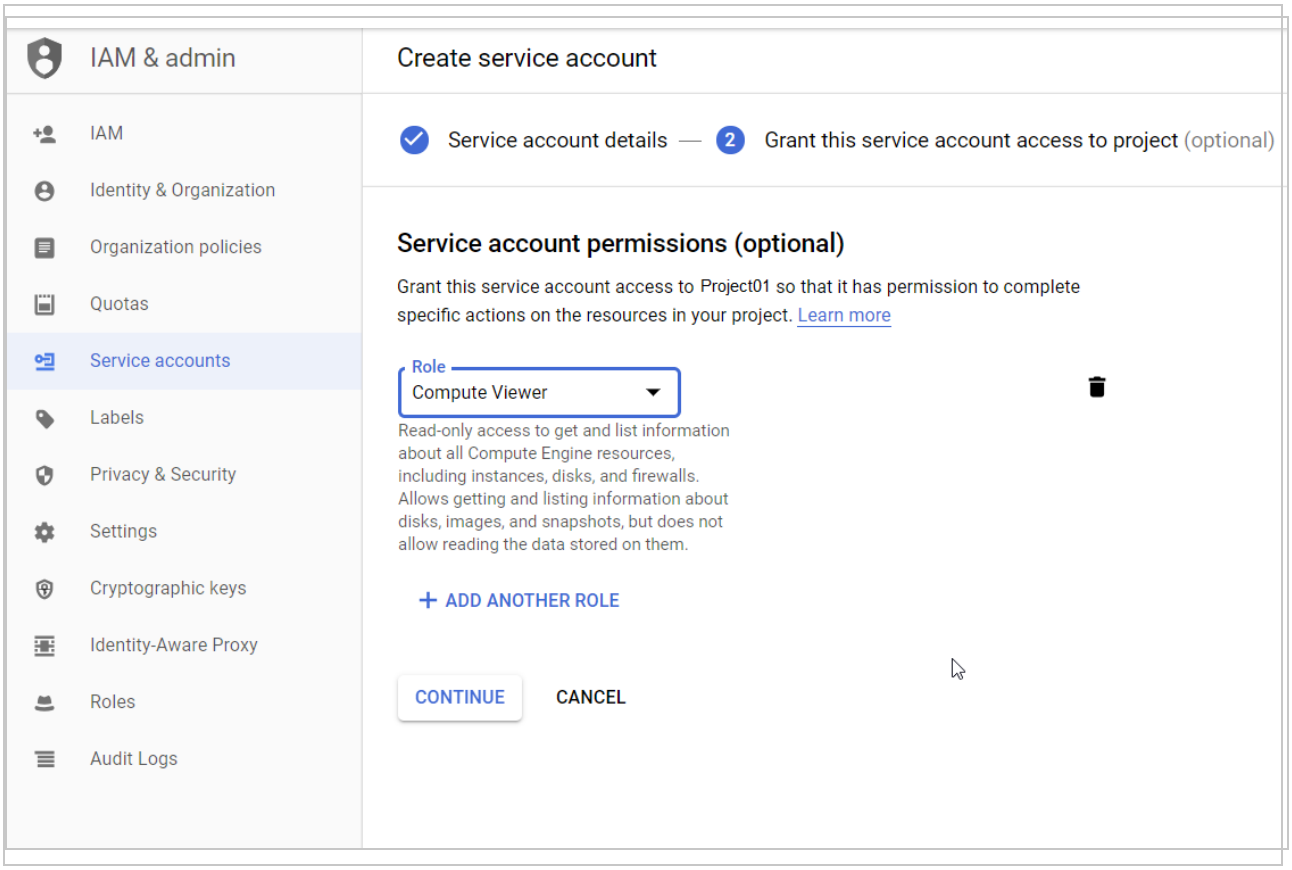
7. Enter a service account name, ID and description.



For example:

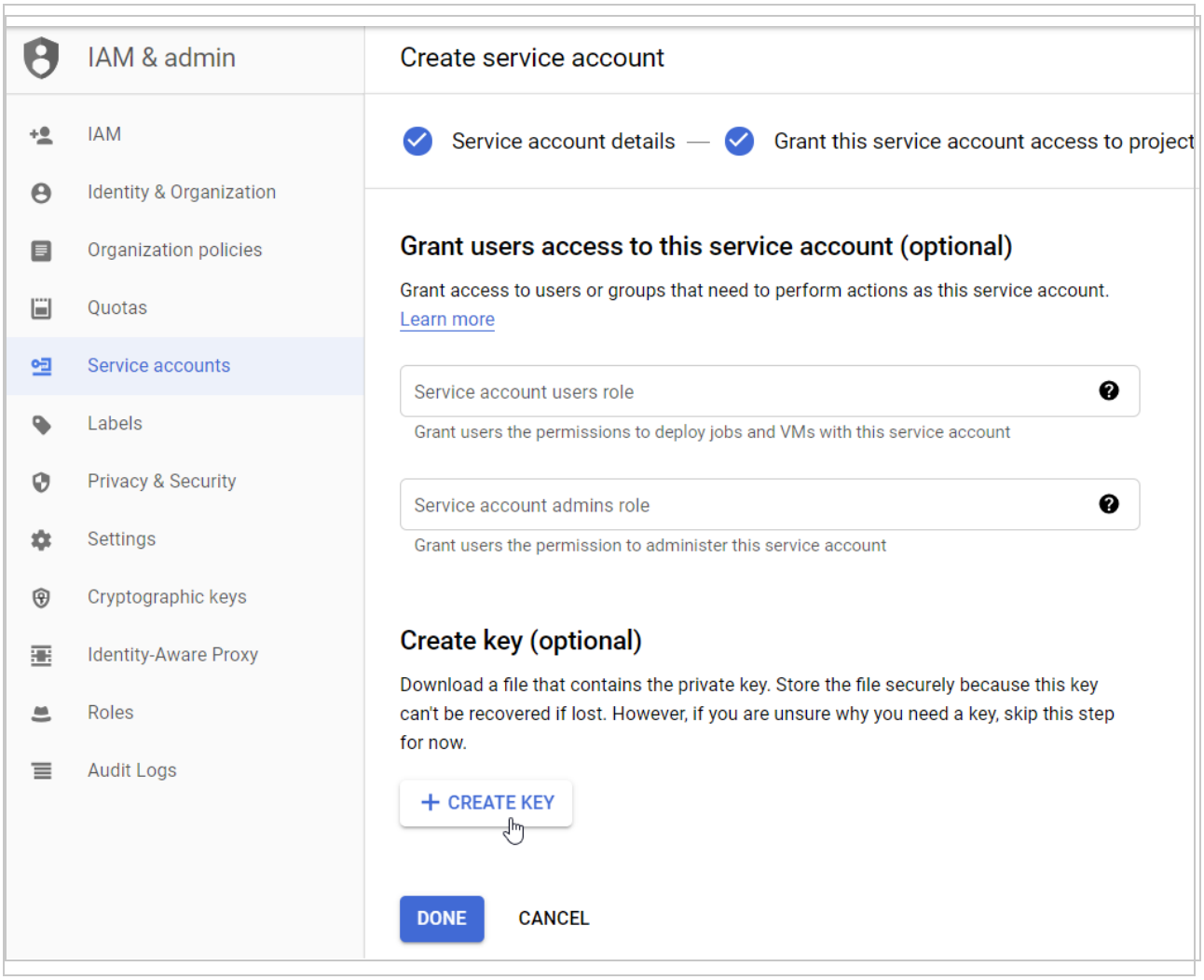
- Service account name: `GCP Deep Security`
- Service account ID: `gcp-deep-security@<your_project_ID>.iam.gserviceaccount.com`
- Service account description: `GCP service account for connecting Deep Security Manager to GCP.`

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**.

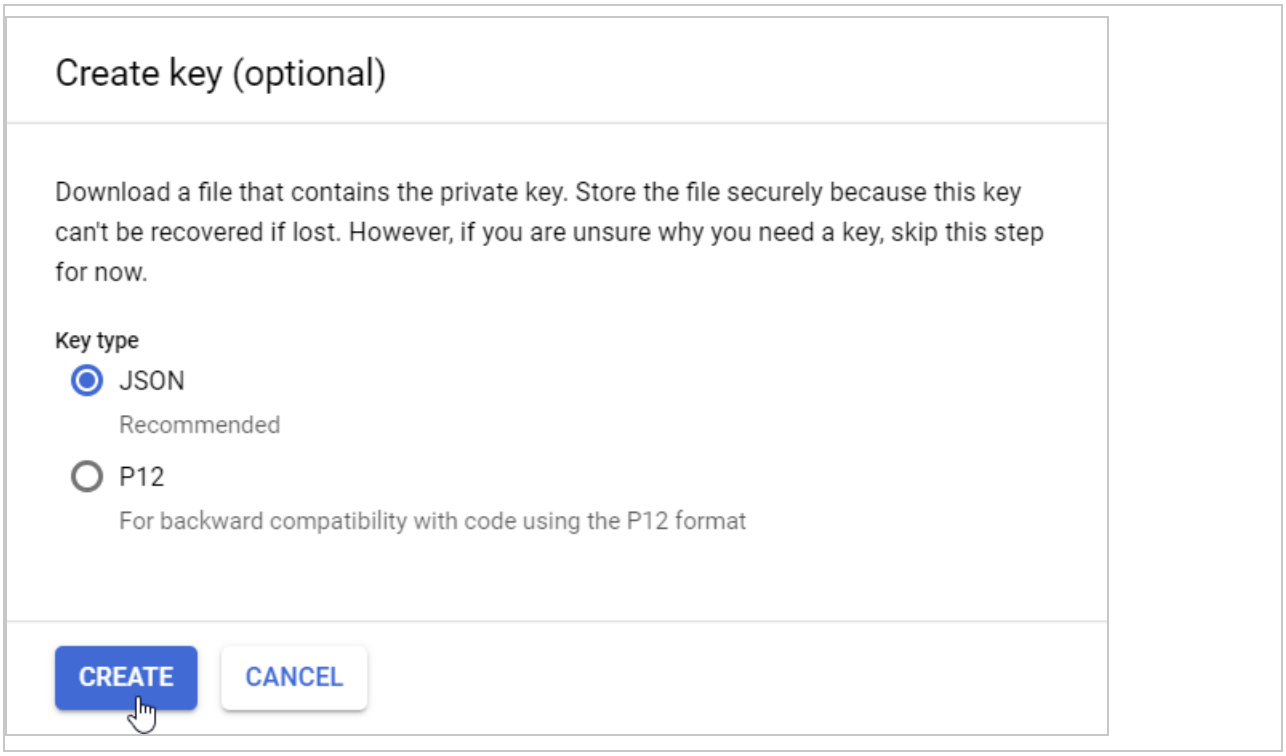


You have now assigned the Compute Viewer role.

11. Click **+ CREATE KEY**.



12. Select **JSON** and click **CREATE**.



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 199.

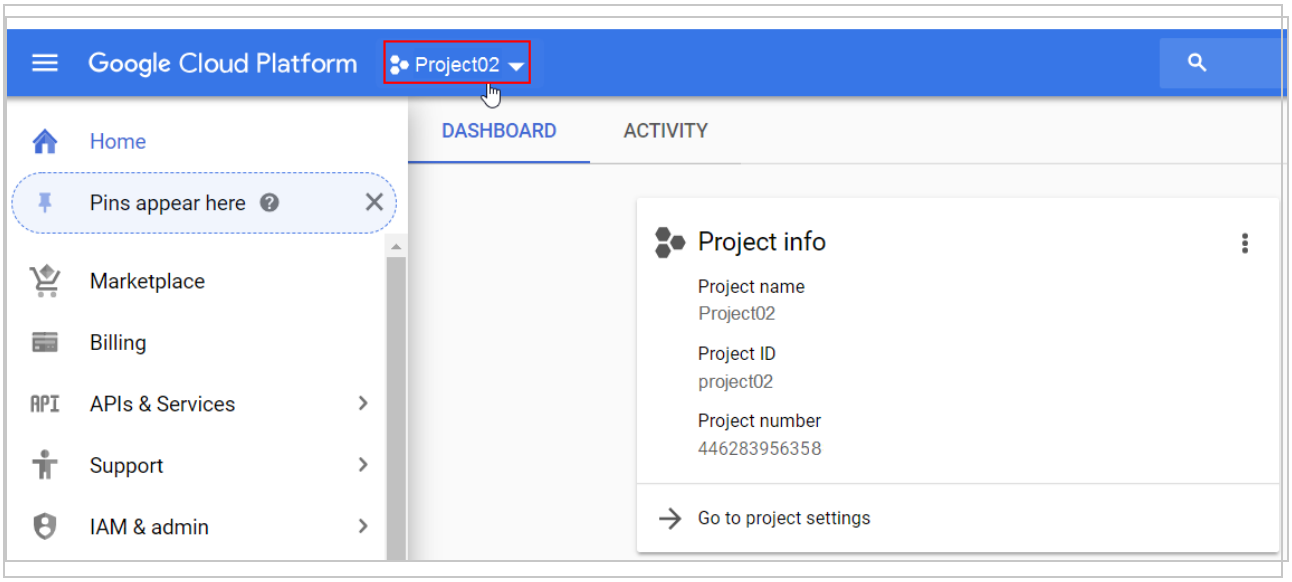
Follow this procedure to associate additional projects with 1 service account:

1. Before you begin, make sure you have completed the procedures in "Prerequisite: Enable the Google APIs" on page 191 and "Create a GCP service account" on page 192.
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`.



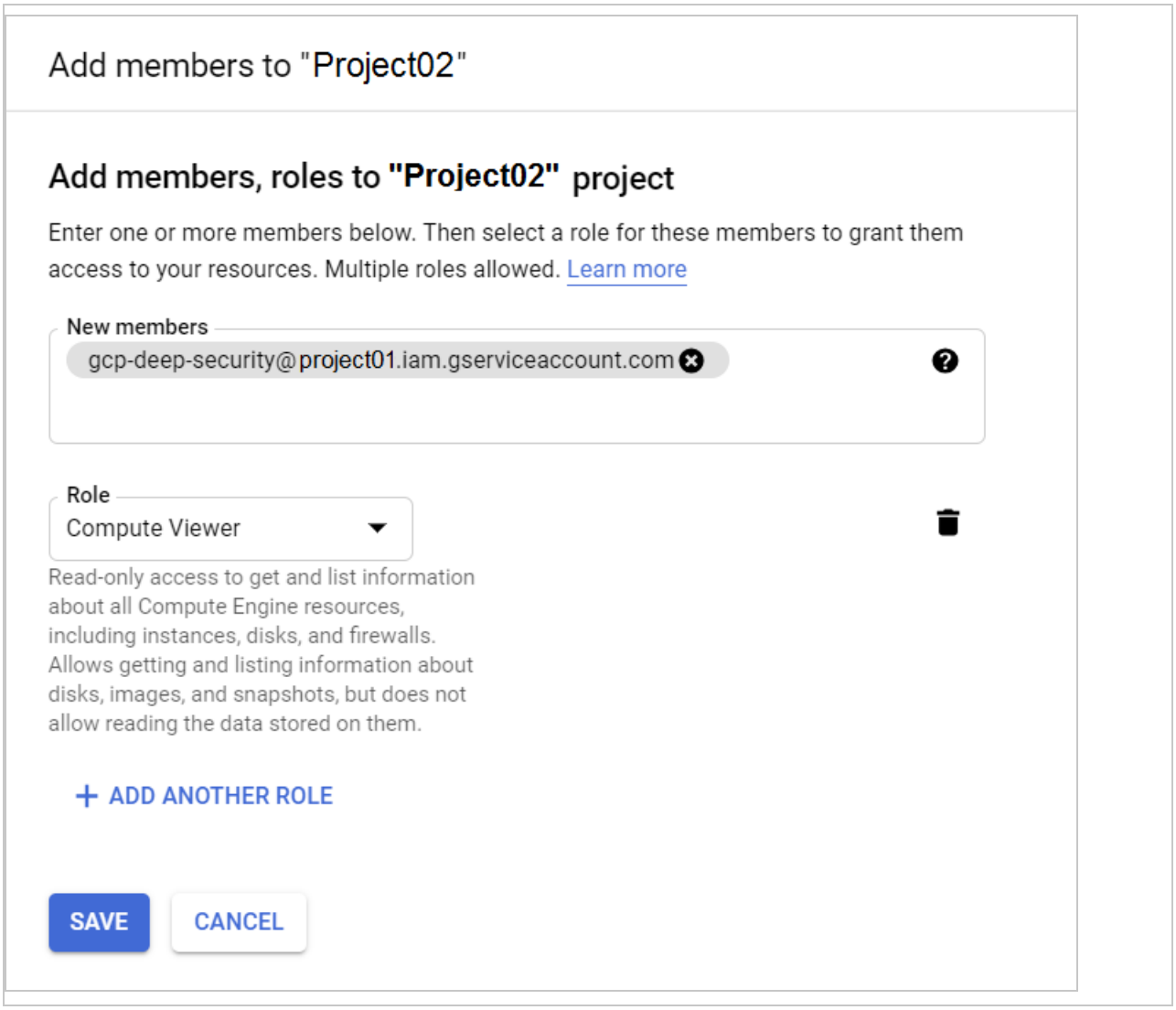
4. Click **Google Cloud Platform** at the top to make sure you're on the Home screen.

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.



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 192 and "Add more projects to the GCP service account" on page 196

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?

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:

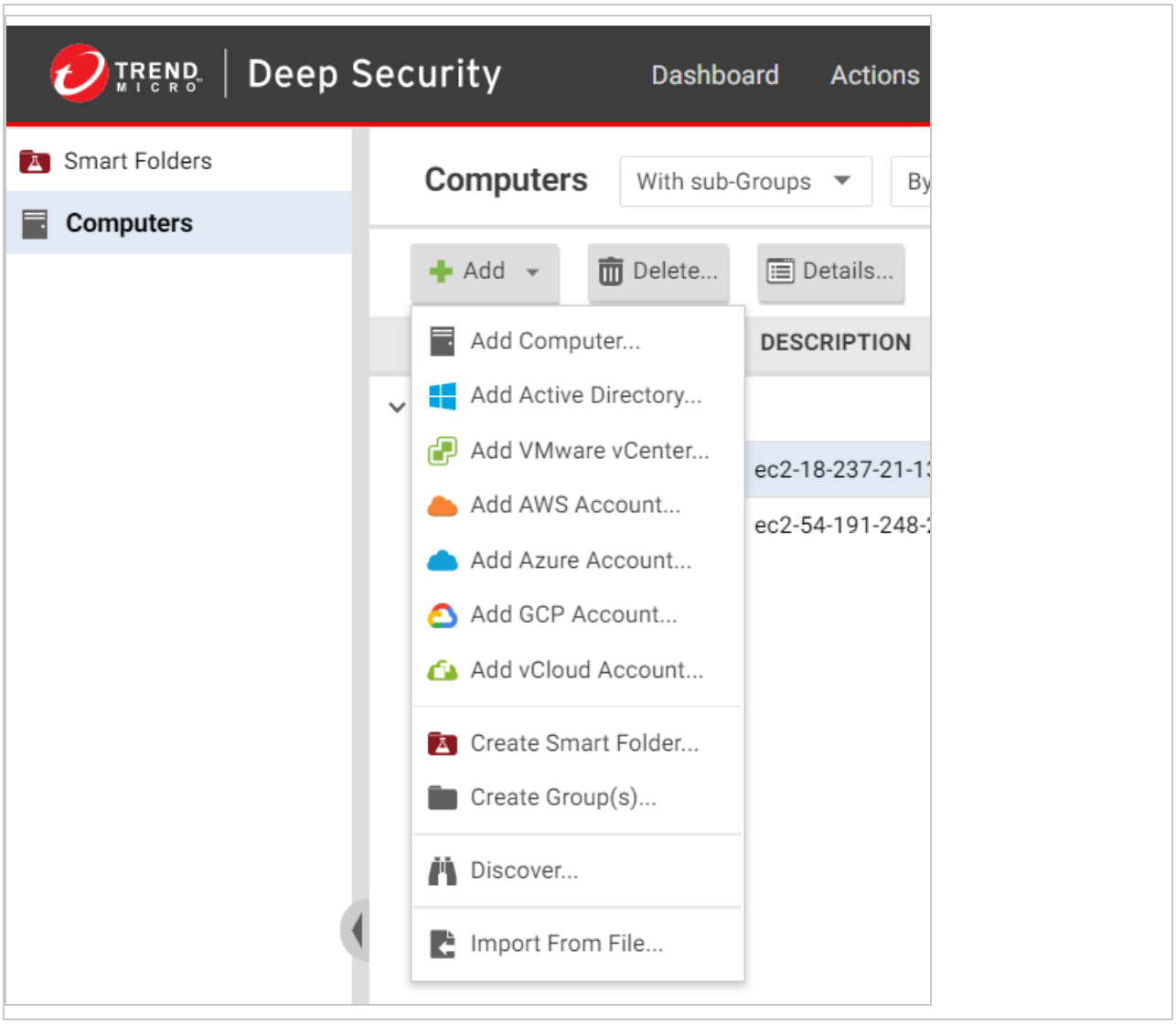
- Changes in your GCP VM inventory are automatically reflected in Deep Security Manager. For example, if you delete a number of VM instances in GCP, those instances disappear automatically from the manager. By contrast, if you use **Computers > Add Computer**, GCP instances that you've deleted remain 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**.
- Your smaller-sized GCP instances will be billed at a lower rate (if you are using metered billing). By contrast, if you use **Computers > Add Computer**, all your GCP instances regardless of size are billed at the highest 'Data Center' rate. For details on billing, see "About billing and pricing" on page 74.

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 191 for Deep Security.

2. In Deep Security Manager, go to **Computers > Add > Add GCP Account**.

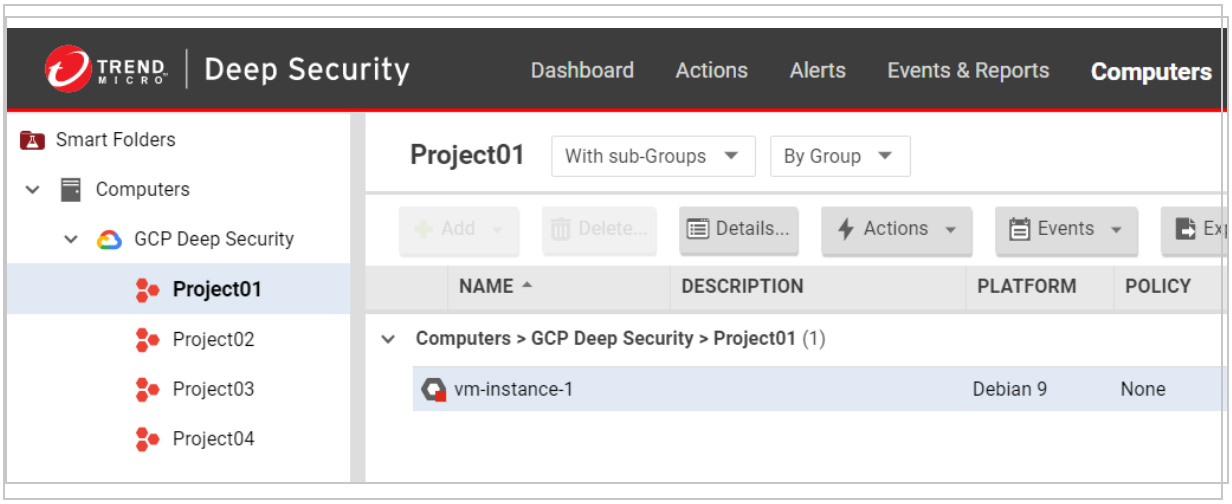


3. Enter a **Display Name**. We recommend using the GCP service account name. Examples: `GCP Deep Security`, `Finance GCP Deep Security`, `Marketing GCP Deep Security`.
4. Choose the **Service Account Key**. The key is a JSON file that you saved earlier, when creating the GCP service account. See "Create a Google Cloud Platform service account" on page 191 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.



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 162 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 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.

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 Azure 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.

Manually upgrade your AWS account connection

In older iterations of Deep Security as a Service, you could add an AWS account to Deep Security Manager by clicking **Add AWS Account** on the **Computers** page. This method used an AWS CloudFormation template to add your account. All of the AWS instances associated with your account would appear on the Computer page, listed under your AWS account name and regions.

Deep Security as a Service now includes the ability to display your AWS instances organized by region, VPC and subnet. The migration from the older type of AWS connection to the new method usually happens automatically. However, if Deep Security encounters a problem and cannot perform the migration automatically, it will produce an "AWS Account Migration Failed" alert. If you encounter this alert, follow the steps in this article to migrate your AWS account connection. The main cause of the migration failure is a lack of permissions for the AWS role listed in the alert message.

Verify the permissions associated with the AWS role

1. Log in to your Amazon Web Services Console and go to the **IAM** service.
2. In the left navigation pane, click **Roles**.
3. Find the role that was identified in the alert message and click the role.
4. Under Permissions, expand the "DeepSecurity" policy, and click **Edit Policy**.
5. The policy in the "Action" section should be:

```
"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"
]
```

Note: The `"sts:AssumeRole"` permission is required only if you are 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** and **Save changes**.
7. Wait for up to 30 minutes and your connection should be upgraded. On the **Computers** tab in Deep Security Manager, your AWS instances are organized by region, VPC and subnet. Your Amazon WorkSpaces are organized by region and WorkSpace directory.

How do I migrate to the new cloud connector functionality?

If you previously used the "Add Cloud Account" wizard 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 provide the ability 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, you will need to 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. In the left navigation pane, click **Policies**.
3. In the list of policies, select the policy that allows Deep Security to access your AWS account.
4. Go to the **Policy Document** tab and click **Edit**.
5. Edit the policy document to include this 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": [
				"*"
			]
		}
	]
}
```

> **Note:** The `"sts:AssumeRole"` permission is required only if you are using cross-account role access. For more information on IAM roles, see Tutorial: Delegate Access Across AWS Accounts Using IAM Roles.

6. Select **Save as default version**.

To migrate your AWS resources in the Deep Security Manager:

1. In the Deep Security Manager, go to the **Computers** page.
2. In the Computers tree, right-click an AWS region and select **Upgrade to Amazon Account**.
3. Click **Finish** and then **Close**. Your AWS instances will now 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 support" on page 84 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 protect them against known and zero-day exploits by virtually patching new found vulnerabilities
- Provide real-time anti-malware detection for the file systems used on Docker hosts and 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

Note: Deep Security Docker protection works at the OS level. This means that the 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 the Docker host

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

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.

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:

[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 216.
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 238 and "Overview section of the computer editor" on page 232 are different)
- Anti-Malware
- Web Reputation
- 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**.

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 221 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. 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**.

---

[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).

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)**.

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.

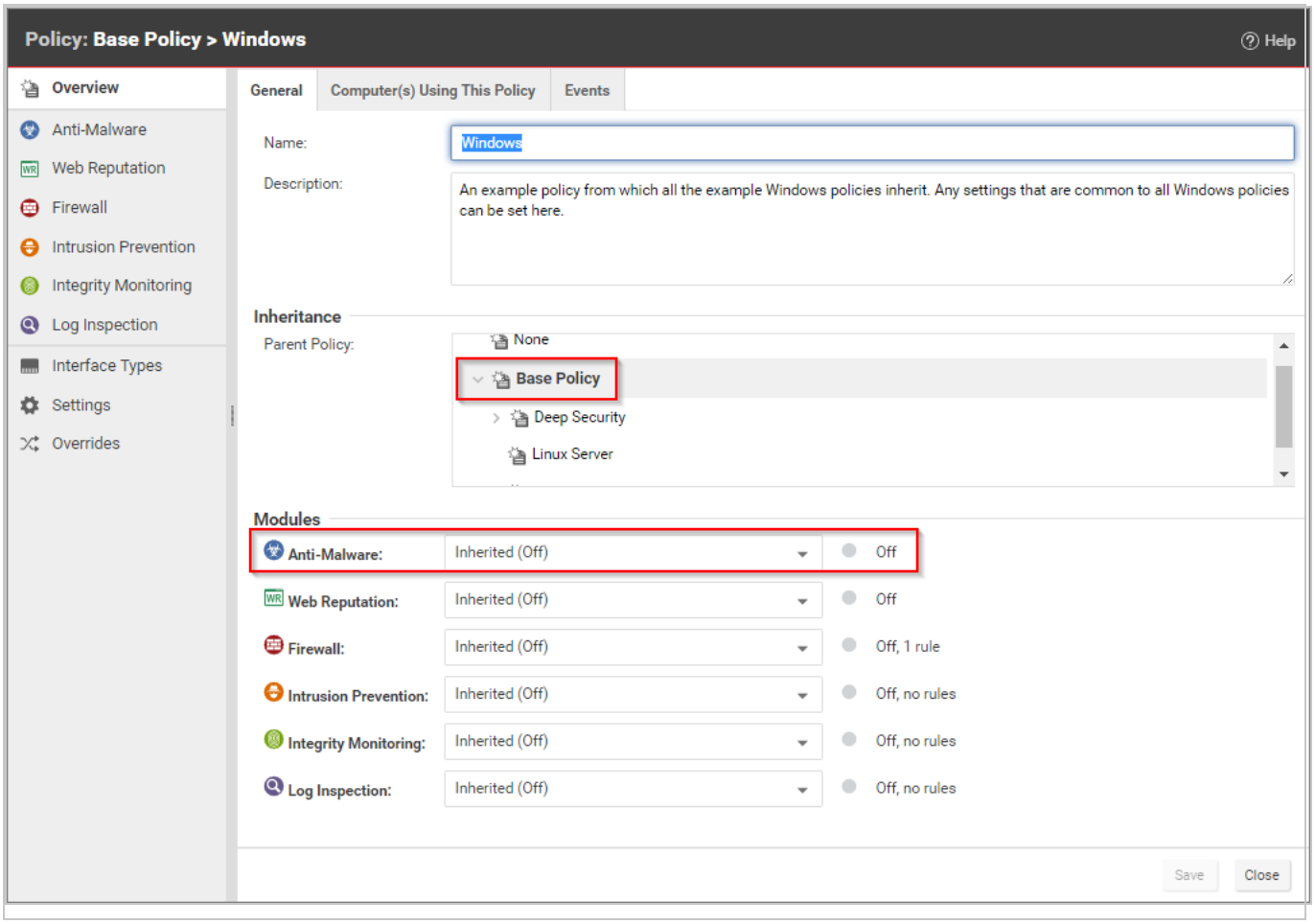
Deep Security provides a collection of policies that you can use as initial templates for the design of your own policies tailored to your environment:

In this topic:

Inheritance

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)**:

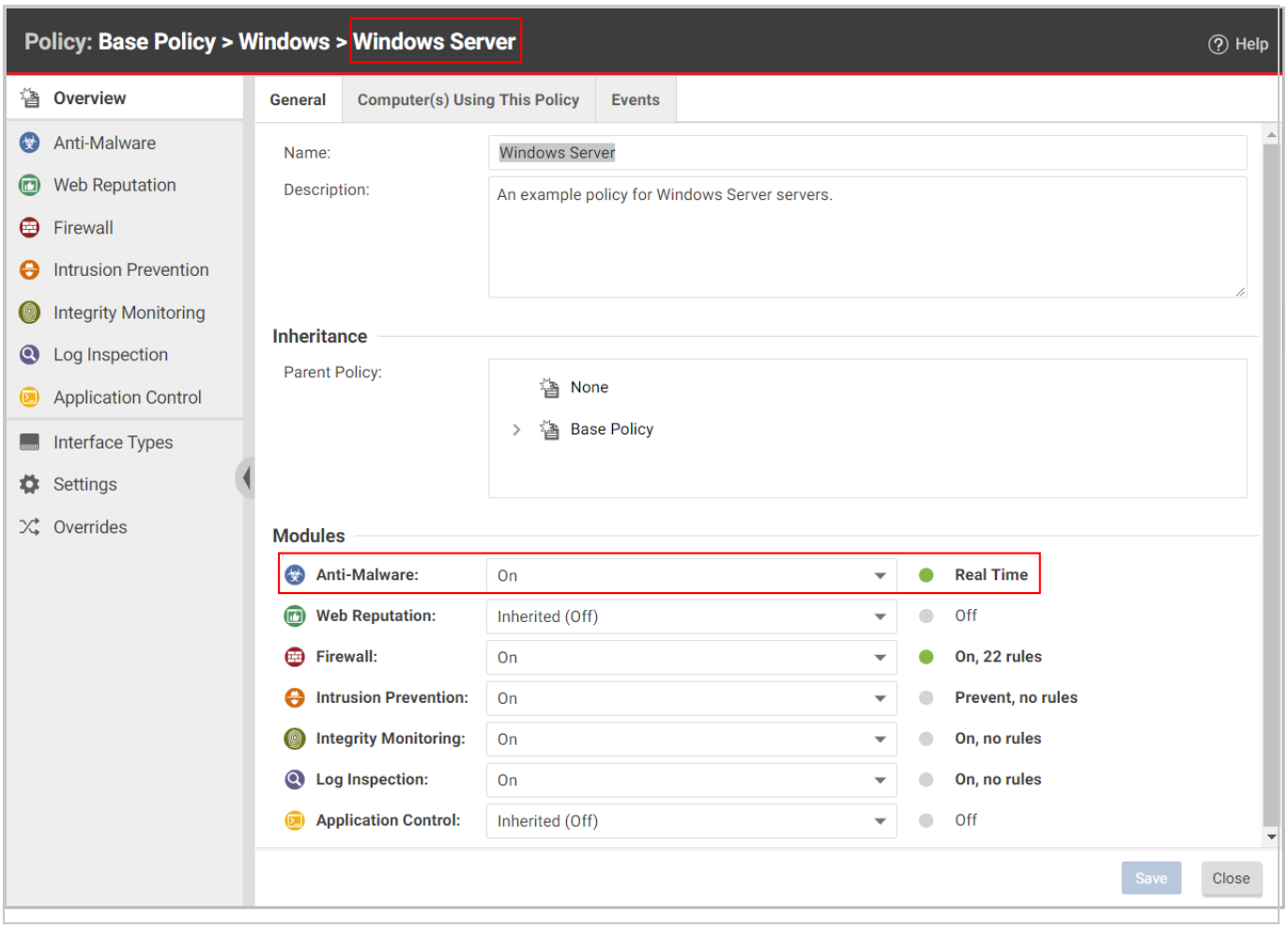


This means that the setting is inherited from the parent **Base** policy, and that if you were to change the anti-malware setting in the **Base** policy from **Off** to **On**, the setting would change in the **Windows** policy as well. (The **Windows** policy setting would then read **Inherited (On)**. 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**.



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.

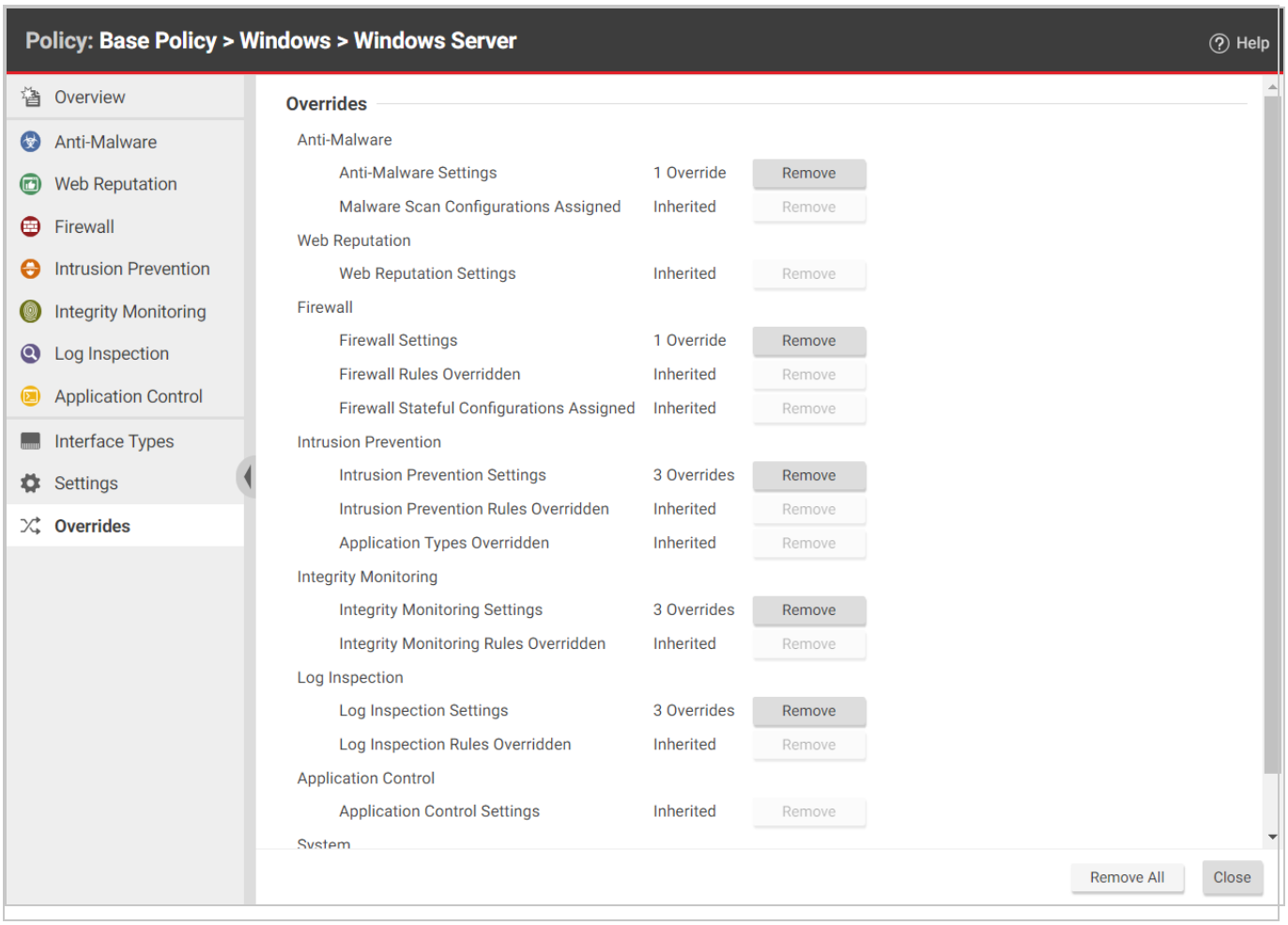
Override rule assignments

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 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 229

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?

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.

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 page 226.
- **Command line:** Initiate a recommendation scan via the Deep Security command-line interface. See "Command-line basics" on page 973.
- **API:** Initiate a recommendation scan via the Deep Security API. See "Use the Deep Security API to automate tasks" on page 990.

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.

[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. 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 216 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. 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.

---

[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).

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**[1].

   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.
- 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.)

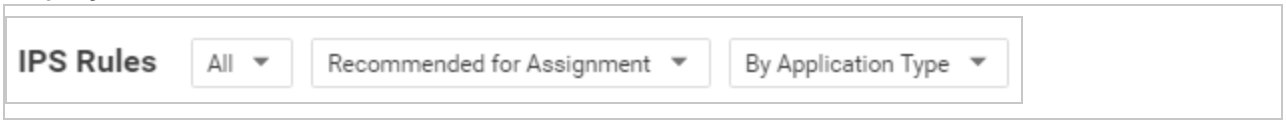
[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

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.)

   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.

---

[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: 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

Rule name	Application type
1003222 - Block Administrative Share	DCERPC Services
1001126 - DNS Domain Blocker	DNS Client
1000608 - Generic SQL Injection Prevention See "Configure an SQL injection prevention rule" on page 386 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
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

Rule name	Application type
	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.

To resolve this issue, ensure that you're using agent-initatied communication. For more information, see "Activate and protect agents using agent-initiated activation and communication" on page 852.

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.

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

- **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).
- **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.
- **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 and logs" on page 1075.

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.

---

[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).

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.

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 717.

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

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.
- **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 717.

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** .

Note: The **Advanced** tab also contains **Events** settings. For information on those settings, see Limit log file sizes. 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.

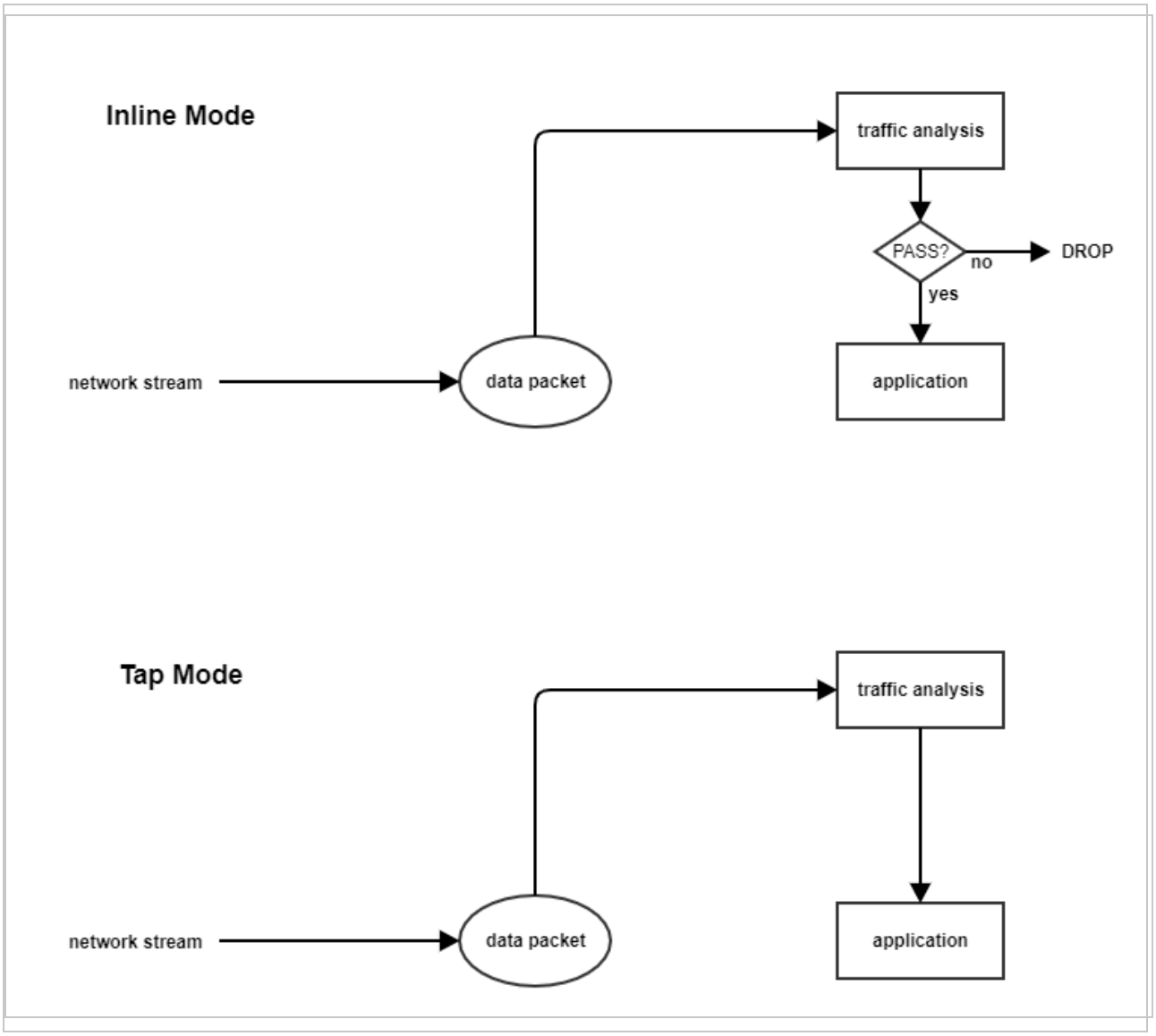
The following settings are available:

---

[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).

- **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.



- **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 403.

- **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.

  > **Note:** 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.
- **Number of Event Nodes:** The maximum amount of kernel memory the driver will use to store log/event information for folding at any one time.

  Note: Event folding occurs when many events of the same type occur in succession. In such cases, the agent/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 (above) 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" (below) if the engine is in tap mode, and will switch to "Normal" (above) 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.

Note: 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 580.

- **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.

  Note: 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/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
- **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

Rule type	Priority	Direction	Protocol	Source port	Destination port
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.

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 216.

Tip: You can automate common object creation and configuration using the Deep Security API. For examples, see the Create and Configure Common Objects for Policies and Computers guide in the Deep Security Automation Center.

Rules

Some protection modules make use of rules:

- "Create a firewall rule" on page 422
- Configure an intrusion prevention rule for use in policies
- "Create an Integrity Monitoring rule" on page 456
- "Define a Log Inspection rule for use in policies" on page 511

Lists

- "Create a list of directories for use in policies" on page 296
- "Create a list of file extensions for use in policies" on page 298
- "Create a list of files for use in policies" on page 299
- "Create a list of IP addresses for use in policies" on page 302

- "Create a list of MAC addresses for use in policies" on page 304
- "Create a list of ports for use in policies" on page 303

Other

- "Define contexts for use in policies" on page 305
- "Define stateful firewall configurations" on page 441
- "Configure malware scans" on page 322
- "Define a schedule that you can apply to rules" on page 311

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 409.

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 254.

When you're done with your firewall rule, you can also learn how to:

- "Configure rule events and alerts" on page 255
- "Set a schedule for the rule" on page 256
- "See policies and computers a rule is assigned to" on page 256
- "Assign a context to the rule " on page 256

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 428.

     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 429.

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	✔	✔		

	IP	MAC	Port	Flags
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 311.

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 305.

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:

For an overview of the intrusion prevention module, see "About Intrusion Prevention" on page 366.

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

[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.

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 216.)

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**.

[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).

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 265.

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 265.

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 265.

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. Agentless protection is not available with Deep Security as a Service.

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 265.

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 265.

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 368.

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**.

[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).

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.

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 449.

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 268 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 269
- "See policies and computers a rule is assigned to" on page 270
- "Export a rule" on page 270
- "Delete a rule" on page 270

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 492 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 476 documentation.

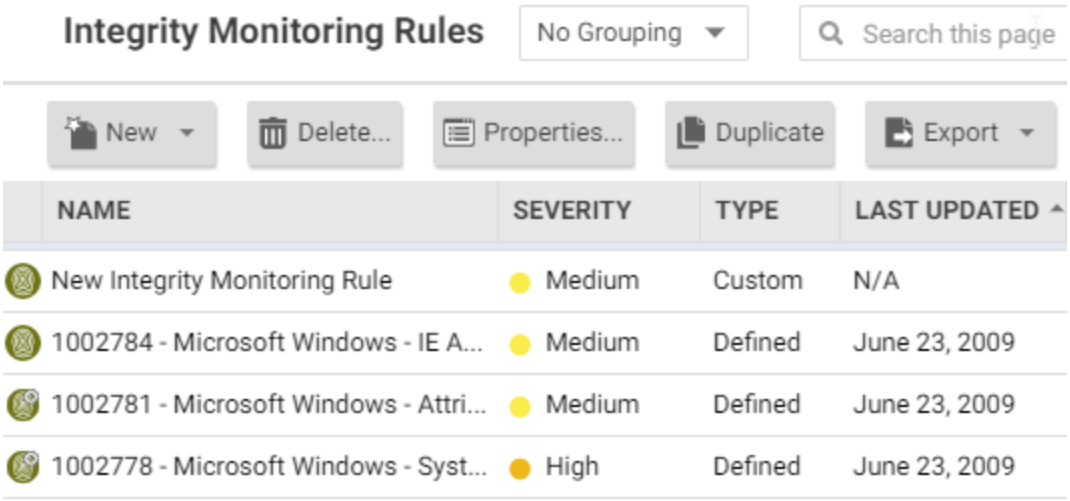
Custom (XML) template

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 460.

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 ().



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.

Log Inspection Rules issued by Trend Micro are not editable (although you can duplicate them and then edit them.)

Note: Log Inspection Rules that are assigned to one or more computers or that 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 273
- "Subrules" on page 274

- "Real world examples" on page 282
- "Log Inspection rule severity levels and their recommended use" on page 290
- "strftime() conversion specifiers " on page 291
- "Examine a Log Inspection rule" on page 292

For an overview of the Log Inspection module, see "About Log Inspection" on page 506.

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.

   Note: Any changes you make in the Custom (XML) view will be 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 will pre-populate 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 will be

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 will cause 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.

Note: 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 any).

1. On the **Files** tab, type the full path to the file(s) you want your rule to monitor and specify the type of file it is.
2. 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.

   Note: 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.
3. 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.

4. 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 we have indicated that our group contains the syslog and sshd rules:

```
<group name="syslog,sshd,">
</group>
```

Note: 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 sub-rule to this one.

Note: 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 essentially a single long Log Inspection rule. Some group definitions are common to all Log Inspection rules written 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 along with any other Trend Micro rules. (If you select a rule for assignment and haven't also selected the "Default Rules Configuration" rule, a notice will appear 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, we have created two rules, 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>
```

Note: 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 web_scan recon	Connection attempt Web scan Generic scan
Authentication Control	authentication_success authentication_failed invalid_login login_denied authentication_failures adduser account_changed	Success Failure Invalid Login Denied Multiple Failures User account added User Account changed or removed
Attack/Misuse	automatic_attack exploit_attempt invalid_access spam multiple_spam sql_injection attack virus	Worm (nontargeted attack) Exploit pattern Invalid access Spam Multiple spam messages SQL injection Generic attack Virus detected
Access Control	access_denied access_allowed unknown_resource firewall_drop multiple_drops client_misconfig client_error	Access denied Access allowed Access to nonexistent resource Firewall drop Multiple firewall drops Client misconfiguration Client error

Group Type	Group Name	Description
Network Control	new_host ip_spoof	New computer detected Possible ARP spoofing
System Monitor	service_start system_error system_shutdown logs_cleared invalid_request promisc policy_changed config_changed low_diskspace time_changed	Service start System error Shutdown Logs cleared Invalid request Interface switched to promiscuous mode Policy changed Configuration changed Low disk space Time changed

Note: If event auto-tagging is enabled, the event will be 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. So, for example, "login_denied" would appear as "Login Denied". Custom rules will be listed by their group name as it appears in the rule.

Description

Include a **<description></description>** tag. The description text will appear 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>
```

Note: 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>
```

Note: 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 will have broken up the log into sections. See "Decoders" on page 273 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)

Regex Syntax	Description
$	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.

Note: 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 will ignore the children of that parent.

Note: 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 on.

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 hh:mm - hh:mm or 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, etc.)	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 will be 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 no_email_alert 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>
```

Real world 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.

In this section we will walk through the creation of 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 our custom 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 functional features which we will create Log Inspection rules for:

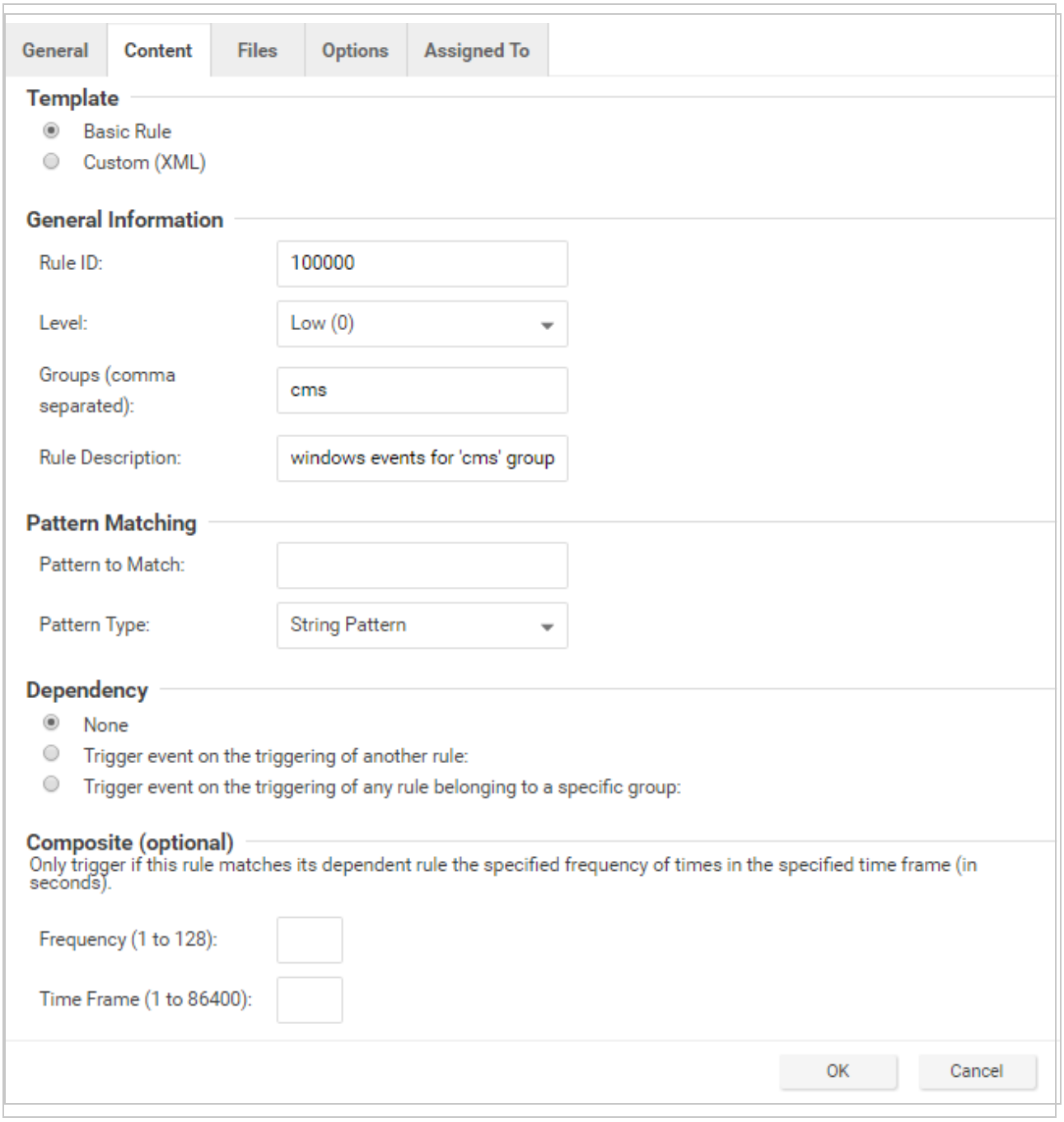
- CMS Application Log (Source: CMS)
  - Authentication (Event: 100 to 119)
    - User Login successful (Event: 100)
    - User Login unsuccessful (Event: 101)
    - Administrator Login successful (Event: 105)
    - Administrator Login unsuccessful (Event: 106)
  - General Errors (Type: Error)
    - Database 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 will provide you with a good basis for rule creation. Now to create a new Log Inspection rule in Deep Security Manager.

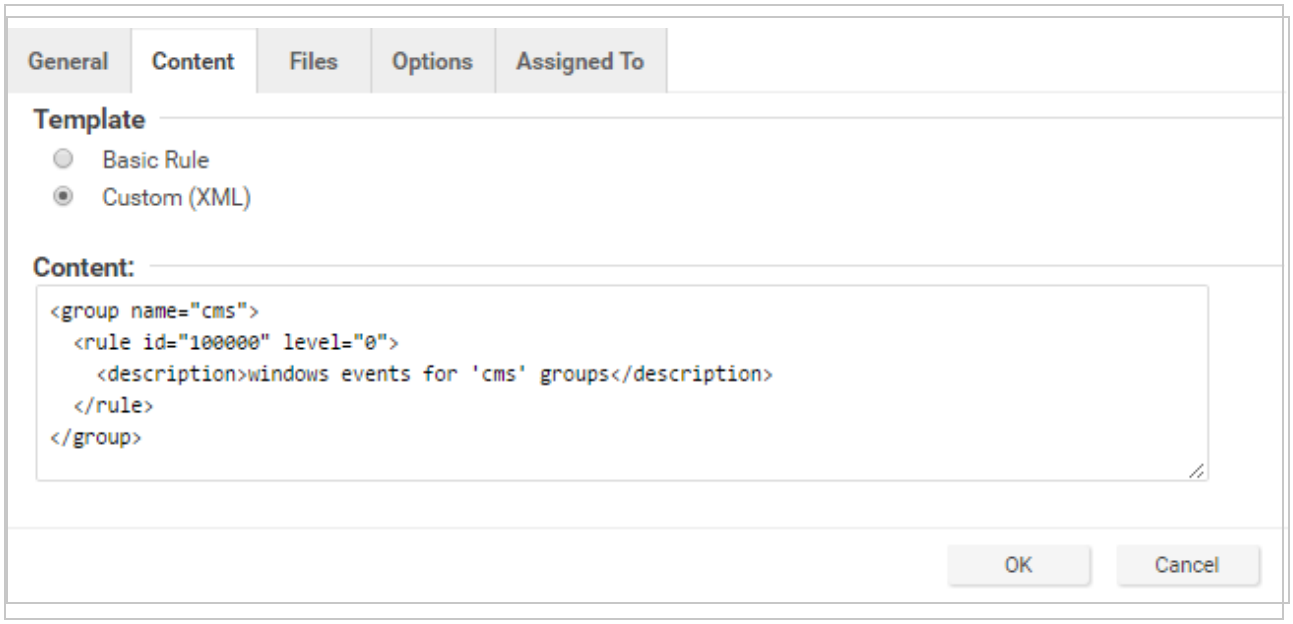
To create the new CMS Log Inspection Rule:

1. In the 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 click the **Content** tab.
3. The quickest way to create a new custom rule is to start with a basic rule template. Select the **Basic Rule** radio button.
4. The **Rule ID** field will be 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".

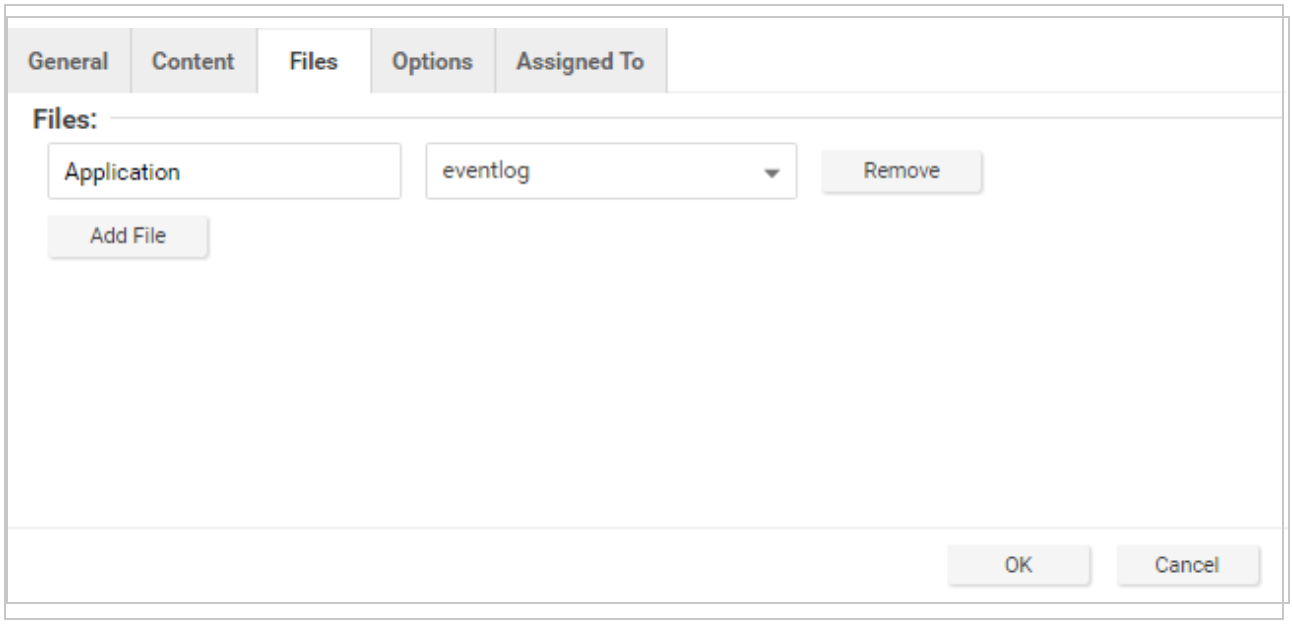
7. Provide a short rule description.



8. Now select the **Custom (XML)** option. The options you selected for your "Basic" rule will be converted to XML.



9. Click the **Files** tab and click the **Add File** button to add any application log files and log types which the rule will be applied to. In this case, "Application", and "eventlog" as the file type.



Note: **Eventlog** is a unique file type in Deep Security because the location and filename of the log files don't 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 will require the log file's location and filename. (*C/C++ strftime()* conversion specifiers are available for matching on filenames. See the table below 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, we can begin adding new rules to the group based on the log groupings identified previously. We will 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. Now we build up 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. Now we add any composite or correlation rules using the established rules. The follow example shows a high severity composite rule that is applied to instances where the repeated login failures have occurred 5 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. Finally, open the newly created rule, click 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, etc.
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, etc. 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	Include attempts to login as an unknown user or from an invalid source. The message might have security relevance especially if repeated. They also

Level	Description	Notes
	source	include errors regarding the **admin** or **root** account.
Level 10	Multiple user generated errors	Include multiple bad passwords, multiple failed logins, etc. 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-importance event	Include error or warning messages from the system, kernel, etc. 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 (e.g., Thu)
%A	Full weekday name (e.g., Thursday)
%b	Abbreviated month name (e.g., Aug)
%B	Full month name (e.g., August)
%c	Date and time representation (e.g., Thu Sep 22 12:23:45 2007)
%d	Day of the month (01 - 31) (e.g., 20)
%H	Hour in 24 h format (00 - 23) (e.g., 13)
%I	Hour in 12 h format (01 - 12) (e.g., 02)
%j	Day of the year (001 - 366) (e.g., 235)
%m	Month as a decimal number (01 - 12) (e.g., 02)
%M	Minute (00 - 59) (e.g., 12)
%p	AM or PM designation (e.g., AM)
%S	Second (00 - 61) (e.g., 55)
%U	Week number with the first Sunday as the first day of week one (00 - 53) (e.g., 52)
%w	Weekday as a decimal number with Sunday as 0 (0 - 6) (e.g., 2)
%W	Week number with the first Monday as the first day of week one (00 - 53) (e.g., 21)
%x	Date representation (e.g., 02/24/79)
%X	Time representation (e.g., 04:12:51)
%y	Year, last two digits (00 - 99) (e.g., 76)
%Y	Year (e.g., 2008)
%Z	Time zone name or abbreviation (e.g., EST)

Specifier	Description
%%	A % sign (e.g., %)

More information can be found at the following websites:

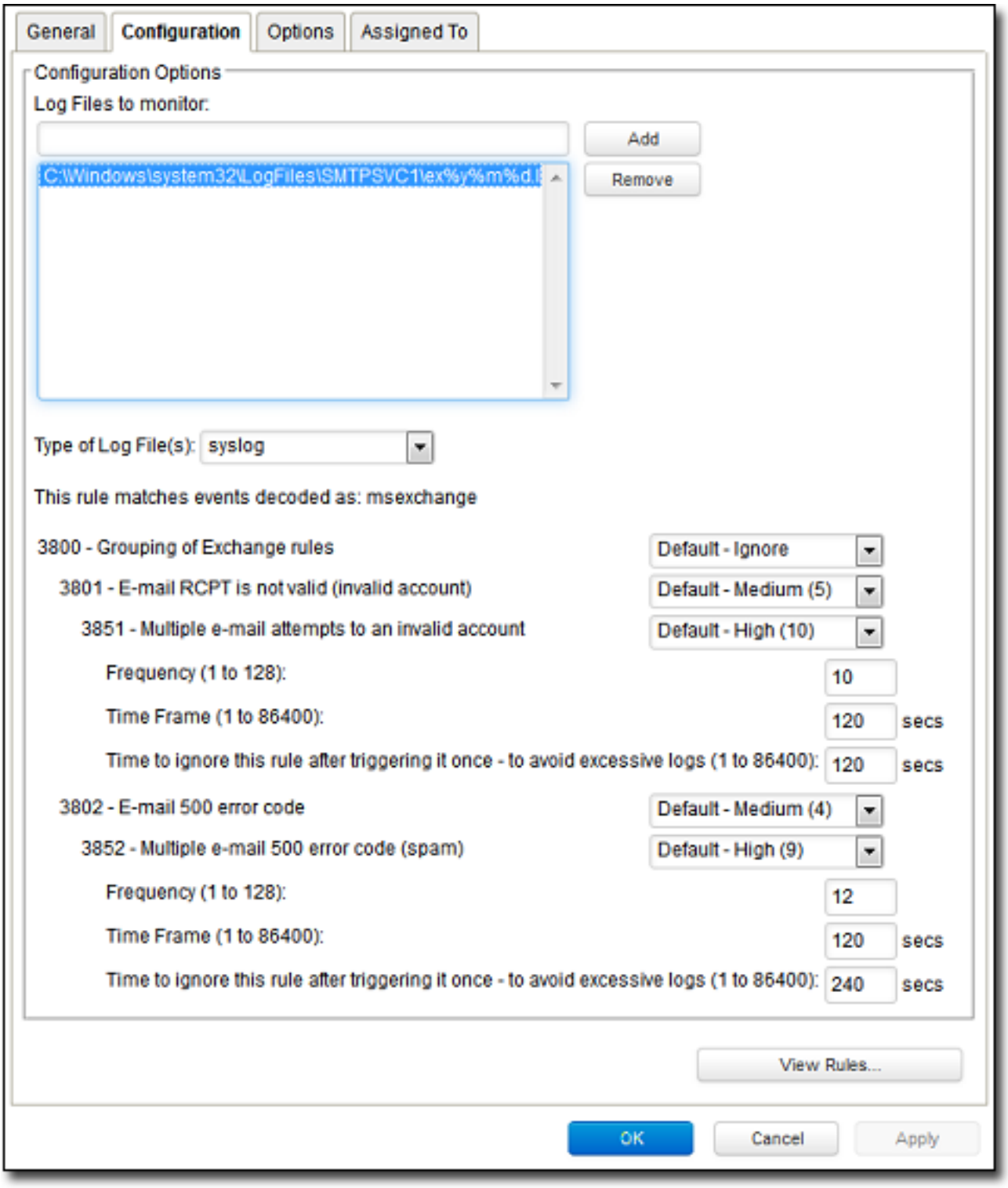
https://www.php.net/manual/en/function.strftime.php
www.cplusplus.com/reference/clibrary/ctime/

Examine a Log Inspection rule

Log Inspection rules are found in the Deep Security Manager at **Policies > Common Objects > Rules > Log Inspection Rules**.

Log Inspection rule structure and the event matching process

This screen shot displays the contents of the **Configuration** tab of the Properties window of the "Microsoft Exchange" Log Inspection rule:



Here is the structure of the rule:

- 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 will apply log events to this structure and see 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 will then be applied to line 3800's sub-rules: 3801 and 3802.

If there is no further match, this "cascade" of matches will stop 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. Sub-rule 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 sub-rule to be applied to the event: sub-rule 3851. Sub-rule 3851 with its three attributes will match 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 sub-rule 3851 to ignore individual events that match sub-rule 3801 for the next 120 seconds. This is useful for reducing "noise".)

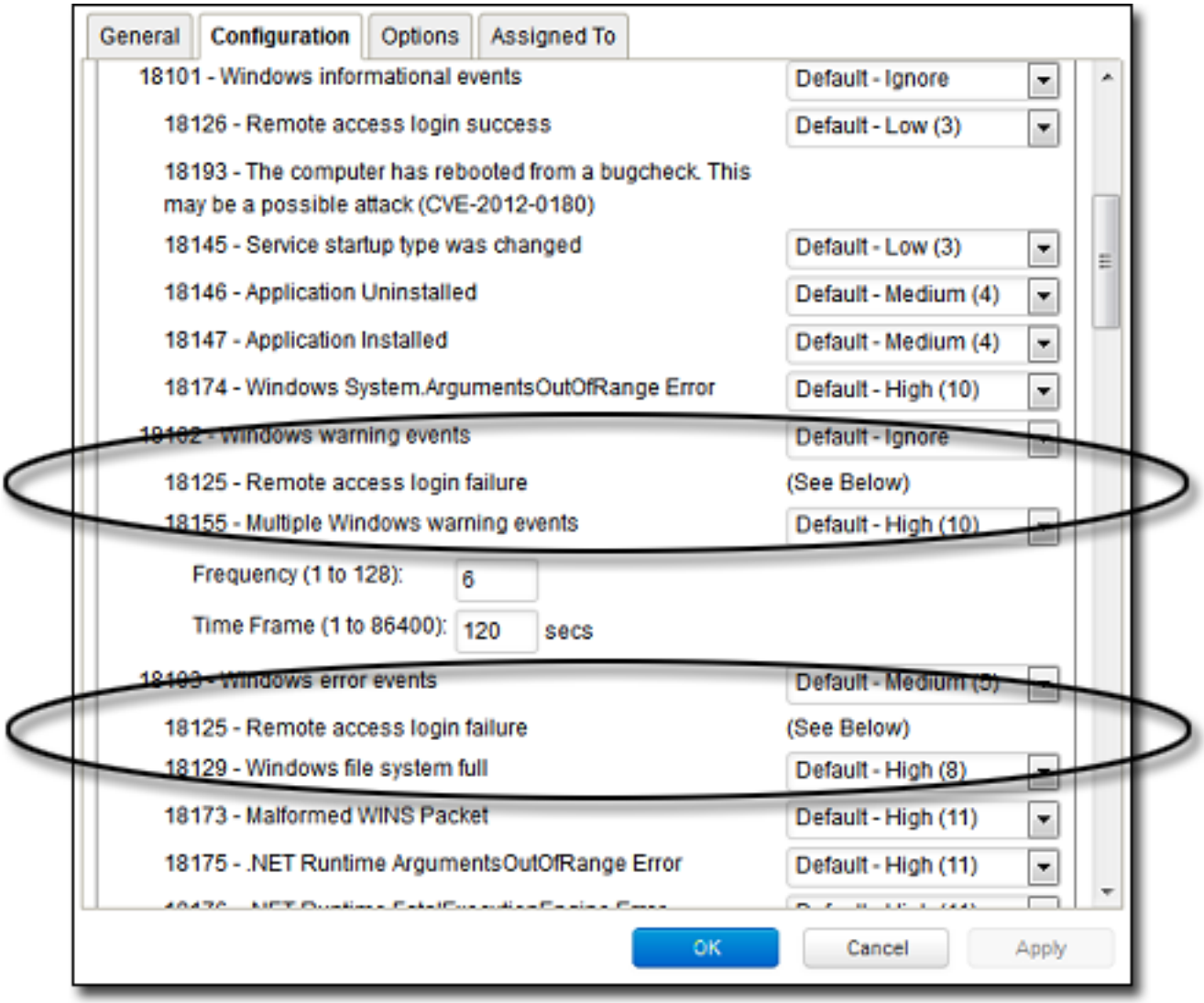
Assuming the parameters of sub-rule 3851 have been matched, a Log Inspection event with Severity "High(9)" is now recorded.

Looking at the Options tab of the Microsoft Exchange Rule, we see that Deep Security Manager will raise an alert if any sub-rules with a severity level of "Medium(4)" have been matched. Since this is the case in our example, the alert will be raised (if "Alert when this rule logs an event" is selected).

Duplicate Sub-rules

Some Log Inspection rules have duplicate sub-rules. To see an example, open the "Microsoft Windows Events" rule and click on the **Configuration** tab. Note that sub-rule 18125 (Remote access login failure) appears under sub-rules 18102 and 18103. Also note that in both cases sub-rule 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:



Create a list of directories for use in policies

Create lists of directory paths 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. 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 326.

Tip: 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 "\" are 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* 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* *\\some-comp-name* Includes all files on a network resource (and its subfolders) identified using an IP or a hostname. *\\12.34.56.78\somefolder* *\\some-comp-name\somefolder* 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** Includes all files in all subdirectories of "abc" but does not include the files in the "abc" directory. *C:\abc\wx*z* *Matches:* C:\abc\wxz\ C:\abc\wx123z\ *Does not match:* C:\abc\wxz C:\abc\wx123z

Directory	Format	Description	Examples
			C:\abc*wx *Matches:* C:\abc\wx\ C:\abc\123wx\ *Does not match:* C:\abc\wx 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**** *Matches:* C:\abc\ C:\abc\1 C:\abc\123 *Does not match:* C:\abc C:\abc\123\ C:\abc\123\456 C:\abx\ C:\xyz\ ***C:\abc*wx*** *Matches:* C:\abc\wx C:\abc\123wx *Does not match:* C:\abc\wx\ C:\abc\123wx\ ***C:\abc\wx*z*** *Matches:* C:\abc\wxz C:\abc\wx123z *Does not match:* C:\abc\wxz\ C:\abc\wx123z\ ***C:\abc\wx**** *Matches:* C:\abc\wx C:\abc\wx\ C:\abc\wx12 C:\abc\wx12\345\ C:\abc\wxz\ *Does not match:* C:\abc\wx123z\
Environment variable	${ENV VAR}	Includes all files and subdirectories defined by an environment variable with the format ${ENV VAR}. For a Virtual Appliance, the value pairs for	***${windir}*** If the variable resolves to "c:\windows", Includes all the files in "c:\windows"

Directory	Format	Description	Examples
		the environment variable must be defined in **Policy or Computer Editor > Settings > General > Environment Variable Overrides.**	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.

See which policies use a 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 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. 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 326.

Tip: 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 "\" are 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*** Includes all files named "abc.doc" in all directories. Does not include "abc.exe".
File path	FILEPATH	Includes the specific file specified by the file path.	***C:\Documents\abc.doc*** Includes only the file named "abc.doc" in the "Documents" directory.
File with wildcard (*)	FILE*	Includes all files with a matching pattern in the file name.	***abc*.exe*** Includes any file that has prefix of "abc" and extension of ".exe". ***.db*** *Matches:* 123.db abc.db *Does not match:* 123db 123.abd cbc.dba ***db*** *Matches:* 123.db 123db ac.db acdb db *Does not match:* db123 ***wxy*.db*** *Matches:* wxy.db wxy123.db *Does not match:* wxydb
File with wildcard (*)	FILE.EXT*	Includes all files with a matching pattern in the file extension.	***abc.v**** Includes any file that has file name of "abc" and extension

Inclusion	Format	Description	Example
			beginning with ".v". ***abc.*pp*** *Matches:* abc.pp abc.app *Does not match:* wxy.app ***abc.a*p*** *Matches:* abc.ap abc.a123p *Does not match:* abc.pp ***abc.**** *Matches:* abc.123 abc.xyz *Does not match:* 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*** *Matches:* ac.ap a123c.ap ac.a456p a123c.a456p *Does not match:* ad.aa
Environment variable	${ENV VAR}	Includes files specified by an environment variable with the format ${ENV VAR}. These can be defined or overridden using **Policy or Computer Editor > Settings > General > Environment Variable Overrides.**	***${myDBFile}*** 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::CD30:0:0:0:0/60. 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 106.

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 231.

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" below.

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 311
- "Export a stateful configuration " on page 311
- "Delete a stateful configuration " on page 311

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: Schedules use the same time zone as the protected computer's operating system.

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 319.

- "Types of malware scans" on the next page
- "Malware scan configurations" on page 314
- "Malware events" on page 315
- "SmartScan" on page 315

- "Predictive Machine Learning" on page 316
- "Types of malware scans" below

Types of malware scans

The anti-malware module performs several types of scans. See also "Select the types of scans to perform" on page 320.

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 991).

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" on page 322.

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 765
- "View and restore identified malware" on page 350
- "Create anti-malware exceptions" on page 357

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 347.

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 339.

Malware types

The anti-malware module protects against many file-based threats. See also "Scan for specific types of malware" on page 324 and "Configure how to handle malware" on page 332

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 anonymously sent back to Trend Micro for analysis.

Set up Anti-Malware

Enable and configure anti-malware

To use anti-malware, perform these basic steps:

1. "Turn on the anti-malware module" on the next page.
2. "Select the types of scans to perform" on the next page.
3. "Configure scan exclusions" on the next page
4. "Ensure that Deep Security can keep up to date on the latest threats" on page 321.

When you have completed these steps, review "Configure malware scans" on page 322 and refine the anti-malware scan behavior.

Tip: For most anti-malware settings, you can either configure them for each individual computer or in a policy that applies to multiple computers (for example, to all Windows 2008 Servers). To make management easier, configure the settings in the policy (not individual computers) wherever possible. For more information, see "Policies, inheritance, and overrides" on page 216.

Tip: CPU usage and RAM usage varies by your anti-malware configuration. To optimize anti-malware performance on Deep Security Agent, see "Performance tips for anti-malware" on page 336.

For an overview of the anti-malware feature, see "About Anti-Malware" on page 312.

Turn on 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 perform

When anti-malware is turned on, Deep Security needs to know what type of scans it should perform (see "Types of malware scans" on page 313).

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**.

Tip: 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 991.)

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.

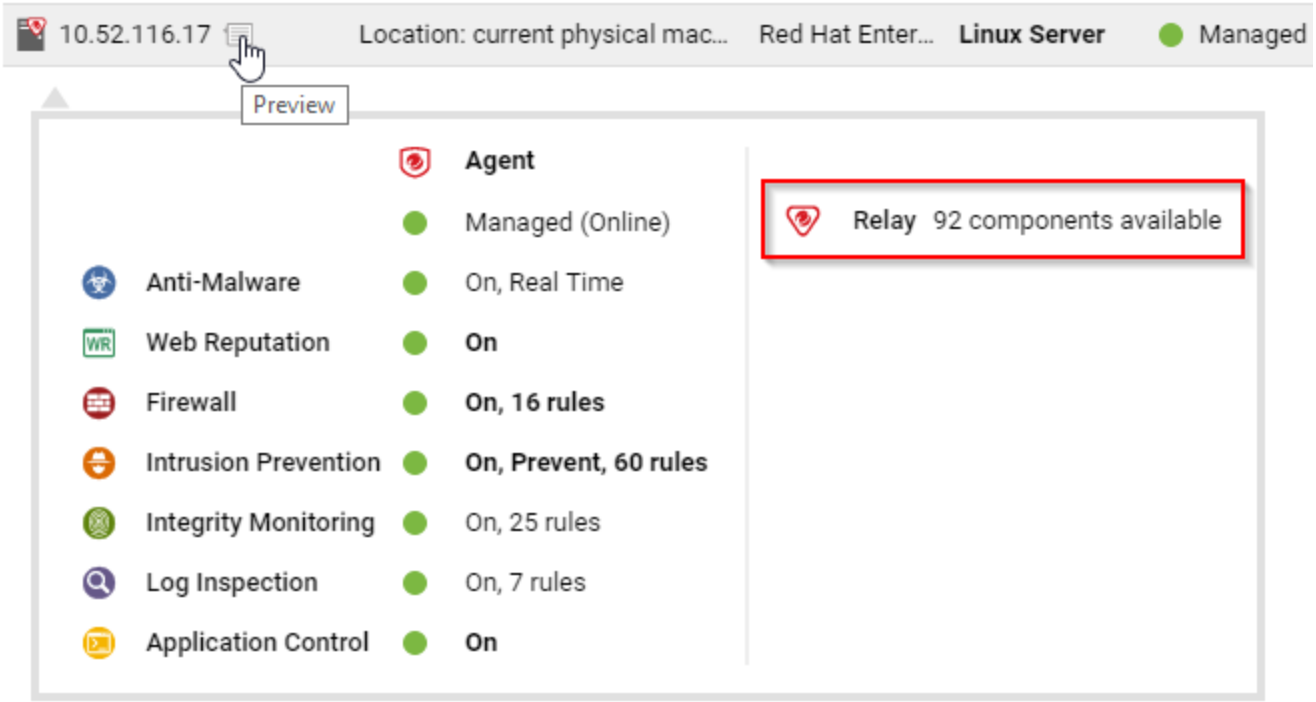
All of these exclusions are specified by selecting exclusion lists on the **Exclusions** tab of the Malware Scan Configuration editor. See "Specify the files to scan" on page 326.

Tip: 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.

Ensure that Deep Security can keep up to date on 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**.



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

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.

- "Create or edit a malware scan configuration" below
- "Scan for specific types of malware" on page 324
- "Specify the files to scan" on page 326
- "Specify when real-time scans occur" on page 332
- "Configure how to handle malware" on page 332
- "Identify malware files by file hash digest" on page 335
- "Configure notifications on the computer" on page 336

The Deep Security Best Practice Guide also provides several recommendations for configuration malware scans.

Tip: CPU usage and RAM usage varies by your anti-malware configuration. To optimize anti-malware performance on the Deep Security Agent, see "Performance tips for anti-malware" on page 336.

Create or edit a malware scan configuration

Create or edit a malware scan configuration to control the behavior of a real-time, manual, or scheduled scan. (For more information, see "Malware scan configurations" on page 314.) You can create multiple malware scan configurations as required.

- After you create a malware scan configuration, you can then associate it with a scan in a policy or computer (see "Select the types of scans to perform" on page 320)
- 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.

Tip: 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 313):

- **Real-time scan configuration:** Controls real-time scans. Some actions such as **Deny Access** are only available to real-time scan configurations
- **Manual/scheduled scan configuration:** Controls either manual or scheduled scans. Some options such as **CPU Usage** are only available to manual/scheduled scan configurations

Deep Security provides a default malware scan configuration for each type of scan.

1. Go to **Policies > Common Objects > Other > Malware Scan Configurations**.
2. To create a scan configuration, click **New** and then click **New Real-Time Scan Configuration** or **New Manual/Scheduled Scan Configuration**.
   a. Type a name to identify the scan configuration. You see the name in a list when configuring malware scans in a policy.
   b. (Optional) 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**.

Tip: To see the policies and computers that are using a malware scan configuration, see the AssignedTo tab of the properties.

Test malware scans

Before continuing with further Anti-Malware configuration steps, test real-time and manual/scheduled scans to ensure they're working correctly.

Test real-time scans:

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 will test 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.

Test manual/scheduled scans:

Note: Before you begin, make sure the real-time scan is disabled before testing manual/scheduled scans.

1. Go to **Administration**.
2. Click **Scheduled tasks > New**.
3. Select **Scan Computers for Malware** from the drop-down menu and select a frequency. Complete the scan configuration with your desired specifications.
4. Go to the EICAR site and download their anti-malware test file. This standardized file will test the manual/scheduled scan's anti-virus capabilities.
5. Select the scheduled scan and click **Run Task Now**. The test file should be quarantined.
6. 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/scheduled scans are working correctly.

Scan for specific types of malware

- "Scan for spyware and grayware" below
- "Scan for compressed executable files (real-time scans only)" on the next page
- "Scan process memory (real-time scans only)" on the next page
- "Scan compressed files" on the next page
- "Scan embedded Microsoft Office objects" on page 326

See also:

- "Enhanced anti-malware and ransomware scanning with behavior monitoring" on page 340

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 specific file that the spyware scan engine should ignore, see "Create anti-malware exceptions" on page 357.

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.

Note: 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. (See "Configure how to handle malware" on page 332.) If users regularly exchange real-time compressed executable files, 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 (real-time scans only)

Monitor process memory in real time and perform additional checks with the Trend Micro Smart Protection network to determine whether 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 347

1. Open the properties of the malware scan configuration.
2. On the **General** tab, select **Scan process memory for malware**.
3. Click **OK**.

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.

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**.

Specify the files to scan

To specify the files to scan for malware, identify files and directories to include in the scan and then of those files and directories, identify exclusions. You can also scan network directories:

- "Inclusions" below
- "Exclusions" on the next page
- "Scan a network directory (real-time scan only)" on page 332

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. (See "Syntax for directory lists" on page 328.)

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. (See "Syntax of file extension lists" on page 332.)

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 drop-down menu either select an existing list or select **New** to create one.
7. Click **OK**.

Exclusions

Exclude specific directories, files, and file extensions from being scanned. For real-time scans (except when performed by Deep Security Virtual Appliance), you can also exclude specific process image files from being scanned.

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.

To exclude directories, files, and process image files, you create a list that uses patterns to identify the item 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. (See "Syntax for directory lists" below.)
   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. (See "Syntax of file lists" on page 330, "Syntax of file extension lists" on page 332, and "Syntax of process image file lists (real-time scans only):" on page 332.)
5. Click **OK**.

Test file exclusions

Before continuing with further Anti-Malware configuration steps, test file exclusions to ensure they're working correctly:

Note: Before you begin, make sure the real-time scan is enabled and a configuration is selected.

1. Go to **Policies > Common Objects > Other > Malware Scan Configurations**.
2. Click **New > New Real-time Scan Configuration**.
3. Go to the **Exclusions** tab, and select **New** from the directory list.
4. Name the directory list.
5. Under **Directory(s)** specify the path of the directory you want to exclude from the scan. For example, `c:\Test Folder\` . Click **OK** .
6. Go to the **General** tab, name the manual scan, and click **OK**.
7. 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

Note: 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	*C:\Program Files* Excludes all files in the

Exclusion	Format	Description	Examples
		subdirectories.	"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**** Excludes all files in all subdirectories of "abc" but does not exclude the files in the "abc" directory. ***C:\abc\wx*z*** *Matches:* C:\abc\wxz\ C:\abc\wx123z\ *Does not match:* C:\abc\wxz C:\abc\wx123z ***C:\abc*wx*** *Matches:* C:\abc\wx\ C:\abc\123wx\ *Does not match:* C:\abc\wx 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**** 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	${ENV VAR}	Excludes all files and subdirectories defined by an environment variable. For a Virtual Appliance, the value pairs for the environment variable must be defined in **Policy or Computer Editor > Settings > General > Environment Variable Overrides.**	***${windir}*** 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*** Excludes all files named "abc.doc" in all directories. Does not exclude "abc.exe".
File path	FILEPATH	Excludes the specific file specified by the file path.	***C:\Documents\abc.doc*** Excludes only the file named "abc.doc" in the "Documents" directory.
File path with wildcard (*)	FILEPATH	Excludes all the specific 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.
File with wildcard (*)	FILE*	Excludes all files with a matching pattern in the file name.	***abc*.exe*** Excludes any file that has prefix of "abc" and extension of ".exe". ***.db*** *Matches:* 123.db abc.db *Does not match:* 123db 123.abd cbc.dba ***db*** *Matches:* 123.db 123db ac.db acdb db *Does not match:* db123 ***wxy*.db*** *Matches:* wxy.db wxy123.db *Does not match:* wxydb

Exclusion	Format	Description	Example
File with wildcard (*)	FILE.EXT*	Excludes all files with a matching pattern in the file extension.	***abc.v**** Excludes any file that has file name of "abc" and extension beginning with ".v". ***abc.*pp*** *Matches:* abc.pp abc.app *Does not match:* wxy.app ***abc.a*p*** *Matches:* abc.ap abc.a123p *Does not match:* abc.pp ***abc.**** *Matches:* abc.123 abc.xyz *Does not match:* wxy.123
File with wildcard (*)	FILE*.EXT*	Excludes all files with a matching pattern in the file name and in the extension.	***a*c.a*p*** *Matches:* ac.ap a123c.ap ac.a456p a123c.a456p *Does not match:* ad.aa
Environment variable	${ENV VAR}	Excludes files specified by an environment variable with the format ${ENV VAR}. These can be defined or overridden using **Policy or Computer Editor > Settings > General > Environment Variable Overrides.**	***${myDBFile}*** 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* 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 (real-time scans only):

Exclusion	Format	Description	Example
File path	FILEPATH	Excludes the specific Process Image file specified by the file path.	*C:\abc\file.exe* Excludes only the file named "file.exe" in the "abc" directory.

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.

Note: Resources accessed in "**~/.gvfs**" via GVFS, a virtual file system available for the GNOME desktop, will be treated as local resources, not network drives.

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 how to handle malware

Configure how Deep Security behaves when malware is detected:

- "Customize malware remedial actions" on the next page
- "Generate alerts for malware detection" on page 335

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.)

  Note: 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 can't 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.

  Note: 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**.

  Note: 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**.

  Note: 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" below.)

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 316	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 317	Quarantine
"Packer" on page 317	Quarantine
"Spyware/grayware" on page 318	Quarantine
"Cookie" on page 319	Delete (Does not apply to real-time scans)
"Other threats" on page 319	Clean

Malware Type	Action
	If a threat cannot be cleaned, it is handled as follows: • on Windows, the infected file is deleted but can be viewed and restored, if needed • on Linux or Solaris, access is denied to the infected file 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 319	ActiveAction

Note: 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).

   Note: When **Inherited** is selected, the file hash settings are inherited from the current policy's parent policy.

   Note: 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 don't 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 866.

Performance tips for anti-malware

To improve system resources utilization on Deep Security Agent, you can optimize these performance-related settings according to best practices.

See also:

- "Create anti-malware exceptions" on page 357
- "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

[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).

Security Virtual Appliances. The setting can be overridden at the policy level and at the computer level.

Tip: Alerts are raised when there is not enough disk space to store an identified file.

1. Open the policy or computer editor that you want to configure.
2. Click **Anti-Malware > Advanced**.
3. Under **Identified Files**, clear **Default**.
4. Specify the disk space to use in the **Maximum disk space used to store identified files** box.
5. Click **Save**.

Optimize CPU usage

- Exclude files from real-time scans if they are normally safe but have high I/O, such as databases, Microsoft Exchange quarantines, and network shares (on Windows, you can use procmon to find files with high I/O). See "Exclusions" on page 327.
- Do not scan network directories. See "Scan a network directory (real-time scan only)" on page 332
- Do not use Smart Scan if the computer doesn't have reliable network connectivity to the Trend Micro Smart Protection Network or your Smart Protection Server. See "Smart Protection in Deep Security" on page 347.
- 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 991.
- 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 324.

Warning: Most malware is small, and nested compression indicates malware. But if you don't scan large files, there is a small risk that anti-malware won't detect some malware. You can mitigate this risk with other features such as integrity monitoring. See

- Use 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, after you have enabled it, restart the computer.

  Note: Do not enable multi-threaded processing under the following circumstances:
  - Resources are limited (for example, CPU-bound tasks)
  - Resources should be held by only one operator at a time (for example, IO-bound tasks)

  a. Click **Policies**.
  b. Double-click to open the policy where you want to enable multi-threaded processing.
  c. Click **Anti-Malware > Advanced**.
  d. In the Resource Allocation for Malware Scans section, select **Yes**.
  e. Restart the computers on which you enabled multi-threaded processing for the setting to take effect.

  Note: Multi-threaded processing may reduce the number of CPU cores available at a given time to the computer's other processes.

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 324.

  Warning: Most malware is small, and nested compression indicates malware. But if you don't scan large files, there is a small risk that anti-malware won't detect some malware. You can mitigate this risk with other features such as integrity monitoring. See "Set up Integrity Monitoring" on page 449

Disable Windows Defender after installing Deep Security anti-malware on Windows Server 2016

When you install the Anti-Malware module for a Deep Security 10.0 Agent on Windows Server 2016, the agent will automatically disable Windows Defender, but not all of the Windows processes related to the Windows Defender service. To do so, you need to reboot Windows Server 2016 after the Deep Security Anti-Malware module installation finishes. The Deep Security Agent will open a Windows message to let you know when to reboot.

Note: The agent will report a computer warning event ("Computer reboot is required for Anti-Malware protection") to the Deep Security Manager. This event will remain indefinitely, and will need to be manually dismissed by an administrator.

Installing the Anti-Malware module when Windows Defender is already disabled

If you disable Windows Defender before installing the Deep Security Anti-Malware module, the Deep Security Agent will not open a Windows reboot message. However, you still need to reboot Windows Server 2016 to ensure that Deep Security Anti-malware functions correctly.

Detect emerging threats using Predictive Machine Learning

Use Predictive Machine Learning to detect unknown or low-prevalence malware. (For more information, see "Predictive Machine Learning" on page 316.)

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. "Enable Predictive Machine Learning" below

As with all detected malware, Predictive Machine Learning logs an event when it detects malware. (See "About Deep Security event logging" on page 566.) You can also create an exception for any false positives. (See "Create anti-malware exceptions" on page 357.)

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" on page 322.) 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 326.

These settings can only be applied to the real-time scan configuration for Windows computers.

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.**
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 machines that are 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 hasn't yet been added to the anti-malware patterns (known as a zero-day attack).

In this article:

For an overview of the anti-malware module, see "About Anti-Malware" on page 312.

How does enhanced scanning protect you?

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 writers 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 writers 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: Recently, 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.

How to enable enhanced scanning

Enhanced scanning is configured as part of the anti-malware settings that are applied to a policy or individual computer. For general information on configuring anti-malware protection, see "Enable and configure anti-malware" on page 319.

Note: These settings can only be applied to Windows machines that are protected by a Deep Security Agent.

Warning: Enhanced scanning may have a performance impact on agent computers running applications with heavy loads. We recommend reviewing the "Performance tips for anti-malware" on page 336 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" on page 322).
3. On the **General** tab, select these options:
   - **Detect suspicious activity and unauthorized changes (incl. ransomware):** Enables the threat detection, anti-exploit, and ransomware detection features that are described above.
   - **Back up and restore ransomware-encrypted files:** When this option is selected, Deep Security will create backup copies of files that are being encrypted, in case they are being encrypted by a ransomware process.
4. Click **OK**.

Note: 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 the **Anti-Malware State** is **On** or **Inherited (On)**.
3. The General tab contains sections for **Real-Time Scan**, **Manual Scan**, and **Scheduled Scan**. In the appropriate sections, use the **Malware Scan Configuration** list to select the scan configuration that you created above.
4. Click **Save**.

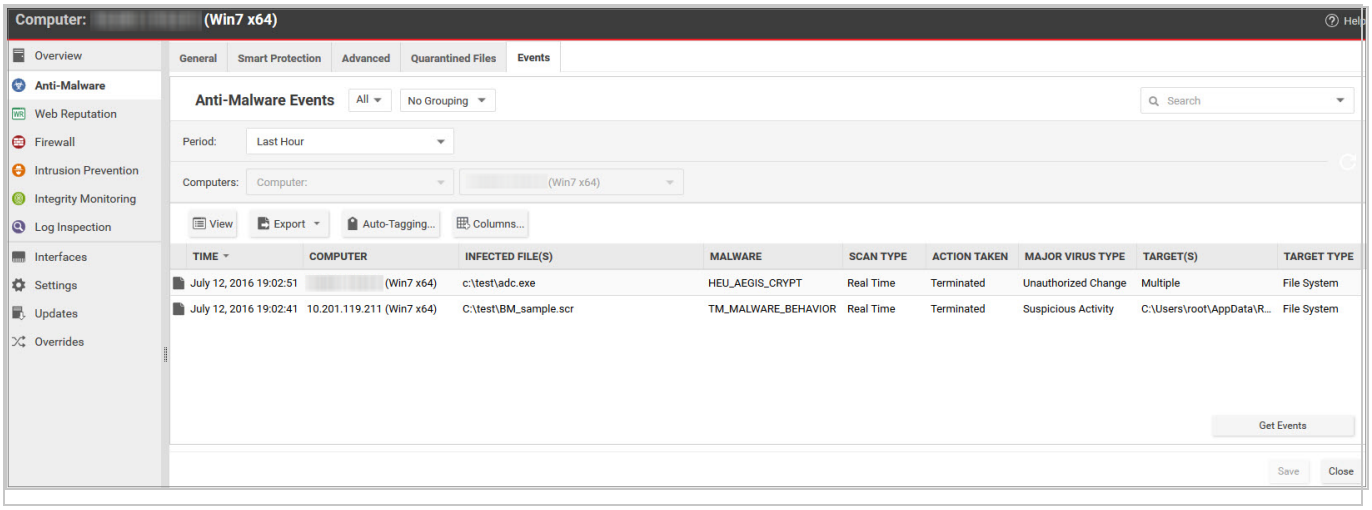
What happens when enhanced scanning finds a problem?

When Deep Security discovers activity or files that match the enhanced scan settings you have enabled, it will log an event (go to **Events & Reports > Events > Anti-Malware Events** to see a list of events). The event will be identified as "Suspicious activity" or "Unauthorized change" in the **Major Virus Type** column and details will be displayed in the **Target(s)** and **TargetType** columns.

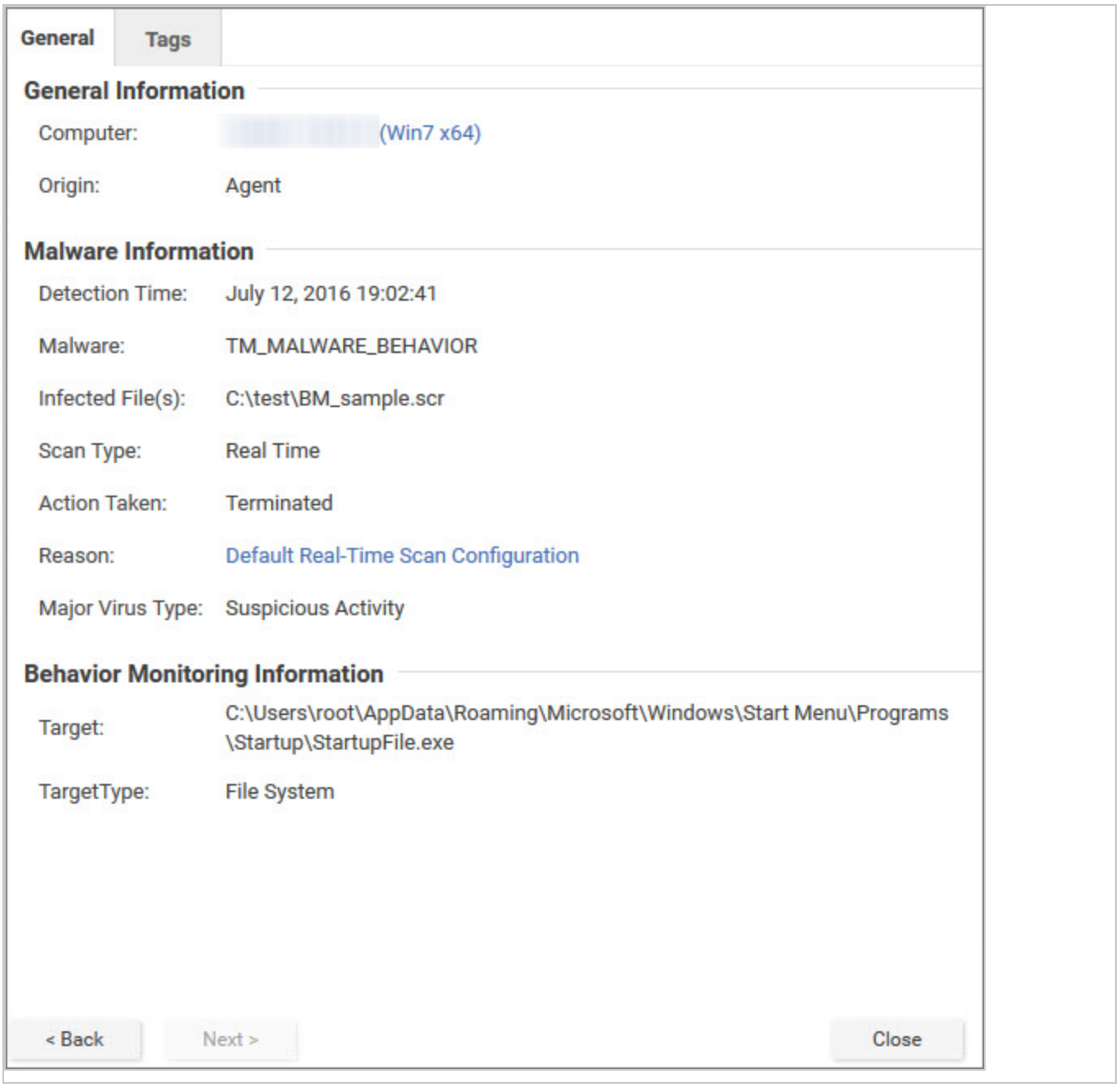
[1]You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

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:

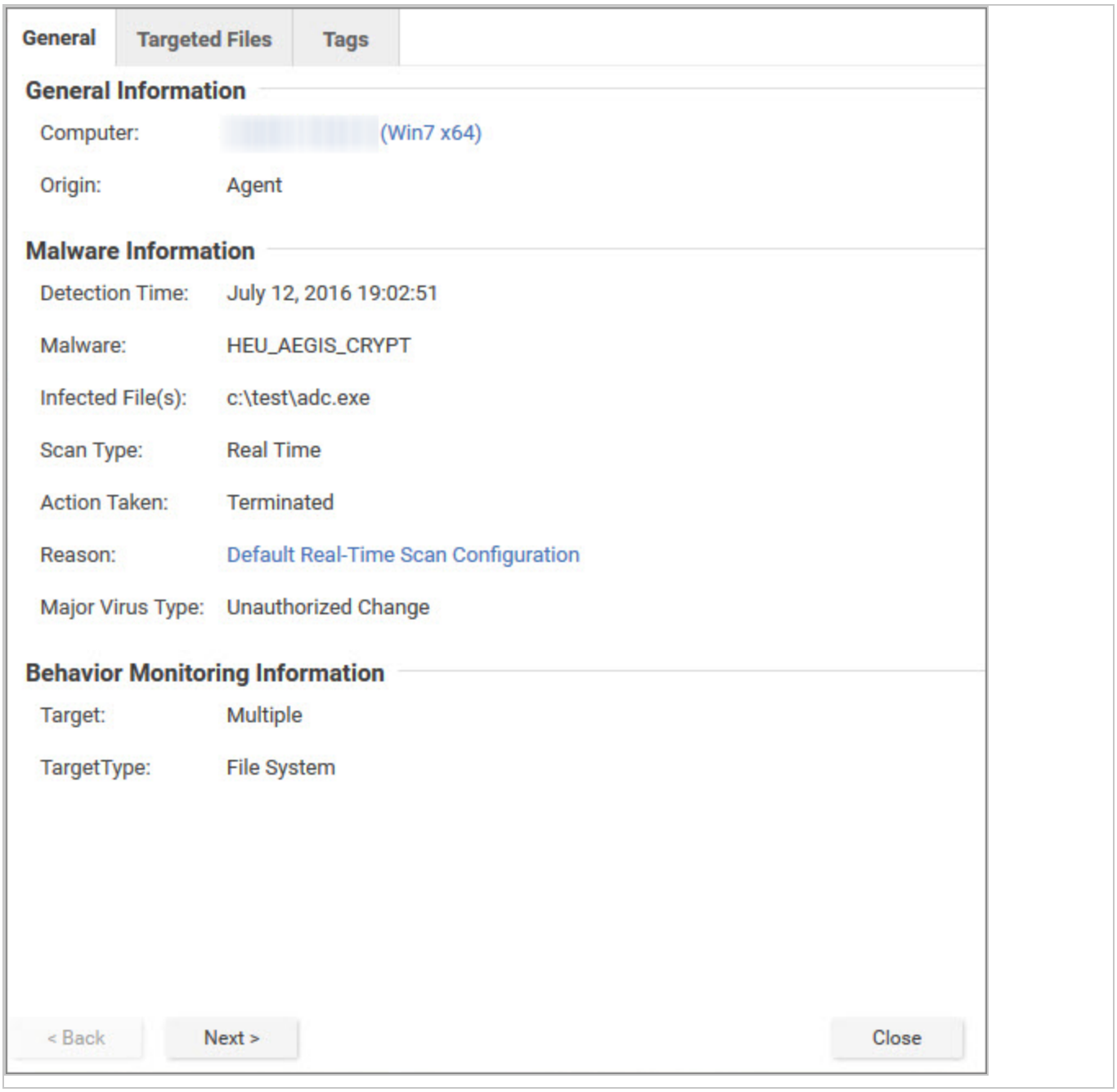
- **Deny Access:** When Deep Security detects an attempt to open or execute a suspicious file, it immediately blocks the operation and records an anti-malware event.
- **Terminate:** Deep Security terminates the process that performed the suspicious operation and records an anti-malware event.
- **Clean:** 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.

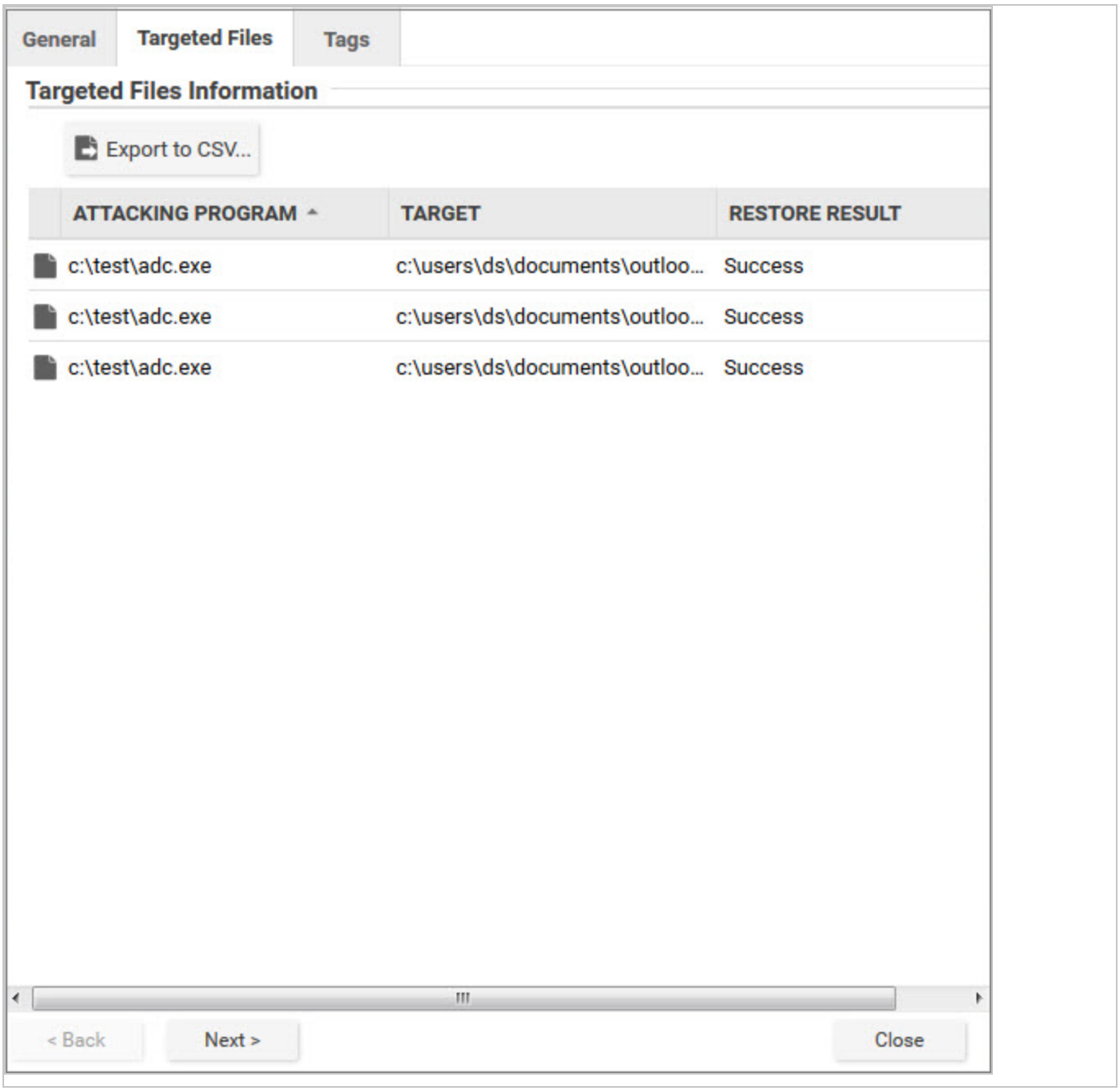


Double-click an event to see details:



Events related to ransomware have an additional **Targeted Files** tab:


General
Targeted Files
Tags
General Information
Computer:
(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
< Back
Next >
Close



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**.

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:

See also "Integrate with Smart Protection Server" on page 1049 for AWS deployment instructions, and the Smart Protection Server documentation for instructions on manually deploying the server.

Anti-malware and Smart Protection

Enable Smart Scan

Smart Scan is available in the anti-malware module. It leverages 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 much larger full malware pattern from a Smart Protection 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, your relay agents must download the full malware pattern from a Smart Protection 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.

Note: Verify that the computer can reliably connect to the global Trend Micro Smart Protection Network URLs (see "Port numbers, URLs, and IP addresses" on page 106 for a list of URLs). If

connectivity is blocked by a firewall, proxy, or AWS security group or if the connection is unreliable, it will reduce anti-malware performance.

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 will 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 will not result in local patterns being used to scan for malware since no anti-malware patterns will be 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.

To edit Smart Protection Server for File Reputation Service:

1. Go to **Computers** or **Policies > Anti-Malware > Smart Protection**.
2. You can 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, we recommend that you 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 808.

   Note: After you select a proxy, you will need to restart any agents that will be using it.
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.)

> **Note:** 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.

5. Set the **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.

To edit Smart Protection Server for Web Reputation Service:

1. Go to **Computers** or **Policies > Web Reputation > Smart Protection**.
2. You can 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, we recommend that you 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 808.

   > **Note:** After you select a proxy, you will need to restart any agents that will be using it.

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.)

   > **Note:** 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.

5. Set the **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 anonymous 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**.

Note: Smart Feedback will use the agents, appliances, and relays (security updates) proxy selected in the Proxy Server Use section on the **Administration > System Settings > Proxies** tab.

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 333 files.
- On Linux agents, you can view and restore only quarantined files.

Topics on this page:

For information about events that are generated when malware is encountered, see "Anti-malware events" on page 765.

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 & 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.

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 right-click context menu, you can:

-  **Restore** identified files back to their original location and condition.
-  **Download** identified files from the computer or Virtual Appliance to a location of your choice.
-  **Delete** one or more identified files from the computer or Virtual Appliance.
-  **Export** information about the identified file(s) (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.

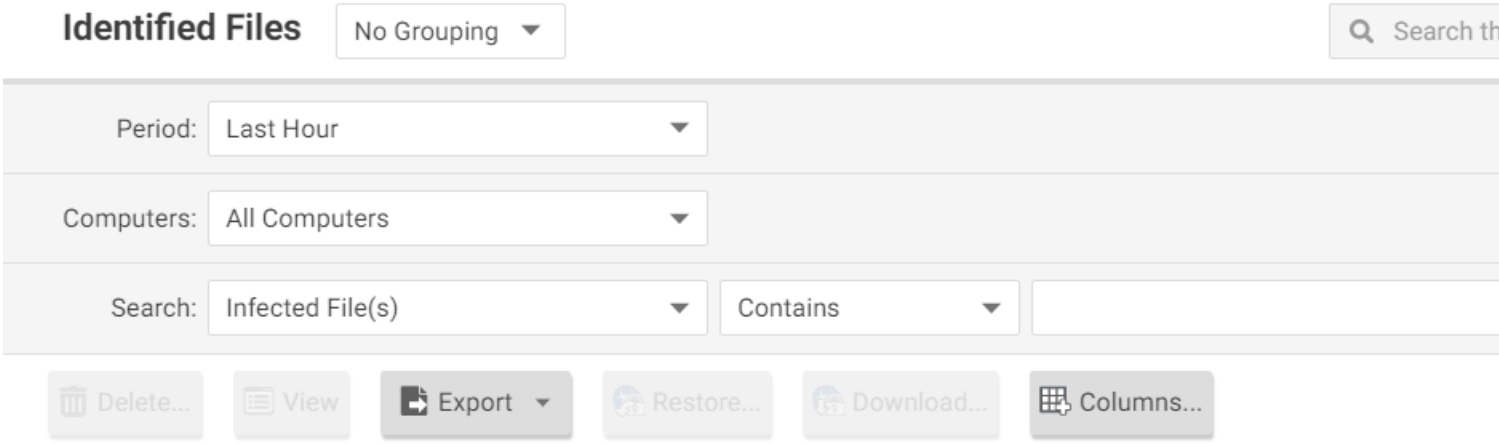
Note:
Identified files are automatically deleted from a Deep Security Virtual Appliance when a:

- VM is moved to another ESXi host by vMotion. Identified files associated with that VM will be deleted from the virtual appliance.
- VM is deactivated from the Deep Security Manager. Identified files associated with that VM will be 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 will be deleted.
- Deep Security Virtual Appliance is deleted from the vCenter. All the identified files stored on that virtual appliance will also be 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:



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

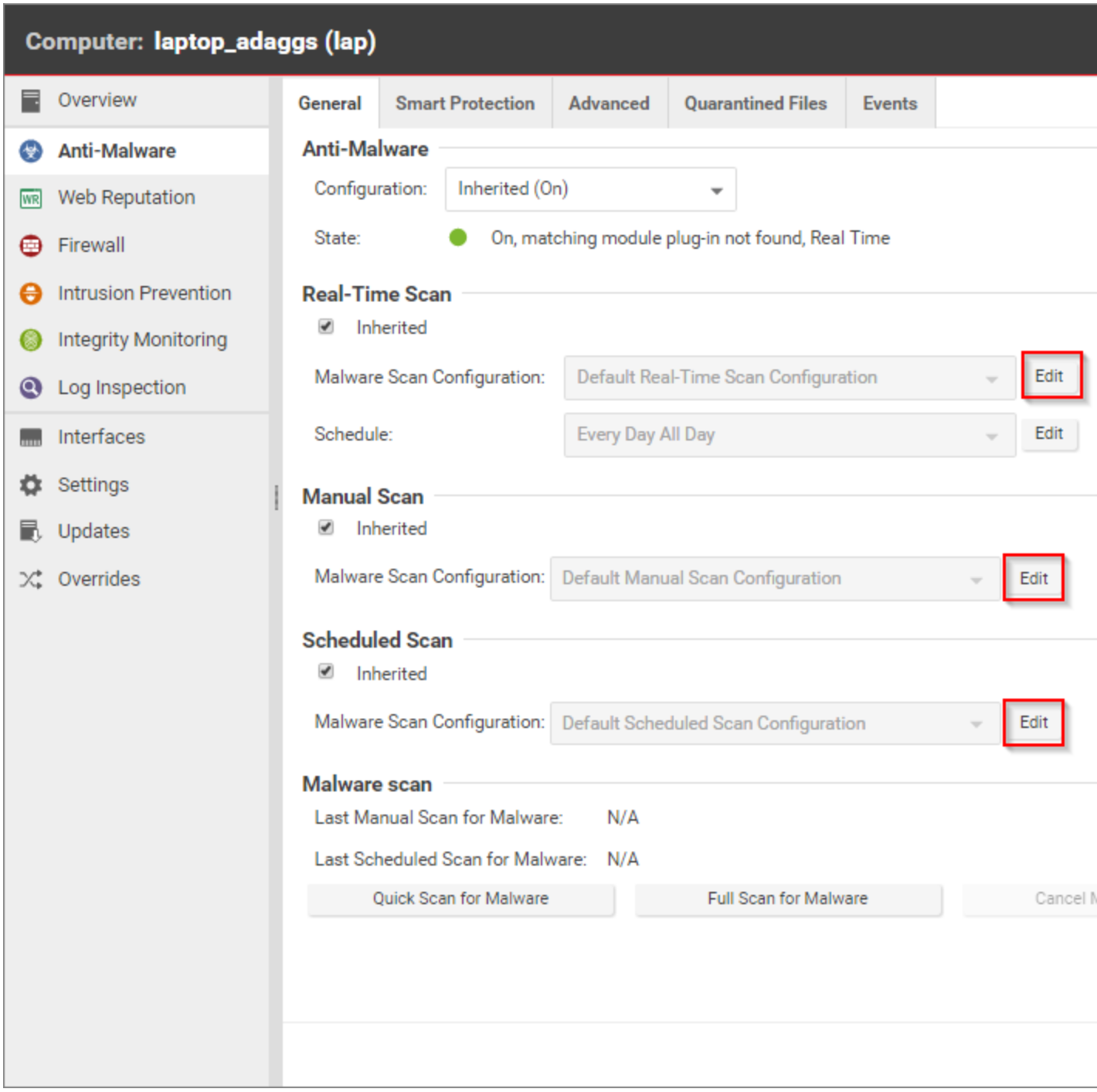
Create a scan exclusion for the file

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.

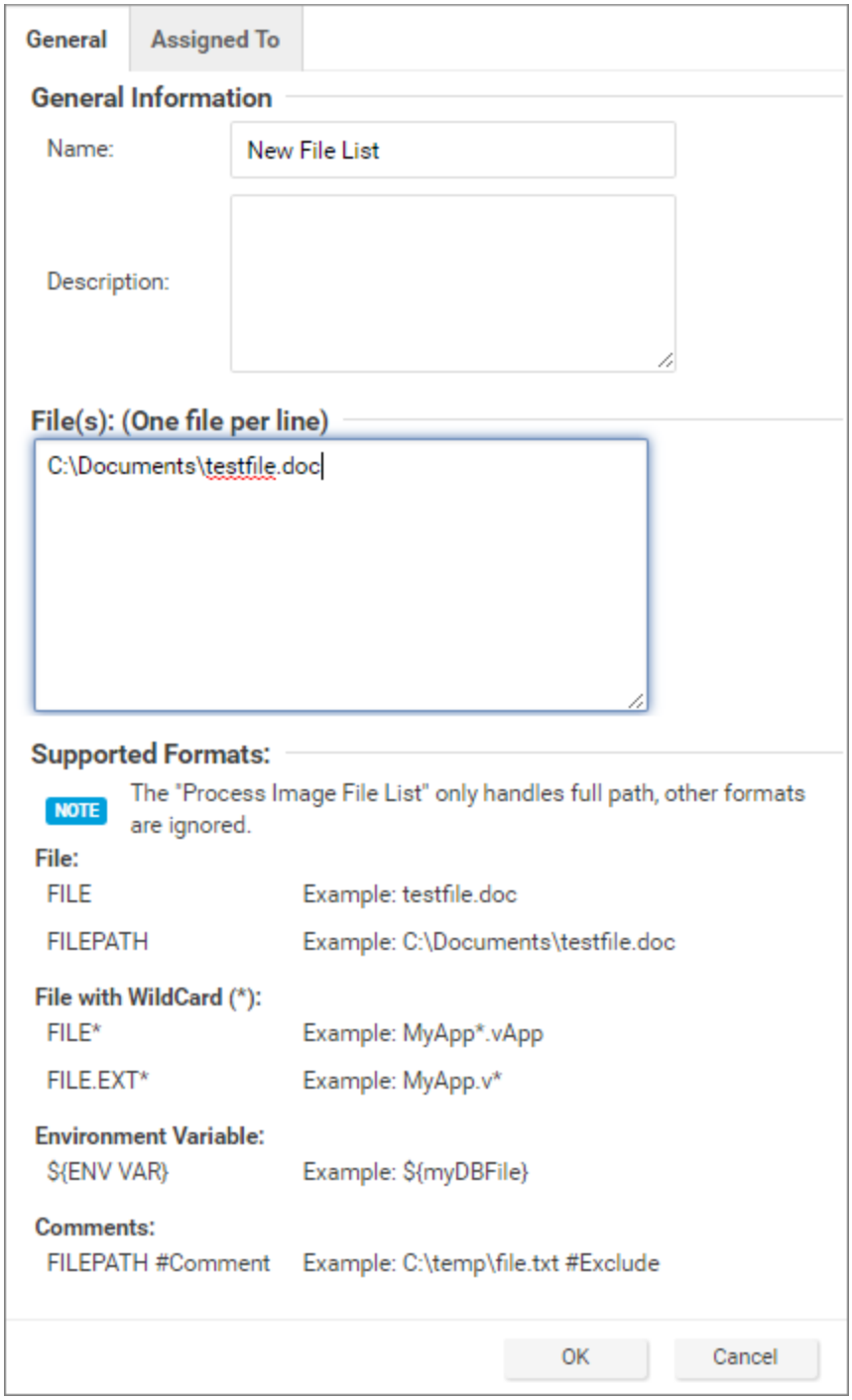
1. Open the Computers page and go to **Anti-Malware > Identified Files** and double click the identified file to view its properties.
2. Note the file's exact name and original location.
3. Still in the Computers page, go to **Anti-Malware > General** and click the Edit button next to each Malware Scan that's in effect to open the Malware Scan Configuration properties

window.



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.



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 only on Windows 32-bit systems.

Create anti-malware 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 312.

Note: You can also exclude files from real-time, manual, and scheduled scans. See "Specify the files to scan" on page 326.

Exceptions can be created for the following types of malware and malware scans:

- Predictive Machine Learning scans (for information, see "Detect emerging threats using Predictive Machine Learning" on page 339.)
- Scans for spyware and grayware (for information, see "Scan for spyware and grayware" on page 324)
- Behavior monitoring protection (for information, see "Enhanced anti-malware and ransomware scanning with behavior monitoring" on page 340)

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**, and **Behavior Monitoring Protection Exceptions** sections.

See also "Scan exclusion recommendations" on the next page.

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.

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 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. (See "Restore identified files " on page 354.)

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 how to handle malware" on page 332.

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.

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 and logs" on page 1075.

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

Note: For a list of operating systems where web reputation is supported, see "Supported features by platform" on page 90.

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 will either block or allow access to the URL.

Note: The web reputation module does not block HTTPS traffic.

To enable and configure web reputation, perform the basic steps below:

1. "Turn on the web reputation module" on the next page
2. "Switch between inline and tap mode" on the next page
3. "Enforce the security level" on the next page
4. "Create exceptions" on page 363
5. "Configure the Smart Protection Server" on page 364
6. "Edit advanced settings" on page 366
7. "Test Web Reputation" on page 366

To suppress messages that appear to users of agent computers, see "Configure notifications on the computer" on page 336

Turn on 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**.

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 410.

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

[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).

- **Suspicious**: Associated with spam or possibly compromised

Security levels determine whether Deep Security will allow or block 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.

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 either:
      - **Allow URLs from the domain**: Allow all pages from the domain. Sub-domains are supported. Only include the domain (and optionally sub-domain) in the entry. For example, "example.com" and "another.example.com" are valid entries.
      - **Allow the URL:**: The URL as entered will be allowed. Wildcards are supported. For example, "example.com/shopping/coats.html", and "example.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 either:
      - **Block URLs from the domain**: Block all pages from the domain. Sub-domains are supported. Only include the domain (and optionally sub-domain) in the entry. For example, "example.com" and "another.example.com" are valid entries.
      - **Block the URL**: The URL as entered will be blocked. Wildcards are supported. For example, "example.com/shopping/coats.html", and "example.com/shopping/*" are valid entries.
      - **Block URLs containing this keyword**: Any URL containing the keyword will be 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** from the drop down menu 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 (ex: "http://[server]:5274")**.
   b. Enter the Smart Protection Server URL into the field and click **Add**. To find the Smart Protection Server URL, do one of the following:
      - 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 11.0 Deep Security Agents and up. If you have 10.3 or earlier agents, use the HTTP URL.

      Or

      - If you deployed the Smart Protection Server in AWS, go to the AWS **CloudFormation** service, select the check box next to the Smart Protection Server stack, and in the bottom pane, click the **Outputs** tab. The Smart Protection Server's HTTP and HTTPS URLs appear in the **WRSurl** and **WRSHTTPSurl** fields. The WRSHTTPSurl is only supported with 11.0 Deep Security Agents and up. If you have 10.3 or earlier agents, use the WRSurl URL.
   c. Optionally select **When off domain, connect to global Smart Protection Service. (Windows only)**.
5. Click **Save**.

Smart Protection Server Connection Warning

This option determines whether 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**.

Note: 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 will be 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**. Click **Save**.
4. Open a browser and attempt to access the website. A message denying the access should appear.
5. 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 370.

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:

- Replace specifically defined or suspicious byte sequences
- 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 216.)

For information about how you can affect the functionality of rules, see "Configure intrusion prevention rules" on page 377.

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 397.

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 383.)

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 221.)

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 371 and "Switch to Prevent mode" on page 376.)

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 410.

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 385.)

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

[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.

Security Manager, event logs are kept for a period of time which can be configured. The default setting is one week. You can configure event logging for individual rules as required. (See "Configure event logging for rules" on page 381.)

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 573.

Support for secure connections

The Intrusion Prevention module supports inspecting packets over secure connections. See "Inspect SSL or TLS traffic" on page 399.

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 305.

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 231.

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 373

3. "Apply recommended rules" on page 374
4. "Monitor your system" on page 375
5. "Enable 'fail open' for packet or system failures" on page 376
6. "Switch to Prevent mode" on page 376
7. "Implement best practices for specific rules" on page 376

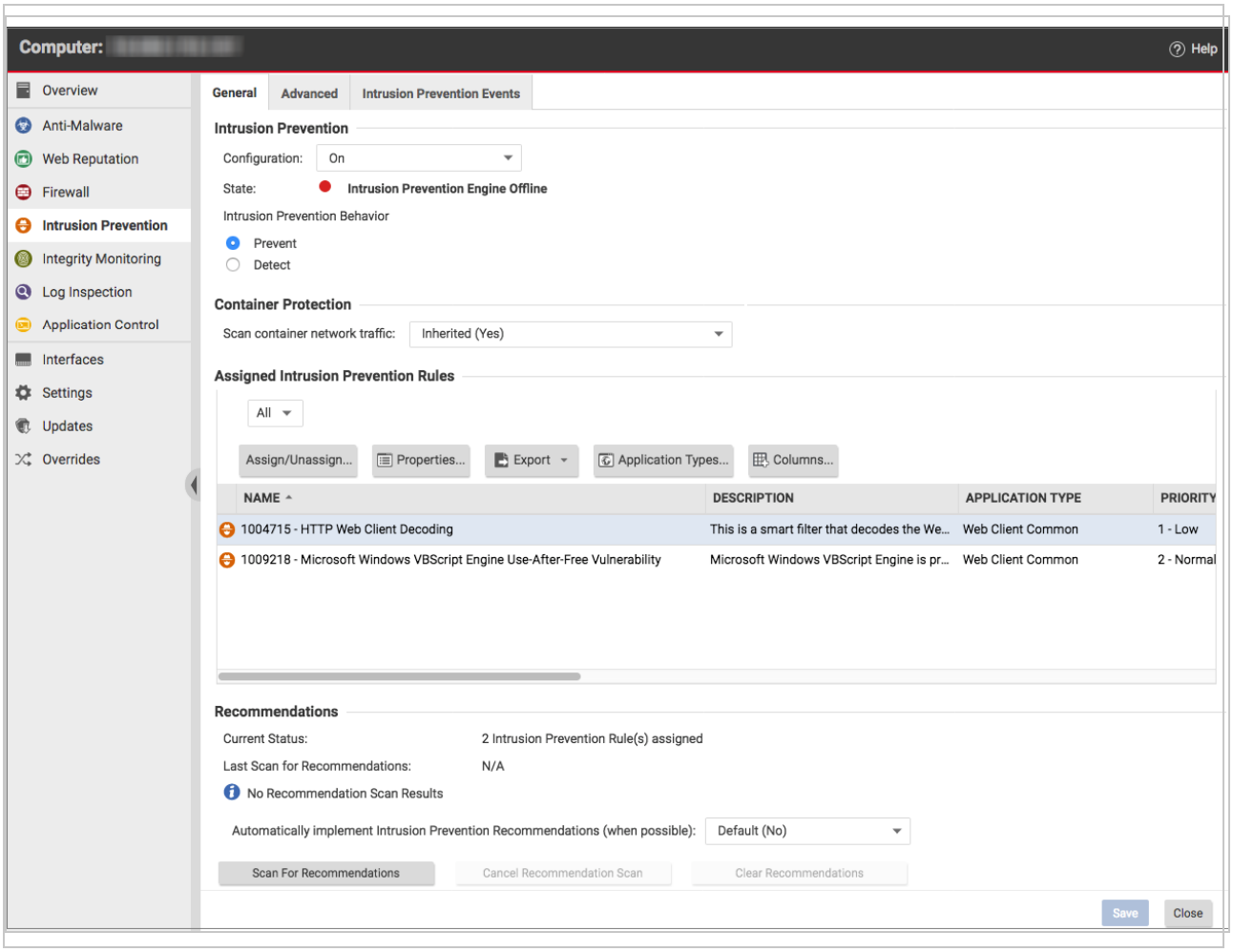
Note: CPU usage and RAM usage varies by your IPS configuration. To optimize IPS performance on Deep Security Agent, see "Performance tips for intrusion prevention" on page 406.

For an overview of the Intrusion Prevention module, see "About Intrusion Prevention" on page 366.

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)**.



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 410.)

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 385.)

Test Intrusion Prevention

You should test that the Intrusion Prevention module is working properly before continuing with further steps.

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. Turn off the Web Reputation module. In Deep Security Manager, click **Computers**, then double-click the computer where you'll test Intrusion Prevention. In the computer's dialog box, 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 box, 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 box, click **Intrusion Prevention**. Click **Assign/Unassign**. Search for `1005924`. The **1005924 - Restrict Download of EICAR Test File Over HTTP** policy appears. Select its check box and click **OK**. The policy is now assigned to the computer.
5. Try to download the EICAR file (you can't, 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.

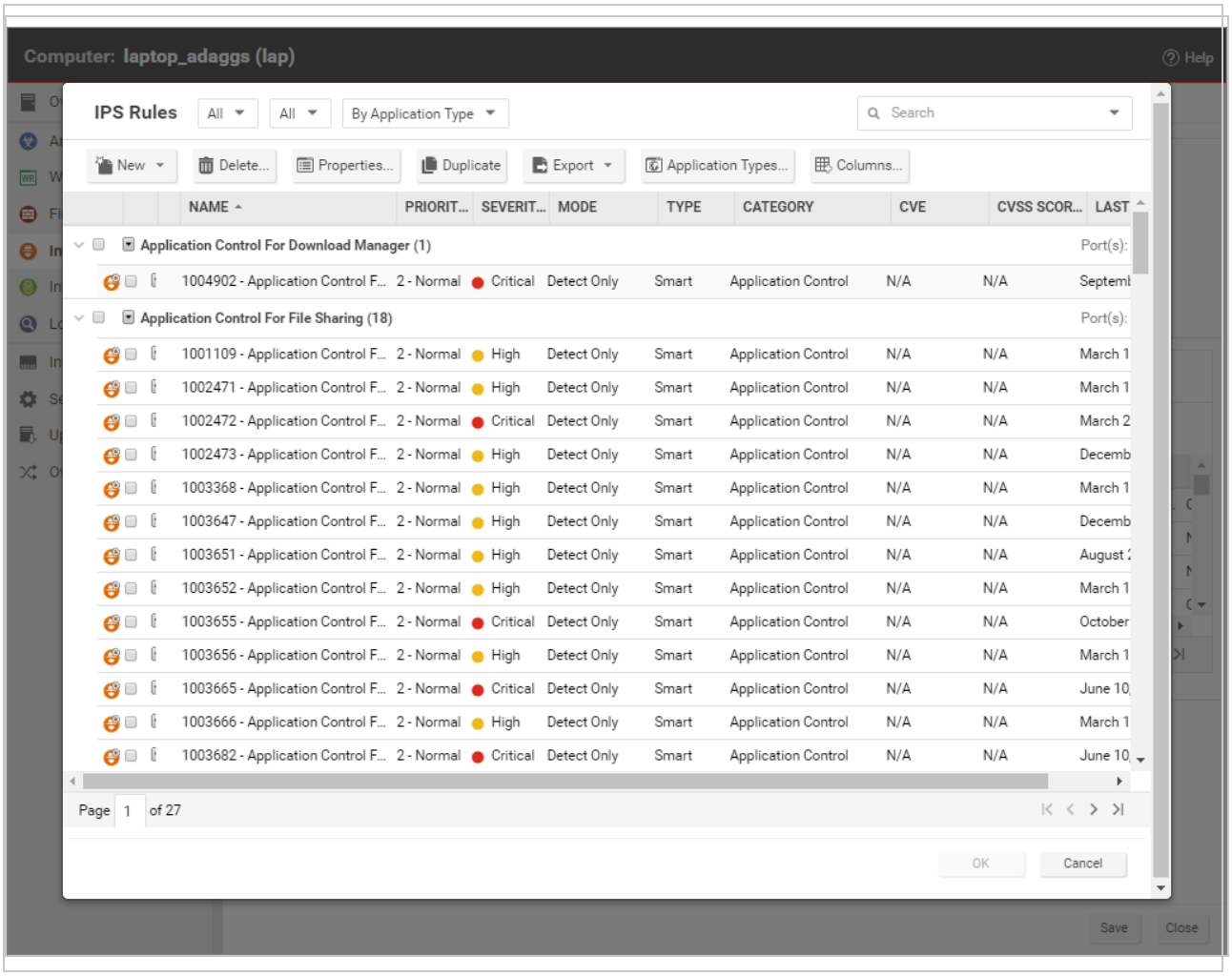
Note: Although recommendation scans are performed for a specific computer, you can assign the recommendations to a policy that the computer uses.

For more information, see "Manage and run recommendation scans" on page 221.

1. Open the properties for the computer to scan. Run the recommendation scan as described in "Manually run a recommendation scan" on page 226.

   Note: You can configure Deep Security to "Automatically implement recommendations" on page 227 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 228.



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 991.

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 406.)

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 380.)

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 411.

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.

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. The 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

[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).

should run in Detect mode for a period of time before switching to Prevent mode to determine if any configuration changes are required.

Quite often, changes are required to the list of illegal characters.

Refer to the following Knowledge Base articles for more details on this rule and how to tune it:

- https://success.trendmicro.com/solution/1098016
- https://success.trendmicro.com/solution/1054481
- https://success.trendmicro.com/solution/1096566

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 https://success.trendmicro.com/solution/1098159

Apply NSX security tags

Configure intrusion prevention rules

Perform the following tasks to configure and work with intrusion prevention rules:

For an overview of the intrusion prevention module, see "About Intrusion Prevention" on page 366.

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 216.)

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 385.

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 385.

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 385.

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. Agentless protection is not available with Deep Security as a Service.

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 368.

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.

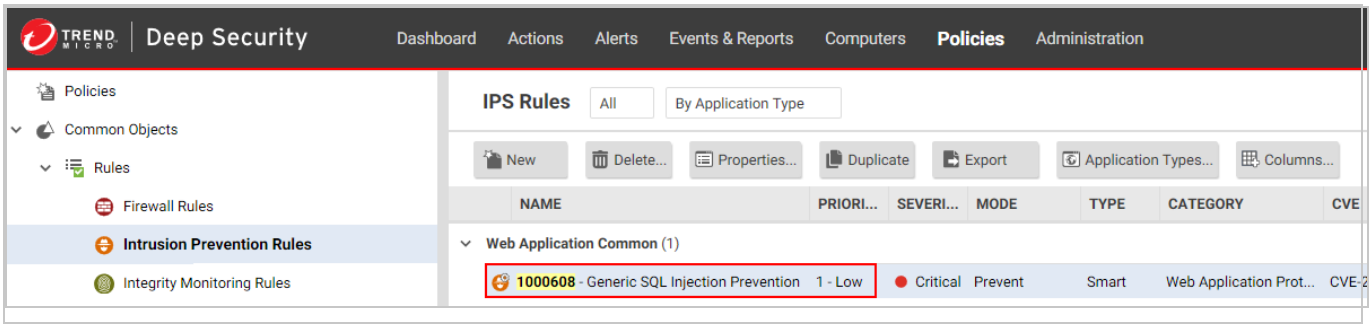
Export and import rules

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.



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, @@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
```

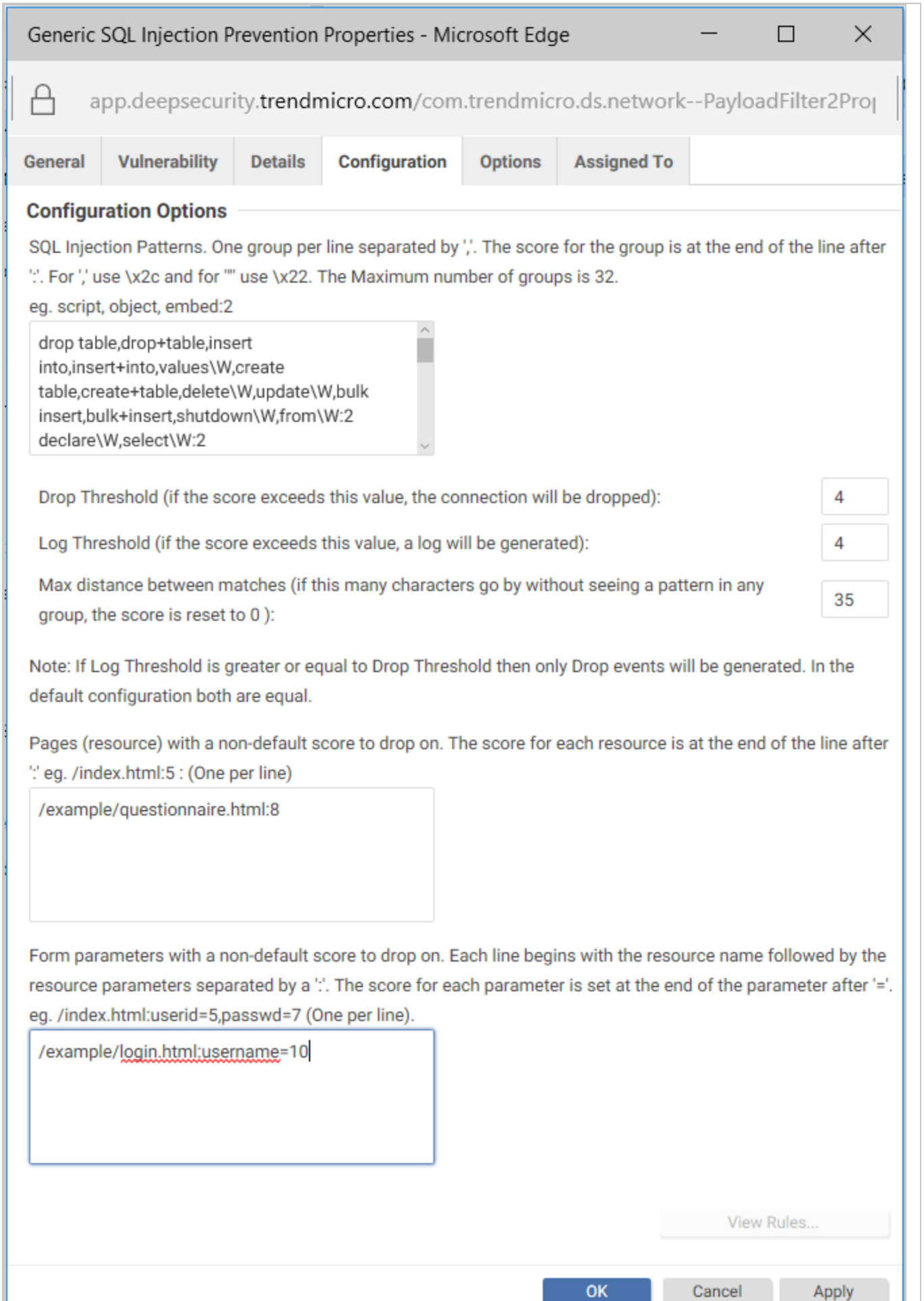
Then the total score is 3 (2+1+0+0) because:

- 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
View Rules...
OK
Cancel
Apply

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 \A	alphabetic characters, a-z A-Z non-alphabetic characters example: `delete\a` means "the word 'delete' followed by alphabetical characters"
\w \W	alphanumeric characters, a-z A-Z 0-9 non-alphanumeric characters

Enter this string...	To denote...
	example: `delete\W` means "the word 'delete' followed by non-alphanumeric characters"
\d \D	digits 0-9 non-digit characters example: `delete\d` means "the word 'delete' followed by digits between zero and nine"
\s \S	whitespace not whitespace [\r,\n,\t,0x32] example: `delete\S` means "the word 'delete' followed by non-whitespace"
\p \P	punctuation character, printable ascii other than above non-punctuation character example: `delete\p` means "the word 'delete' followed by a punctuation character or printable ascii"
\c \C	control character, below 32, or greater than or equal to 127, not including whitespace non-control character You can find details on control characters here.
\.	any
\xDD	hex byte 0xDD
\x2c	comma character (,)
\x22	double-quotes character (")
\\	escaped backslash (\)

Enter this string...	To denote...
|	escaped pipe (|)
|xx xx xx...|	hex pipe (byte sequence)

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 385.

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 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.

---

[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.

Inspect SSL or TLS traffic

For the intrusion prevention module, you can configure SSL inspection for a given credential-port pair on one or more interfaces of your protected computer.

Note: Compressed traffic does not support SSL inspection.

Credentials can be imported in PKCS#12 or PEM format. The credential file must include the private key. Windows computers can use CryptoAPI directly.

For an overview of the intrusion prevention module, see "About Intrusion Prevention" on page 366.

In this topic:

Configure SSL inspection

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 SSL inspection through the Intrusion Prevention module.

To work around this issue, we recommend you 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 below) 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

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 configuration 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
```

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
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
0x00,0x35	AES256-SHA	TLS_RSA_WITH_AES_256_CBC_SHA	TLS_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
0x00,0x84	CAMELLIA256-SHA	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA

Hex Value	OpenSSL Name	IANA Name	NSS Name
0x00,0xBA	CAMELLIA128-SHA256	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256	TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
0x00,0xC0	not implemented	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256	TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256

Supported protocols

The following protocols are supported:

- SSL 3.0
- TLS 1.0
- TLS 1.1
- TLS 1.2

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) or **Deny Silent** (same behavior as Deny, but no event is logged):

Note: Deny (Deep Security drops the packet and logs an event) is not a customizable option.

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 (same function as Allow)	Deny	Deny	Ignore (same function as Allow)
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 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).	1 for Linux agents, otherwise 0	1 for Linux agents, otherwise 0	0	1 for Linux agents, otherwise 0
Timestamp PAWS Zero Allowed	Action to take when a TCP timestamp is zero	Deny for Linux agents or NDIS5, otherwise	Deny for Linux agents or NDIS5, otherwise	Deny	Deny for Linux agents or NDIS5, otherwise

Setting	Description	Normal value	Strict value	Default custom value (pre-10.2)	Default custom value (10.2 or later)
		Allow	Allow		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 Flags	Action to take when a packet has both SYN and FIN flags set	Deny	Deny	Deny	Deny
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

Setting	Description	Normal value	Strict value	Default custom value (pre-10.2)	Default custom value (10.2 or later)
FIN Packet Out of Connection	Action to take for a FIN packet without a known connection	Allow	Deny	Deny	Allow
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 366.

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 381) • Include packet data in the event log only during troubleshooting. (See "Configure event logging for rules" on page 381) • Assign only intrusion prevention rules that apply to the computer's OS and applications. See "Manage and run recommendation scans" on page 221 for information about using recommendation scans to discover applicable vulnerabilities and rules.

System resource	Settings that impact performance
	• 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 381) • Include packet data in the event log only during troubleshooting. (See "Configure event logging for rules" on page 381) • Do not monitor HTTP responses from the web server, especially if the policy has many signatures applied: a. Click **Policies > Intrusion Prevention Rules**. b. Right-click a rule in the Web Server Common application type and click **Application Type Properties**. 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 381)

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 221.)
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 429.

For more detailed information on how to create firewall rules, see "Create a firewall rule" on page 422.

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].

[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).

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**[1], 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**[2].
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**.

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:

---

[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).

- 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 '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**.

---

[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).

You have now enabled fail open behavior for system or packet check failures.

Turn on Firewall

To enable Firewall functionality on a computer:

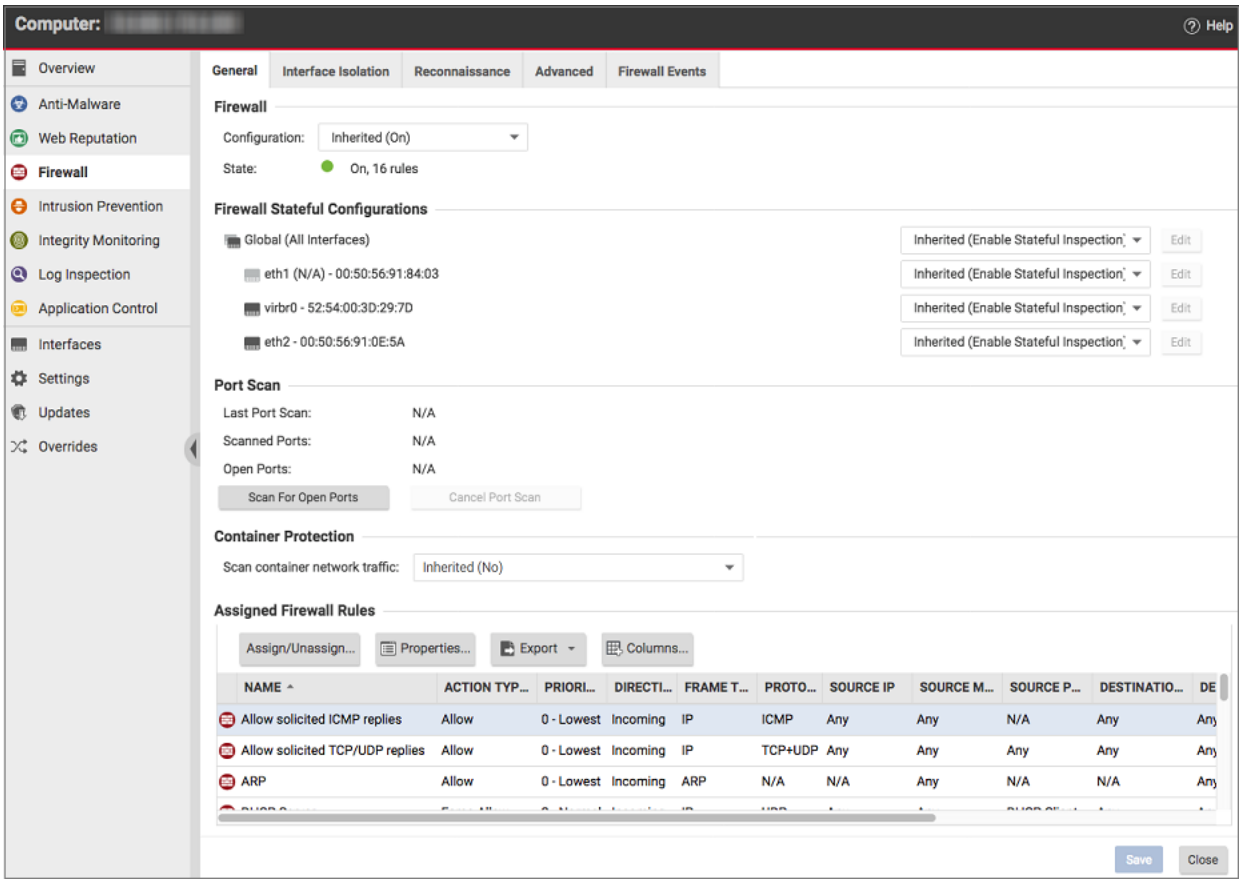
1. In the **Computer or Policy editor**[1], go to **Firewall** > **General**.
2. With Deep Security Agent 11.1 and earlier, the Firewall module inspects traffic that passes through the host computer's network interface to containers. With Deep Security Agent 11.2 or later, it can also inspect traffic 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**.

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).



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 believed to be malicious based on signatures or other information. 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. **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. 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. 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 422.

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 429.

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.

---

[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).

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 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 805.

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 409.

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 425.

When you're done with your firewall rule, you can also learn how to:

[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.

- "Configure rule events and alerts" on page 427
- "Set a schedule for the rule" on page 427
- "See policies and computers a rule is assigned to" on page 427
- "Assign a context to the rule " on page 427

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 428.

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 429.

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 311.

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 305.

> **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" on the next page
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:

- "Rule priority" on page 435
- "Putting rule action and priority together" on page 435

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 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)**
    a. **Bypass**
    b. **Force Allow**
    c. **Deny**
    d. **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

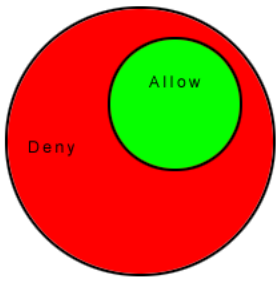
Deep Security firewall rules have both a rule action and a rule priority. Used in conjunction, these two properties allow you to create very flexible and powerful rule-sets. Unlike rule-sets used by other firewalls, which may require that the rules be defined in the order in which they should be run, 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

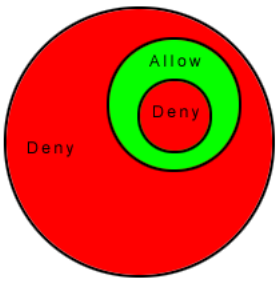
Each rule can have one of four actions.

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.

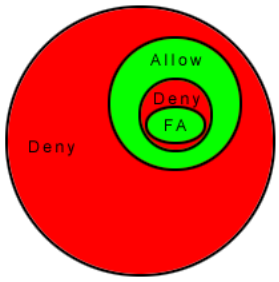
Implementing an Allow rule will cause all other traffic not specifically covered by the Allow rule to be denied:



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 the next page
- "Reconnaissance" on page 438
- "Advanced" on page 440
- "Events" on page 441

Note: This article includes references to the Deep Security Virtual Appliance, which is not available with Deep Security as a Service.

[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 441.

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.

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 422.

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

[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).

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.

Interface Patterns

When Interface Isolation is enabled, the firewall will try to match the regular expression patterns to interface names on the local computer.

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.

- **Reconnaissance Scan Detection Enabled:** Turn the ability to detect reconnaissance scans on or off.
- **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.)

Note: If you want 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.

For each type of attack, the **agent or appliance**[3] 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. (See **Administration > System Settings > Alerts**. The alerts are: "Network or Port Scan Detected", "Computer OS Fingerprint Probe Detected", "TCP Null Scan Detected", "TCP FIN Scan Detected", and "TCP Xmas Scan Detected.") 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**[4] **> 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** lists to set the number of minutes.

- **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

---

[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] 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.

[4] 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).

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).

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 805.

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.

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.

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 " below.
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 446
- "Export a stateful configuration " on page 445
- "Delete a stateful configuration " on page 446

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.

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 source port	Force Allow	0 - Lowest	Outgoing	IP	TCP	Any	80	Any	Any
K8s incoming TCP 10054 port	Force Allow	0 - Lowest	Incoming	IP	TCP	Any	Any	Any	10054
K8s outgoing	Force Allow	0 - Lowest	Outgoing	IP	TCP	Any	Any	Any	10054

Name	Action Type	Priority	Direction	Frame Type	Protocol	Source IP	Source Port	Destination IP	Destination Port
TCP 10054 port									
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
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 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" on the next page.

To more information on creating integrity monitoring rules, see "Create an Integrity Monitoring rule" on page 456. 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 460.

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.

Note: Integrity Monitoring detects changes made to the system, but will not prevent or undo the changes.

How to enable Integrity Monitoring

You can enable Integrity Monitoring in policies or at the computer level. To do so, you will need to:

1. "Turn on Integrity Monitoring" below.
2. "Run a Recommendation scan" on the next page.
3. "Apply the Integrity Monitoring rules" on page 451.
4. "Build a baseline for the computer" on page 453.
5. "Periodically scan for changes" on page 453.
6. "Test Integrity Monitoring" on page 453.

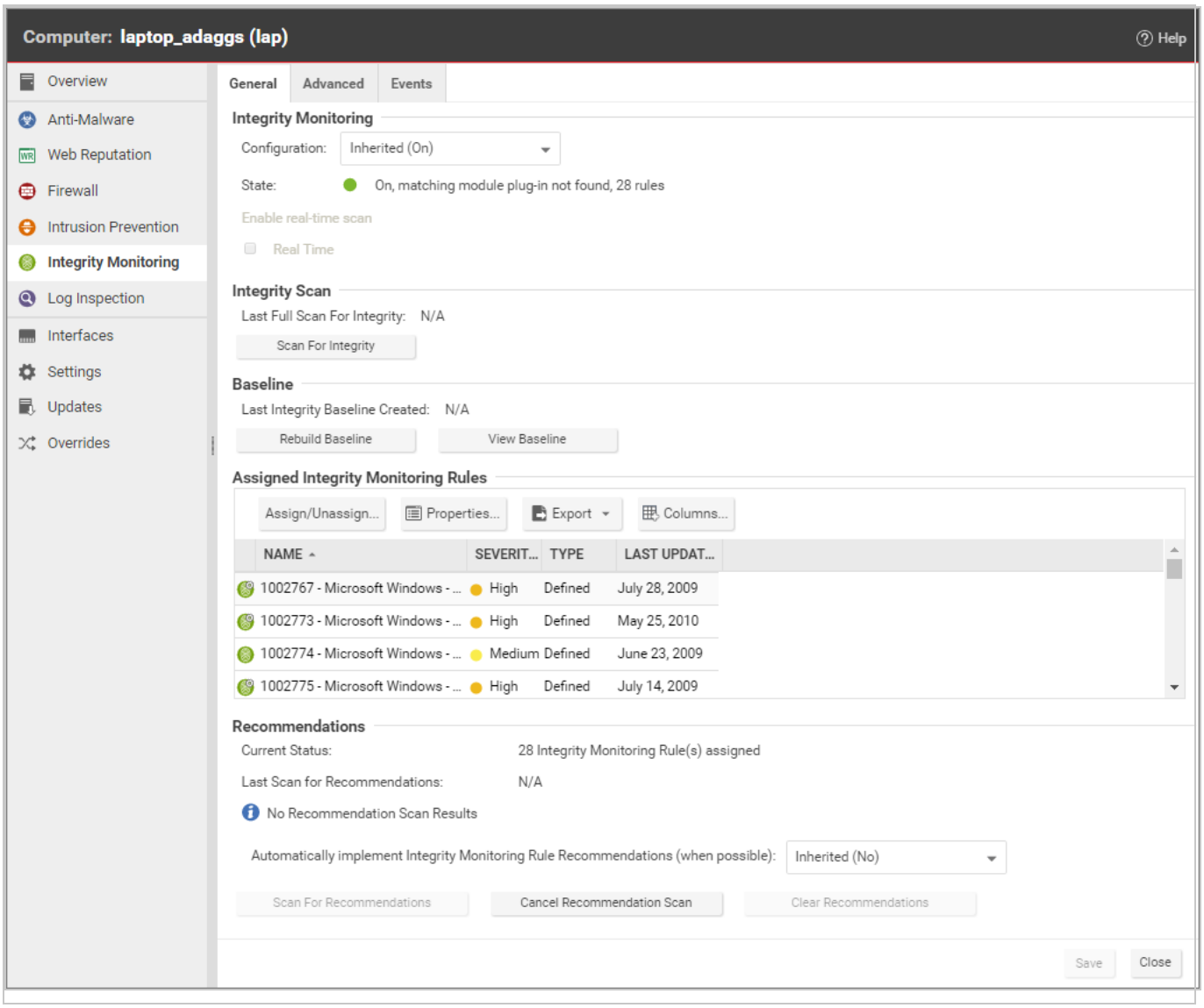
Once you've enabled Integrity Monitoring, you can also learn more about:

- "When Integrity Monitoring scans are performed" on page 454
- "Integrity Monitoring scan performance settings" on page 455
- "Integrity Monitoring event tagging" on page 456

The following is a typical procedure for enabling Integrity Monitoring:

Turn on 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 the Configuration to "On" or "Inherited (On)" and then click **Save**.



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.

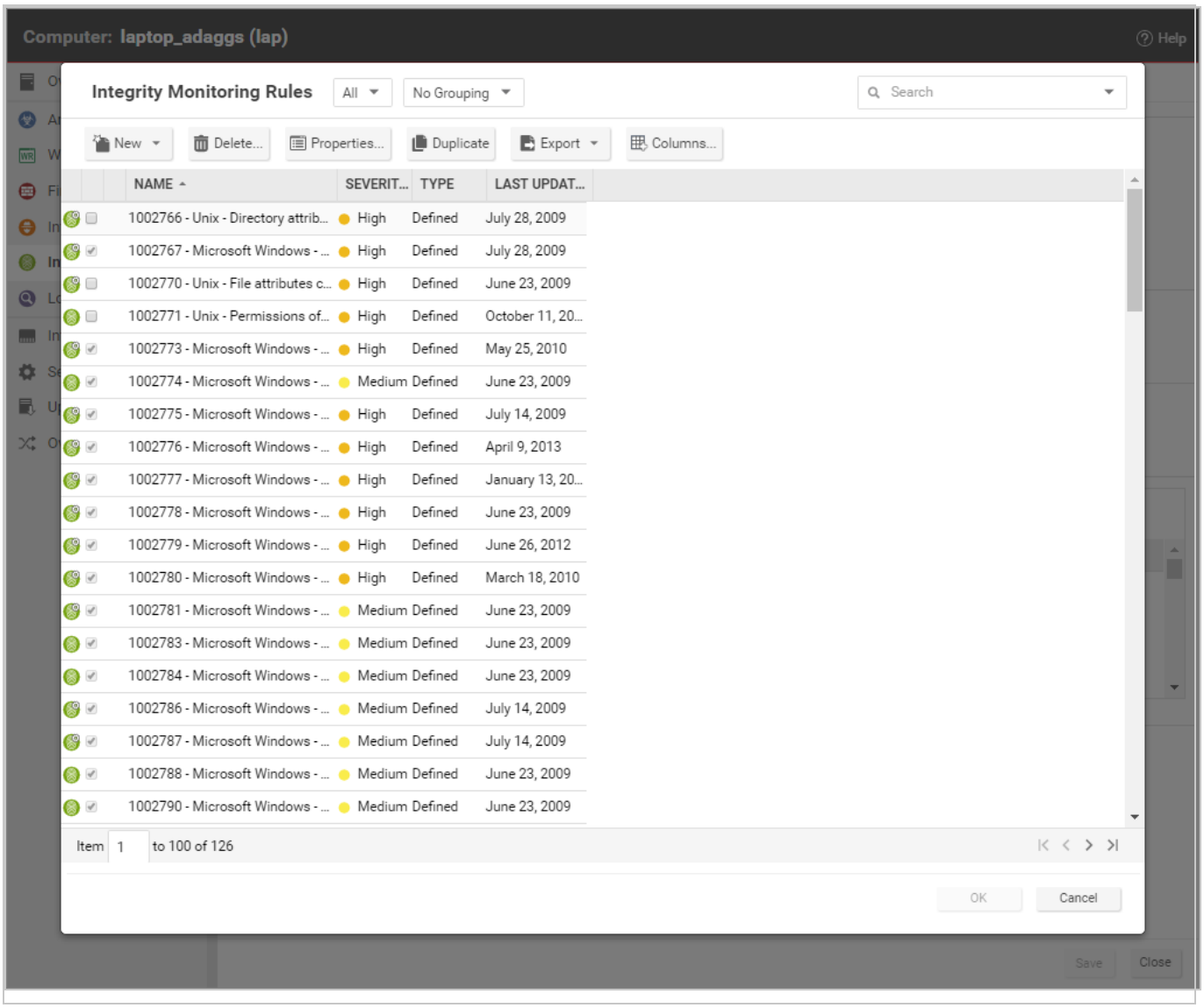
Recommended Integrity Monitoring rules may result in too many monitored entities and attributes. The best practice is to decide what is critical and should be monitored, then create custom rules or tune the predefined rules. Pay extra attention to rules that monitor frequently-changed properties such 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, clear the **Allow Real Time Monitoring** checkbox.

Apply the Integrity Monitoring rules

As described above, 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 will display a window showing all available Integrity Monitoring Rules, from which you can select or deselect rules.



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 will be 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 460.

Tip: 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 that an Integrity Scan's results will be compared against. 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**.

Tip: It's a best practice 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're 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`.

   If you're 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.

[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. Modify the above 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.

When Integrity Monitoring scans are performed

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 will not be tracked; only the last change will be 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 991.
- **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-time scans, go to the **Computer or Policy Editor**[3] **> Integrity Monitoring > General** and select **Real Time**. With Deep Security Agent 11.0 or higher on 64-bit Linux platforms and with Deep Security Agent 11.2 or higher on 64-bit Windows servers, the real-time scan

---

[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] 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).

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 90.

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 will only monitor 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**[1] and go to **Integrity Monitoring** > **Advanced**.

Change the content hash algorithm

You can select the hash algorithm(s) that will 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

[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).

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.

For more information on event tagging, see "Apply tags to identify and group events" on page 573.

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 449.

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 459 section.

To create a new Integrity Monitoring rule, you need to:

1. "Add a new rule" below.
2. "Enter Integrity Monitoring rule information " below.
3. "Select a rule template and define rule attributes" below.

When you're done with your rule, you can also learn how to

- "Configure rule events and alerts" on page 459
- "See policies and computers a rule is assigned to" on page 460
- "Export a rule" on page 460
- "Delete a rule" on page 460

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 492 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 476 documentation.

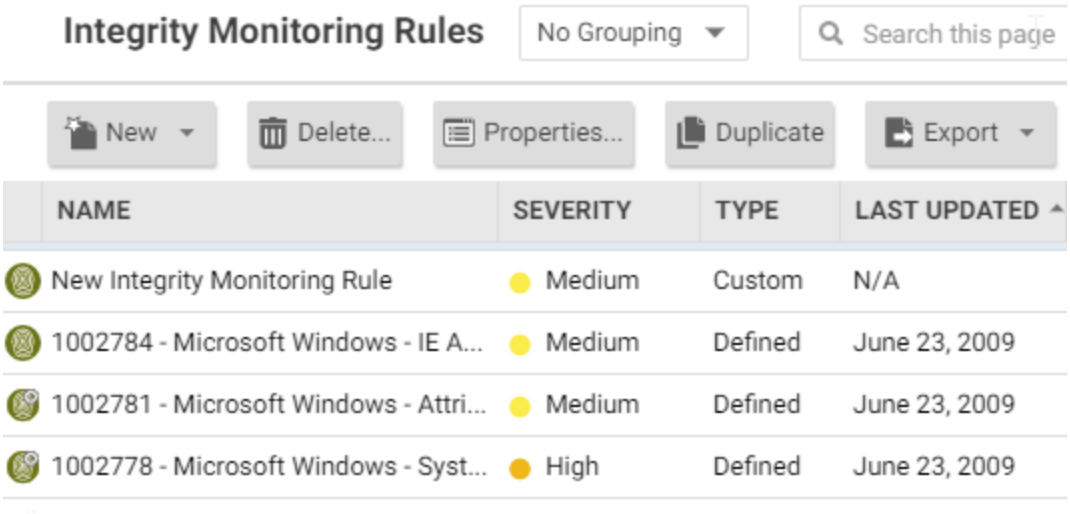
Custom (XML) template

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 460.

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 ( ).



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 456.

To create a new custom Integrity Monitoring rule, start with the procedure in "Create an Integrity Monitoring rule" on page 456 (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 474: rules will scan the integrity of directories
- "FileSet" on page 476: rules will scan the integrity of files
- "GroupSet" on page 481: rules will scan the integrity of groups
- "InstalledSoftwareSet" on page 482: rules will scan the integrity of installed software
- "PortSet" on page 484: rules will scan the integrity of listening ports
- "ProcessSet" on page 488: rules will scan the integrity of processes
- "RegistryKeySet" on page 491: rules will scan registry keys
- "RegistryValueSet" on page 492: rules will scan registry values
- "ServiceSet" on page 495: rules will scan the integrity of services
- "UserSet" on page 497: rules will scan the integrity of users
- "WQLSet" on page 501: 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 461 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 461.)

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 461.
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.

---

[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 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 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 449.

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. 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	No	false	true, false

Attribute	Description	Required	Default Value	Allowed Values
	real time.			
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 460 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 449.

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, 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. 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.

- **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:** (DSA 7.5+) contains the value "true" if the size of the file stays the same or increases between scans, 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:** (DSA 7.5+) contains the value "true" if the size of the file stays the same or decreases between scans, 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**
- **Sha256**
- **Md5** (deprecated)
- **Contents**

---

[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 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 460 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 449.

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 460 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 449.

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 460 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 449.

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 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".
- **Process:** (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.
- **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 460 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 449.

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 460 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 449.

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: HKEY_CLASSES_ROOT (or HKCR), HKEY_LOCAL_MACHINE (or HKLM), HKEY_USERS (or HKU), 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 460 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 449.

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.	Yes	N/A	String values resolving to

Attribute	Description	Required	Default Value	Allowed Values
	The base must begin with one of the registry branch names: HKEY_CLASSES_ROOT (or HKCR), HKEY_LOCAL_MACHINE (or HKLM), HKEY_USERS (or HKU), HKEY_CURRENT_CONFIG (or HKCC)			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 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
```

[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 "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 460 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 449.

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 460 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 449.

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 460 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 449.

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. 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. 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 At present this is only required/supported for group policy queries, and "RsopLoggingModeProvider" is the only supported value. Group policy queries are special since it's recommended that the

Attribute	Description	Required	Default Value	Allowed Values
				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". 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 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,Me
diaType,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,Me
diaType,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,Fi
leType,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,FileT
ype,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\\Sys
tem\\LegalNoticeText",precedence=1
 \\TEST-DESK\root\cimv2:BRCM_NetworkAdapter.DeviceID="8"
```

Include Exclude

See "About the Integrity Monitoring rules language" on page 460 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 90.

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 510.

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 511.

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 509
5. "Configure log inspection event forwarding and storage" on page 510

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**.

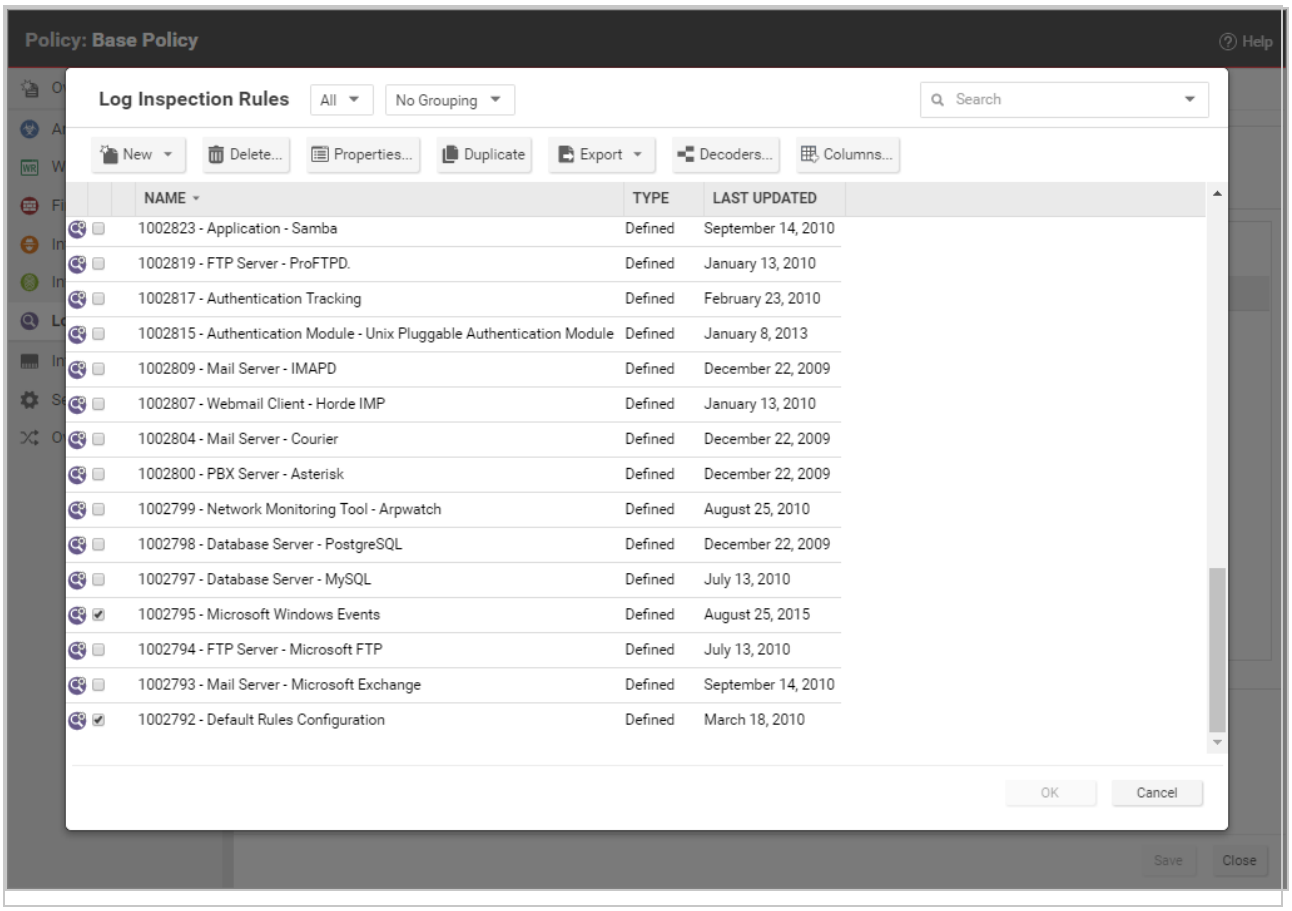
4. In the **Recommendations** section, click **Scan For Recommendations**. Some log inspection rules written by Trend Micro require local configuration to function properly. If you assign one of these rules to your computers or one of these rules gets assigned automatically, an alert will be raised to notify you that configuration is required.

For more information about recommendation scans, see "Manage and run recommendation scans" on page 221.

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**.



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 533.
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 511.

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 784.

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 583.) 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.

Log Inspection Rules issued by Trend Micro are not editable (although you can duplicate them and then edit them.)

Note: Log Inspection Rules that are assigned to one or more computers or that 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 513
- "Subrules" on page 515
- "Real world examples" on page 522
- "Log Inspection rule severity levels and their recommended use" on page 531
- "strftime() conversion specifiers " on page 532
- "Examine a Log Inspection rule" on page 533

For an overview of the Log Inspection module, see "About Log Inspection" on page 506.

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.

   > **Note:** Any changes you make in the Custom (XML) view will be 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 will pre-populate 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 will be 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 will cause 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.

Note: 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 any).

1. On the **Files** tab, type the full path to the file(s) you want your rule to monitor and specify the type of file it is.
2. 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.

   Note: 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.
3. 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.
4. 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 we have indicated that our group contains the syslog and sshd rules:

```
<group name="syslog,sshd,">
</group>
```

Note: 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 sub-rule to this one.

Note: 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 essentially a single long Log Inspection rule. Some group definitions are common to all Log Inspection rules written 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 along with any other Trend Micro rules. (If you select a rule for assignment and haven't also selected the "Default Rules Configuration" rule, a notice will appear 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, we have created two rules, 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>
```

Note: 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 web_scan recon	Connection attempt Web scan Generic scan
Authentication Control	authentication_success authentication_failed invalid_login login_denied authentication_failures adduser account_changed	Success Failure Invalid Login Denied Multiple Failures User account added User Account changed or removed
Attack/Misuse	automatic_attack exploit_attempt invalid_access spam multiple_spam sql_injection attack virus	Worm (nontargeted attack) Exploit pattern Invalid access Spam Multiple spam messages SQL injection Generic attack Virus detected
Access Control	access_denied access_allowed unknown_resource firewall_drop multiple_drops client_misconfig client_error	Access denied Access allowed Access to nonexistent resource Firewall drop Multiple firewall drops Client misconfiguration Client error
Network Control	new_host ip_spoof	New computer detected Possible ARP spoofing
System Monitor	service_start system_error system_shutdown logs_cleared invalid_request promisc policy_changed config_changed low_diskspace time_changed	Service start System error Shutdown Logs cleared Invalid request Interface switched to promiscuous mode Policy changed Configuration changed Low disk space Time changed

Note: If event auto-tagging is enabled, the event will be 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. So, for example, "login_denied" would appear as "Login Denied". Custom rules will be listed by their group name as it appears in the rule.

Description

Include a **<description></description>** tag. The description text will appear 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>
```

Note: 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>
```

Note: 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 will have broken up the log into sections. See "Decoders" on page 513 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.

Note: 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 will ignore the children of that parent.

Note: 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 on.

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.

Tag	Description	Notes
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 hh:mm - hh:mm or 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, etc.)	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 will be 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 no_email_alert 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>
```

Real world 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.

In this section we will walk through the creation of 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 our custom 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 functional features which we will create Log Inspection rules for:

- 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)

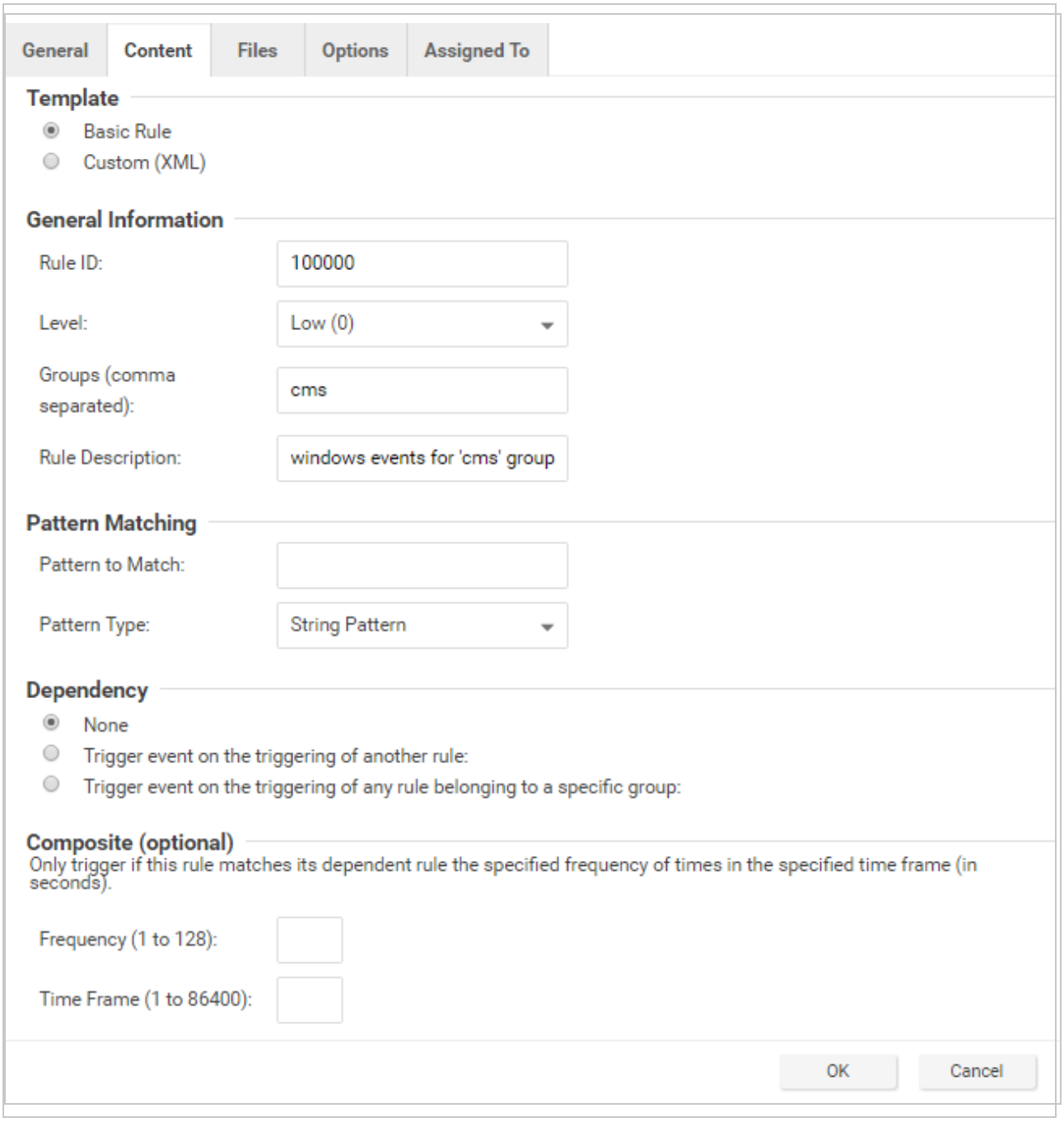
- Application Audit (Type: Information)
  - Content
    - New content added (Event: 450 to 459)
    - Existing content modified (Event: 460 to 469)
    - Existing content deleted (Event: 470 to 479)
  - Administration
    - User
      - New User created (Event: 445 to 446)
      - Existing User deleted (Event: 447 to 449)

This structure will provide you with a good basis for rule creation. Now to create a new Log Inspection rule in Deep Security Manager.

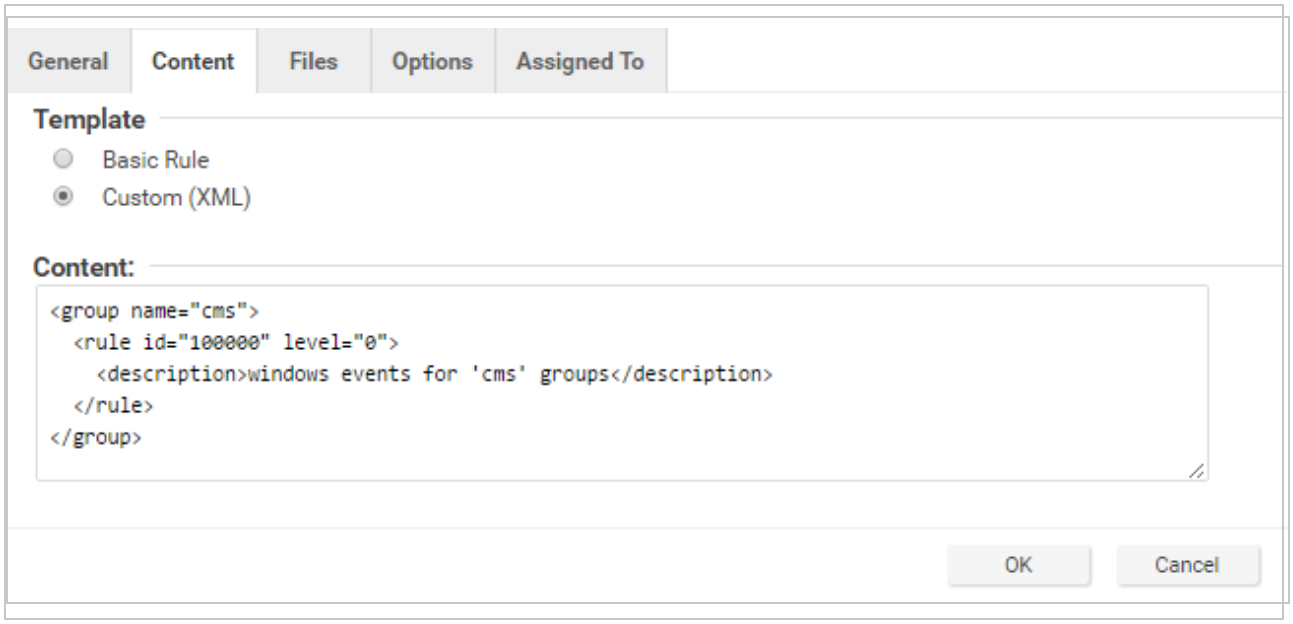
To create the new CMS Log Inspection Rule:

1. In the 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 click the **Content** tab.
3. The quickest way to create a new custom rule is to start with a basic rule template. Select the **Basic Rule** radio button.
4. The **Rule ID** field will be 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".

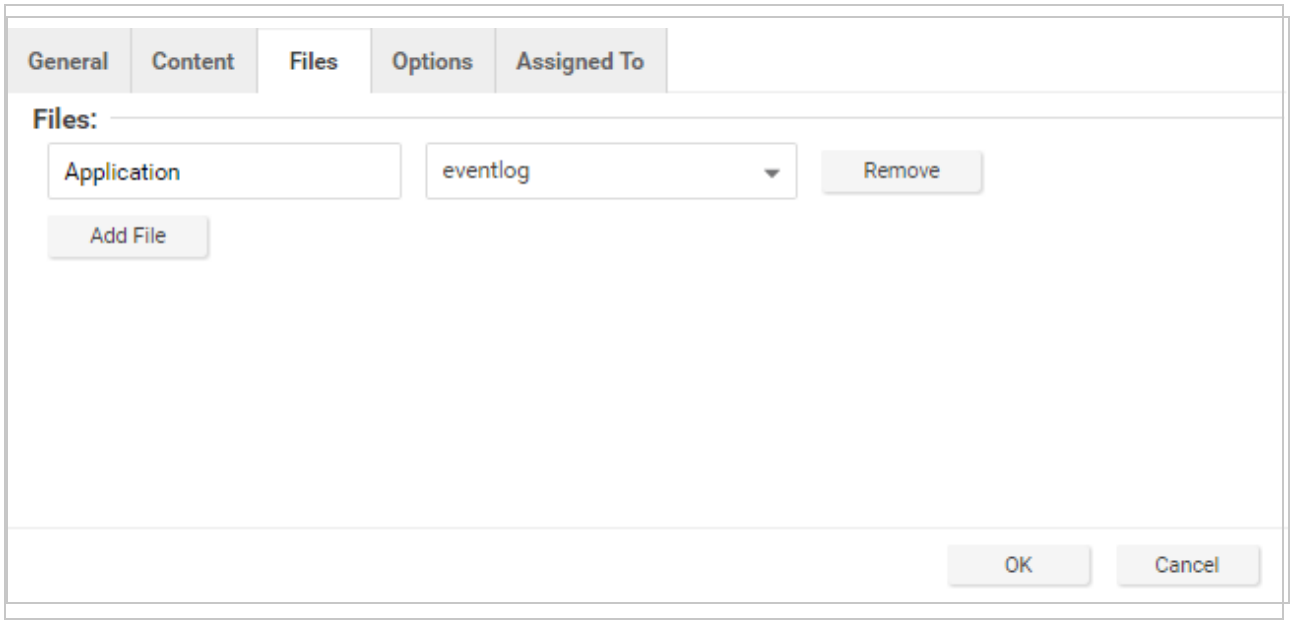
7. Provide a short rule description.



8. Now select the **Custom (XML)** option. The options you selected for your "Basic" rule will be converted to XML.



9. Click the **Files** tab and click the **Add File** button to add any application log files and log types which the rule will be applied to. In this case, "Application", and "eventlog" as the file type.



Note: **Eventlog** is a unique file type in Deep Security because the location and filename of the log files don't 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 will require the log file's location and filename. (*C/C++ strftime()* conversion specifiers are available for matching on filenames. See the table below 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, we can begin adding new rules to the group based on the log groupings identified previously. We will 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. Now we build up 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. Now we add any composite or correlation rules using the established rules. The follow example shows a high severity composite rule that is applied to instances where the repeated login failures have occurred 5 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. Finally, open the newly created rule, click 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, etc.
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, etc. 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	Include attempts to login as an unknown user or from an invalid source. The message might have security relevance especially if repeated. They also

Level	Description	Notes
	source	include errors regarding the **admin** or **root** account.
Level 10	Multiple user generated errors	Include multiple bad passwords, multiple failed logins, etc. 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-importance event	Include error or warning messages from the system, kernel, etc. 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 (e.g., Thu)
%A	Full weekday name (e.g., Thursday)
%b	Abbreviated month name (e.g., Aug)
%B	Full month name (e.g., August)
%c	Date and time representation (e.g., Thu Sep 22 12:23:45 2007)
%d	Day of the month (01 - 31) (e.g., 20)
%H	Hour in 24 h format (00 - 23) (e.g., 13)
%I	Hour in 12 h format (01 - 12) (e.g., 02)
%j	Day of the year (001 - 366) (e.g., 235)
%m	Month as a decimal number (01 - 12) (e.g., 02)
%M	Minute (00 - 59) (e.g., 12)
%p	AM or PM designation (e.g., AM)
%S	Second (00 - 61) (e.g., 55)
%U	Week number with the first Sunday as the first day of week one (00 - 53) (e.g., 52)
%w	Weekday as a decimal number with Sunday as 0 (0 - 6) (e.g., 2)
%W	Week number with the first Monday as the first day of week one (00 - 53) (e.g., 21)
%x	Date representation (e.g., 02/24/79)
%X	Time representation (e.g., 04:12:51)
%y	Year, last two digits (00 - 99) (e.g., 76)
%Y	Year (e.g., 2008)
%Z	Time zone name or abbreviation (e.g., EST)

Specifier	Description
%%	A % sign (e.g., %)

More information can be found at the following websites:

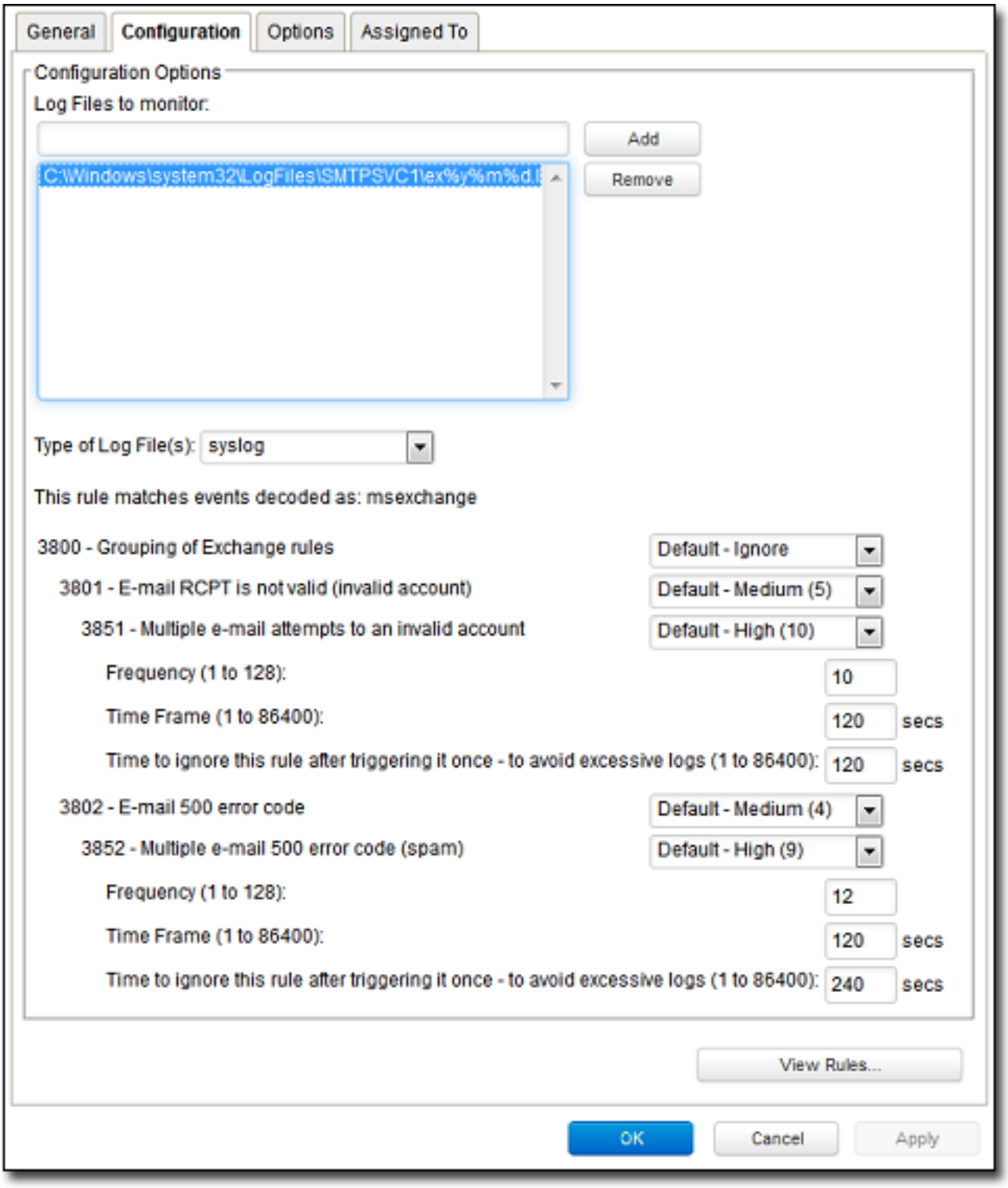
https://www.php.net/manual/en/function.strftime.php
www.cplusplus.com/reference/clibrary/ctime/

Examine a Log Inspection rule

Log Inspection rules are found in the Deep Security Manager at **Policies > Common Objects > Rules > Log Inspection Rules**.

Log Inspection rule structure and the event matching process

This screen shot displays the contents of the **Configuration** tab of the Properties window of the "Microsoft Exchange" Log Inspection rule:



Here is the structure of the rule:

- 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 will apply log events to this structure and see 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 will then be applied to line 3800's sub-rules: 3801 and 3802.

If there is no further match, this "cascade" of matches will stop 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. Sub-rule 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 sub-rule to be applied to the event: sub-rule 3851. Sub-rule 3851 with its three attributes will match 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 sub-rule 3851 to ignore individual events that match sub-rule 3801 for the next 120 seconds. This is useful for reducing "noise".)

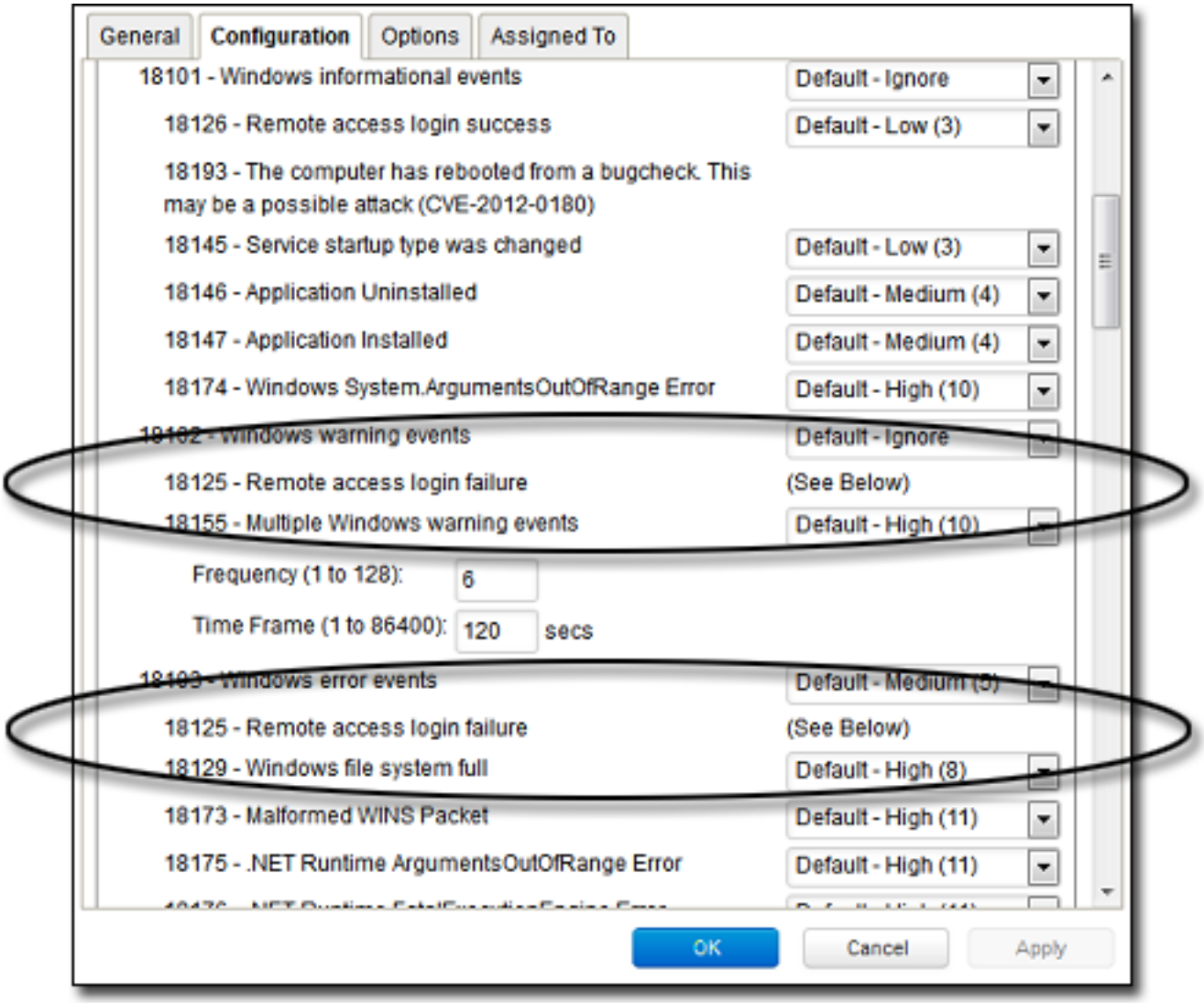
Assuming the parameters of sub-rule 3851 have been matched, a Log Inspection event with Severity "High(9)" is now recorded.

Looking at the Options tab of the Microsoft Exchange Rule, we see that Deep Security Manager will raise an alert if any sub-rules with a severity level of "Medium(4)" have been matched. Since this is the case in our example, the alert will be raised (if "Alert when this rule logs an event" is selected).

Duplicate Sub-rules

Some Log Inspection rules have duplicate sub-rules. To see an example, open the "Microsoft Windows Events" rule and click on the **Configuration** tab. Note that sub-rule 18125 (Remote access login failure) appears under sub-rules 18102 and 18103. Also note that in both cases sub-rule 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:



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 90.

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 542.

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.

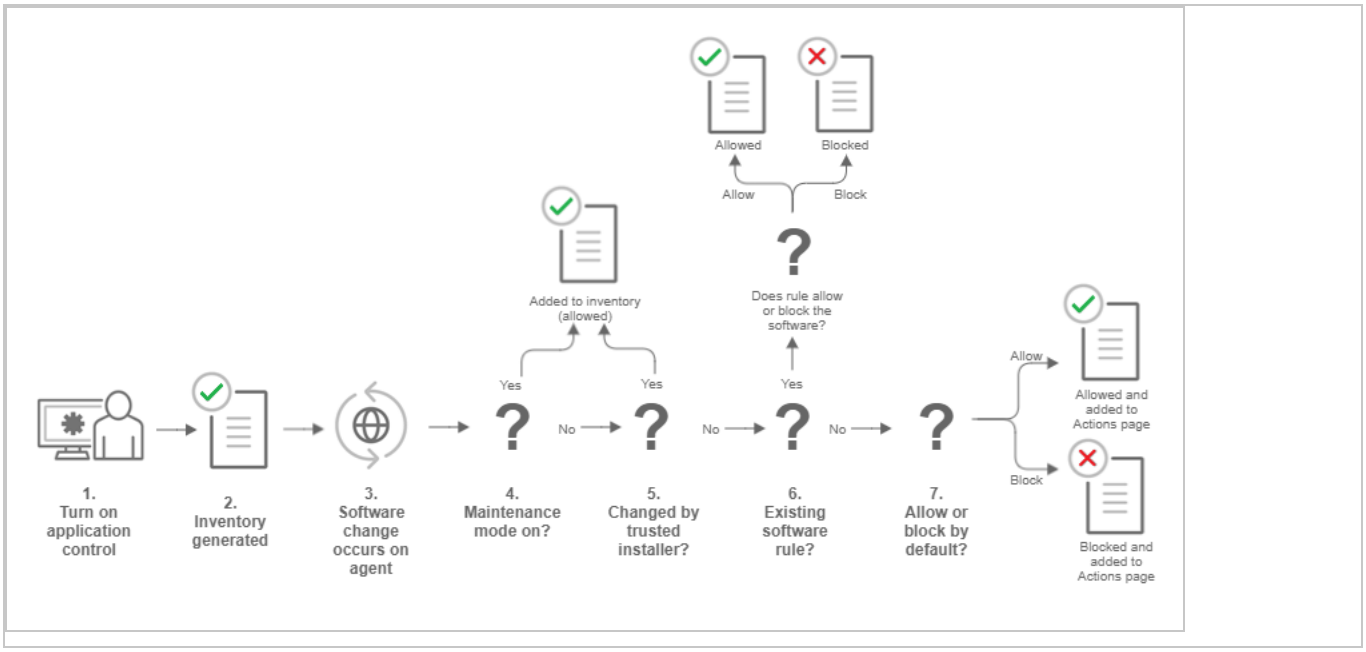
Inventory: Initial list of software that is installed on the computer and allowed to run. Make sure only software that you want to allow is installed on the computer. When you enable application

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 542

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 548.

How does application control work?



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 544).
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 548.
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 542
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.

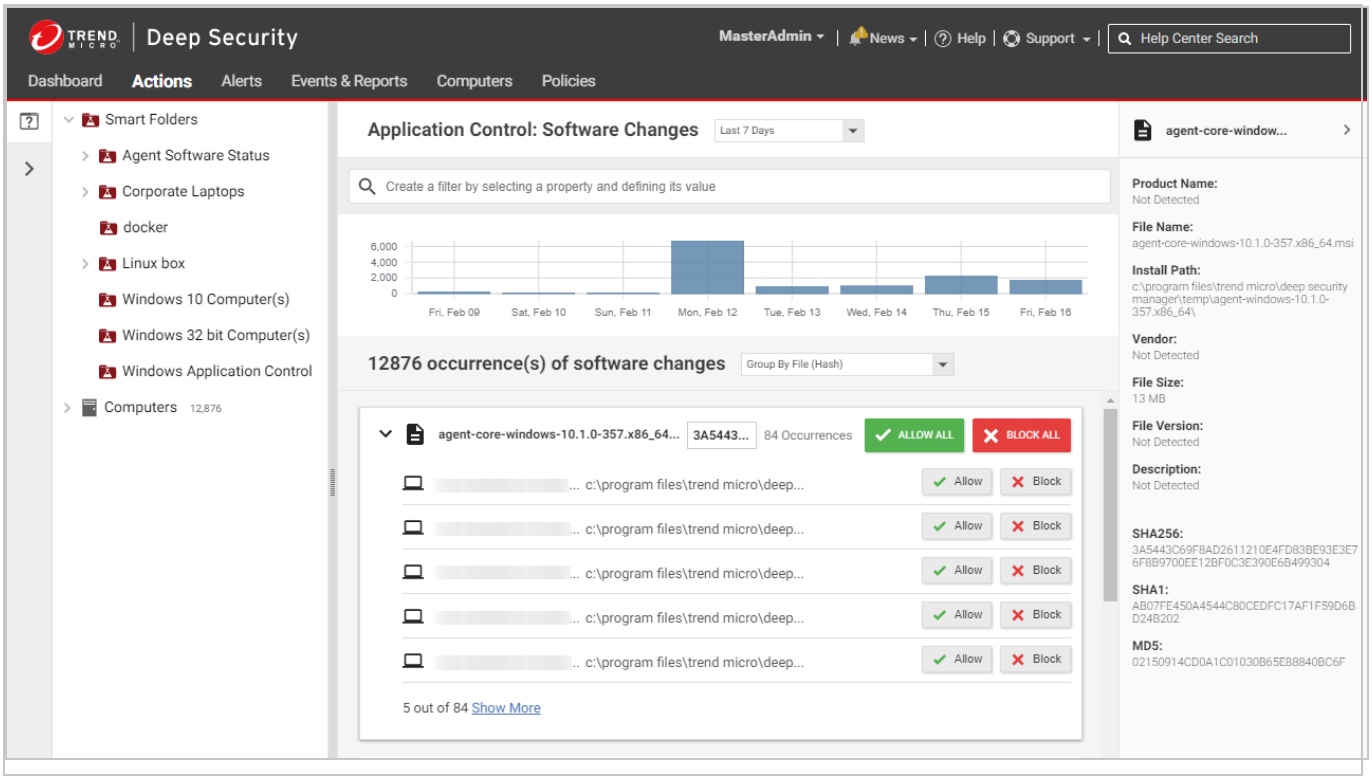
   The unrecognized software appears on the **Application Control - Software Changes** page in Deep Security Manager. On that page, an administrator can click **Allow** or **Block** to create an allow or block rule for that piece of software on a particular computer. An allow or block rule takes precedence over the default action specified in the policy. See "Monitor new and changed software" on page 545.

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)" on the next page
- "Application Control Rulesets" on page 541
- "Security Events" on page 542

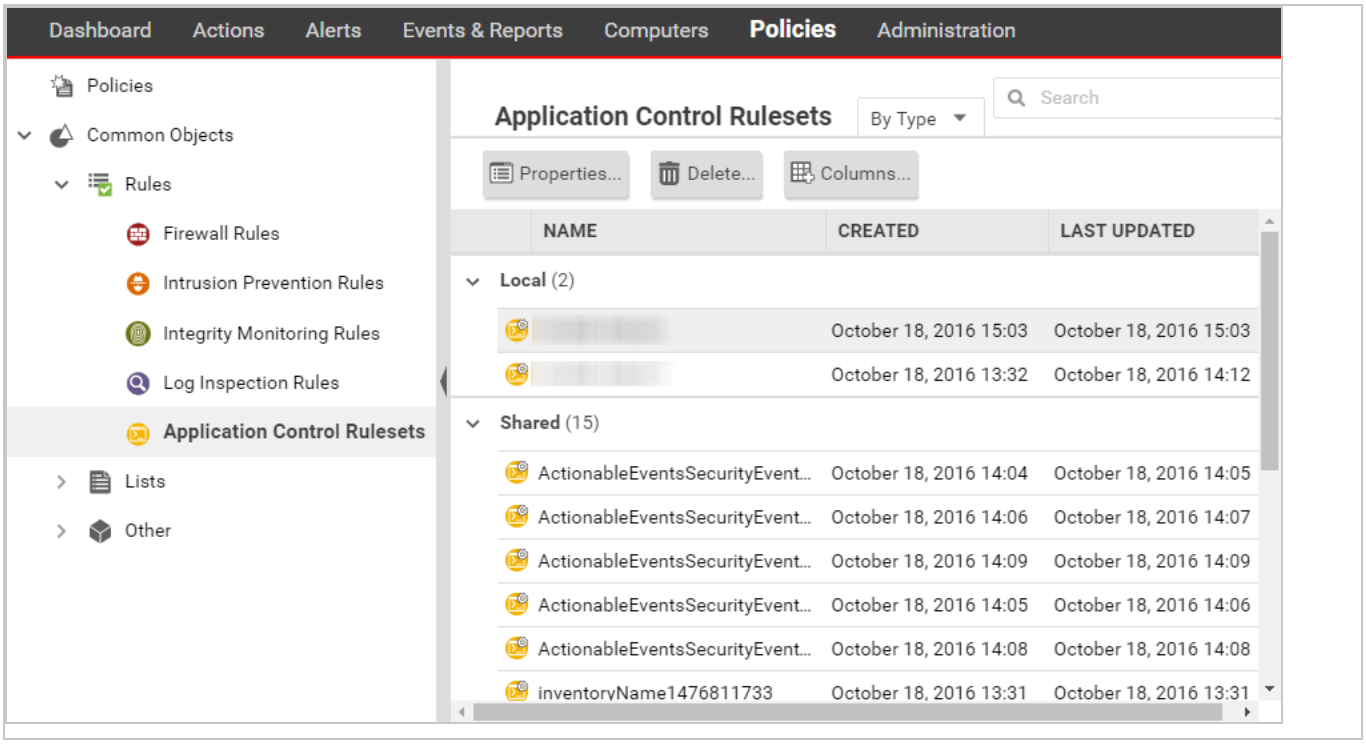
Application Control: Software Changes (Actions)



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.

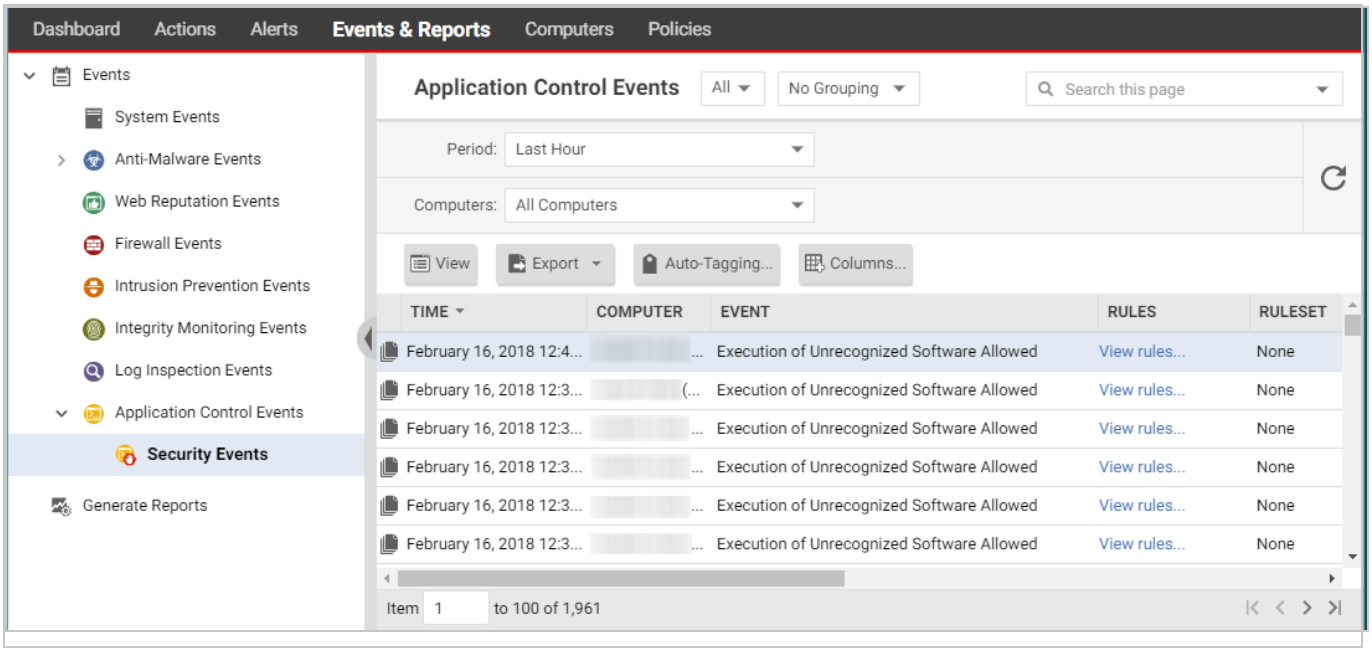
The policy applied to a computer specifies whether it will allow all unrecognized software to run by default, or block all unrecognized software, but no explicit application control rule is created until you click "Allow" or "Block" on the Actions page. When you click Allow or Block, a corresponding rule appears in the ruleset for the computer. The rulesets are displayed on the **Application Control Rulesets** page.

Application Control Rulesets



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



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 537.

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 548

This article also provides "Application Control tips and considerations" on page 549 that you should be aware of when working with Application Control.

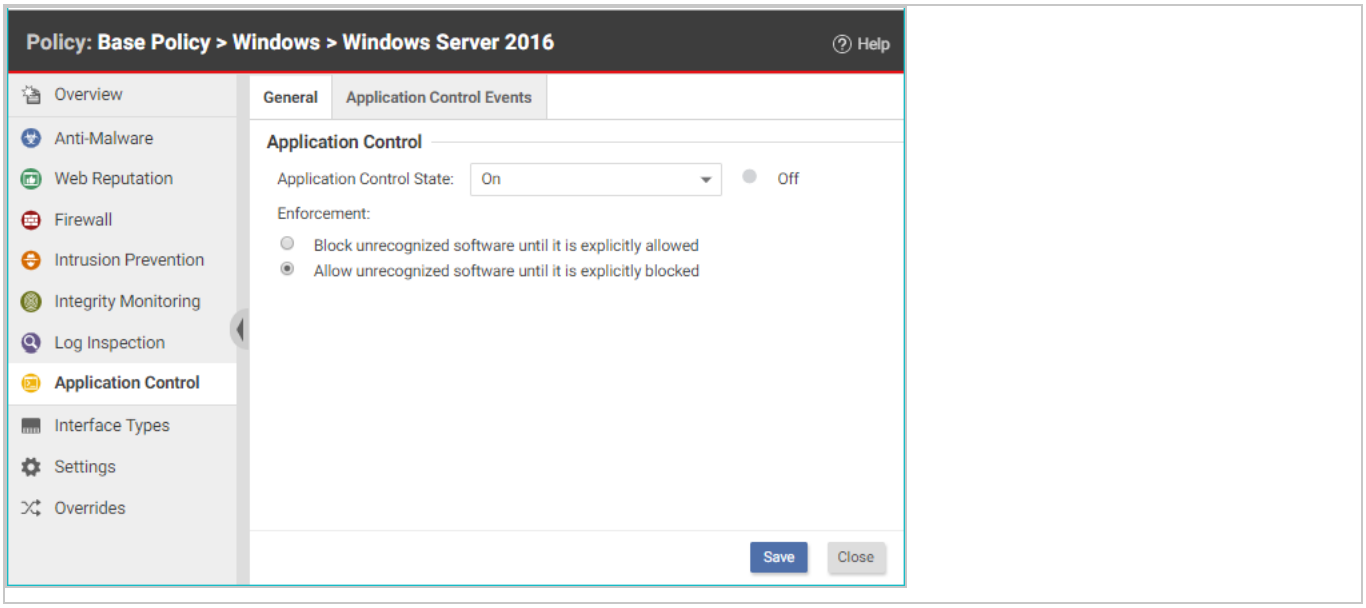
Once you've enabled Application Control, you can also learn how to:

- "View and change Application Control rulesets" on page 554
- "Reset Application Control after too much software change" on page 558
- "Monitor Application Control events" on page 551
- "Use the API to create shared and global rulesets" on page 559

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**.



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.

To check that Application Control is working as expected, follow the instructions in "Verify that Application Control is enabled" on page 549.

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 763

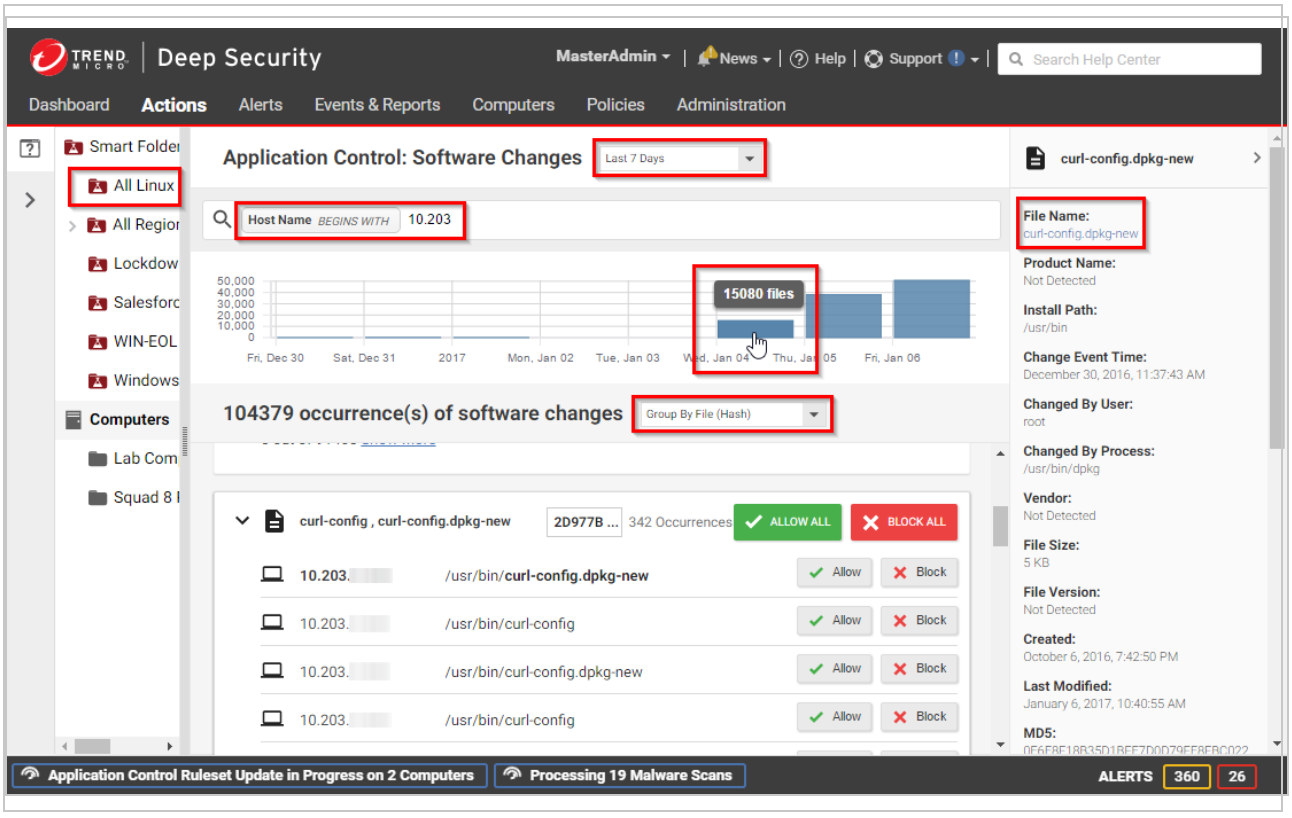
After you initially enable Application Control, you will likely see a lot of software changes on the **Actions** page. This can happen when allowed software creates new executables, renames files, or relocates files through the normal course of operation. As you add rules to tune Application Control, 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.



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 922).

> **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 551.

- 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

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

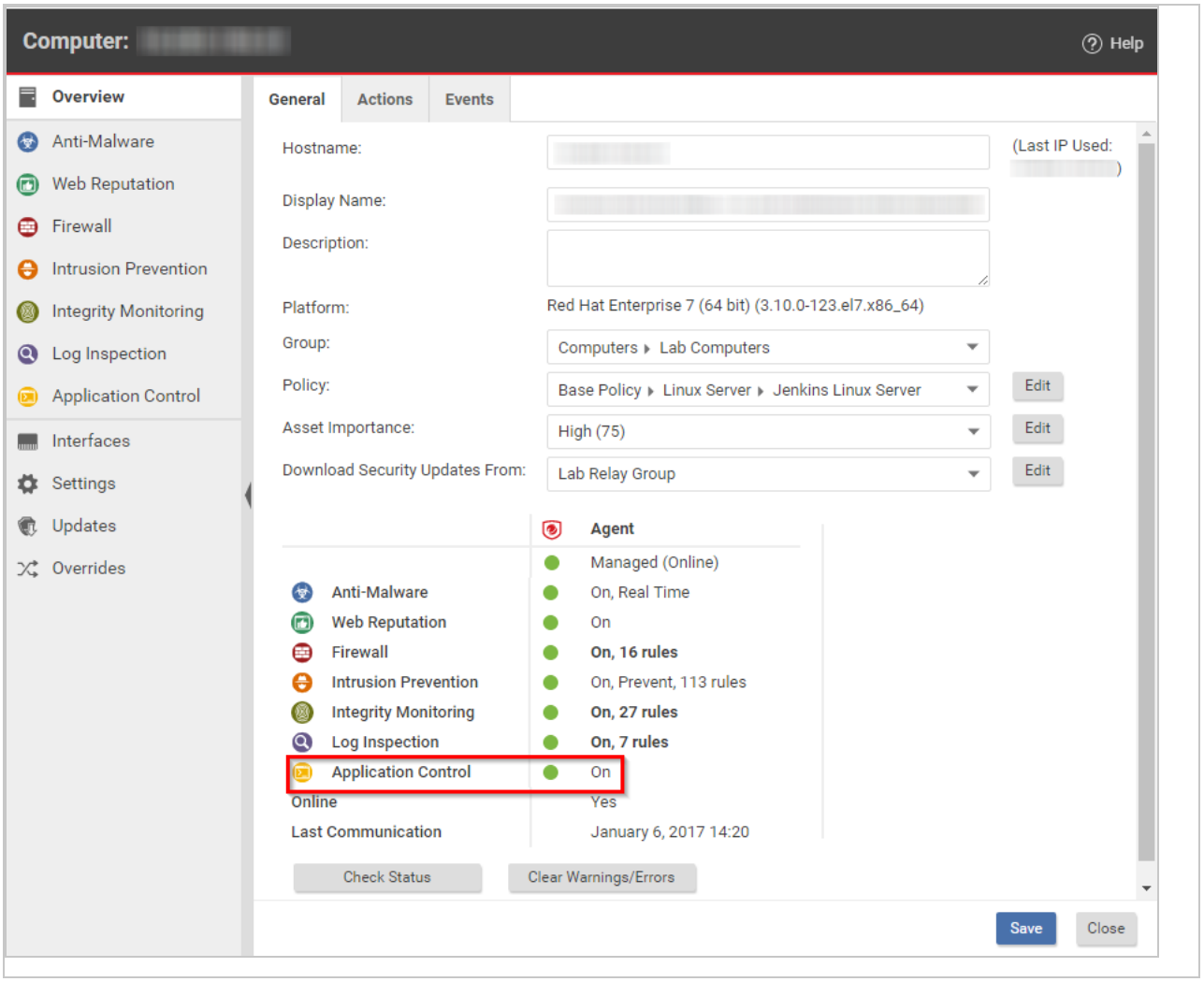
- For better performance with Application Control, use Deep Security anti-malware instead of Windows Defender. See "Disable Windows Defender after installing Deep Security anti-malware on Windows Server 2016" on page 339.
- If you create a block rule for a batch file or PowerShell script, you will not 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 542)
- 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 699.
- 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 558.

Verify that Application Control is enabled

For an overview of Application Control, see "About Application Control" on page 537. For initial configuration instructions, see "Set up Application Control" on page 543.

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 the next page.)



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 545). 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 537. For initial configuration instructions, see "Set up Application Control" on page 543.

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" below
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 553

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 566.

> **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 717 and "Application Control events" on page 763.

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 717.
- **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 763.

Interpret aggregated security events

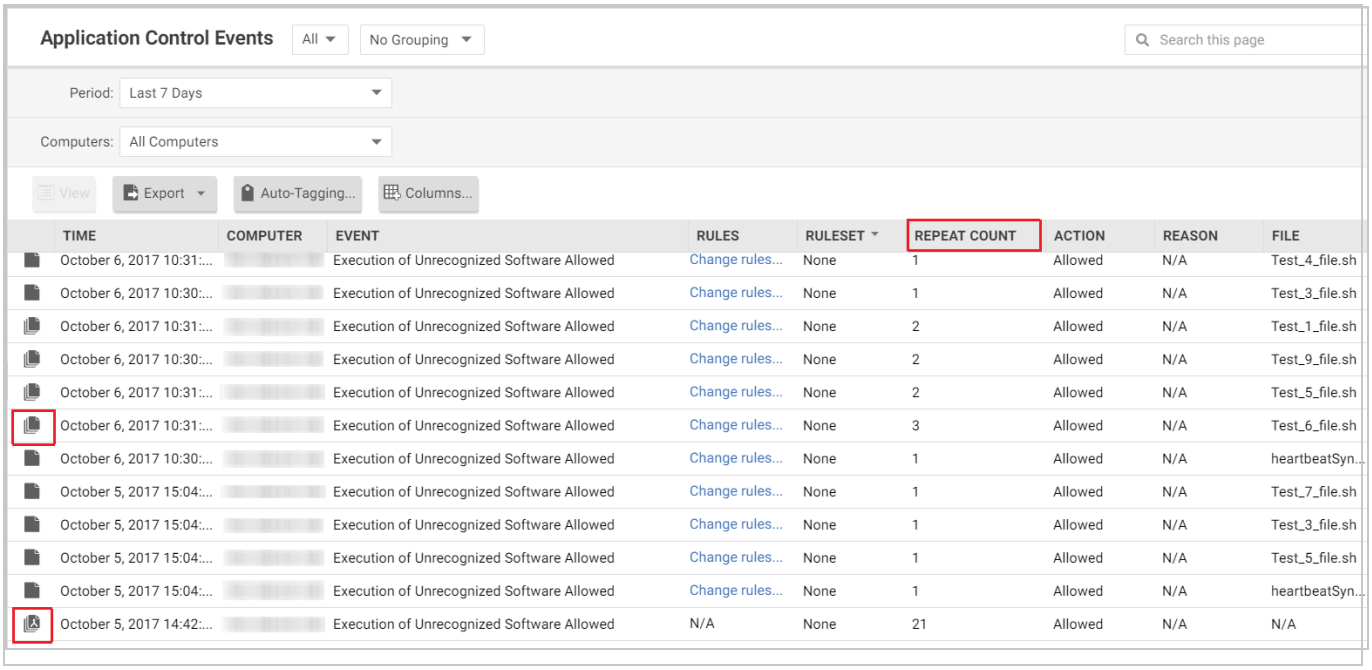
When an agent heartbeat includes several instances of the same security event, Deep Security aggregates the events in the Security Events log. Event aggregation reduces the number of items in the log, making it easier to find important events:

- 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.

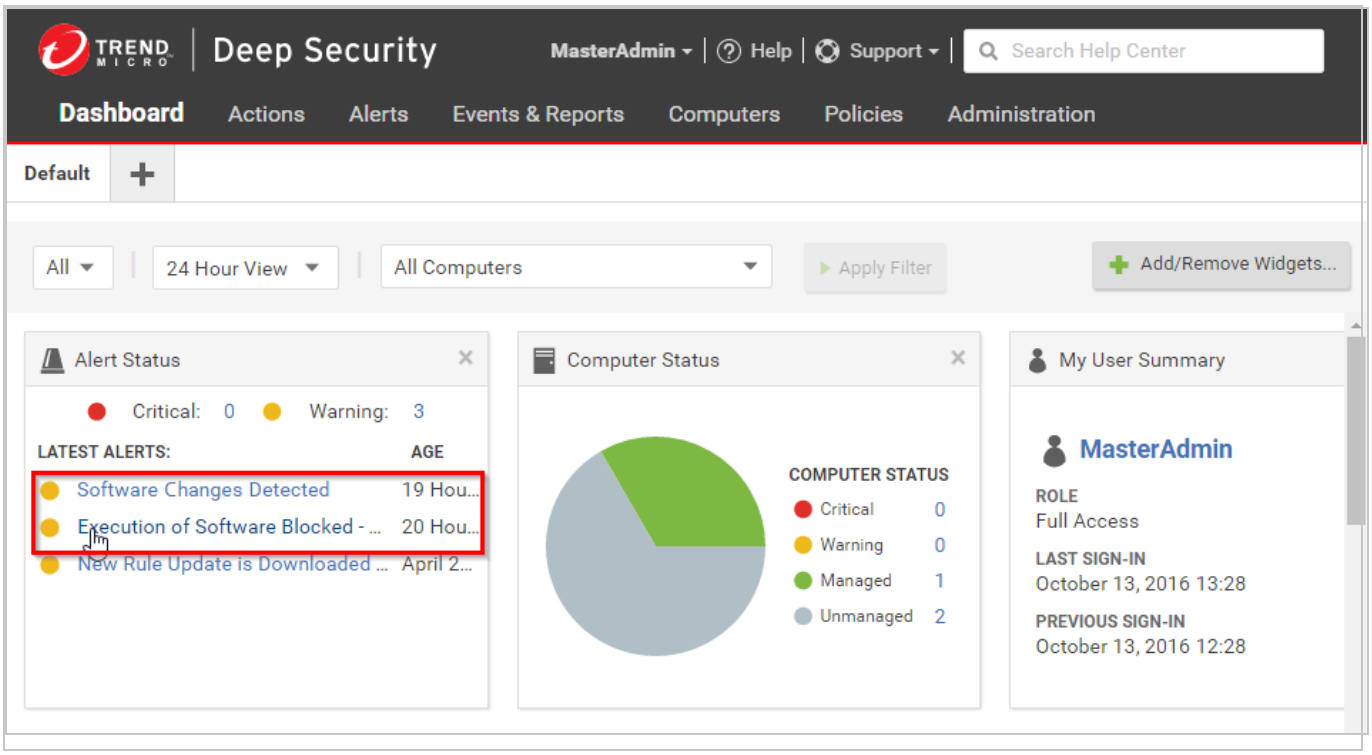
In the log, aggregated events use special icons, and the **Repeat Count** column indicates the number of events that are aggregated.



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 689.

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.



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 559). In Deep Security Manager, a computer's ruleset appears empty until you create some allow/block rules for the computer.

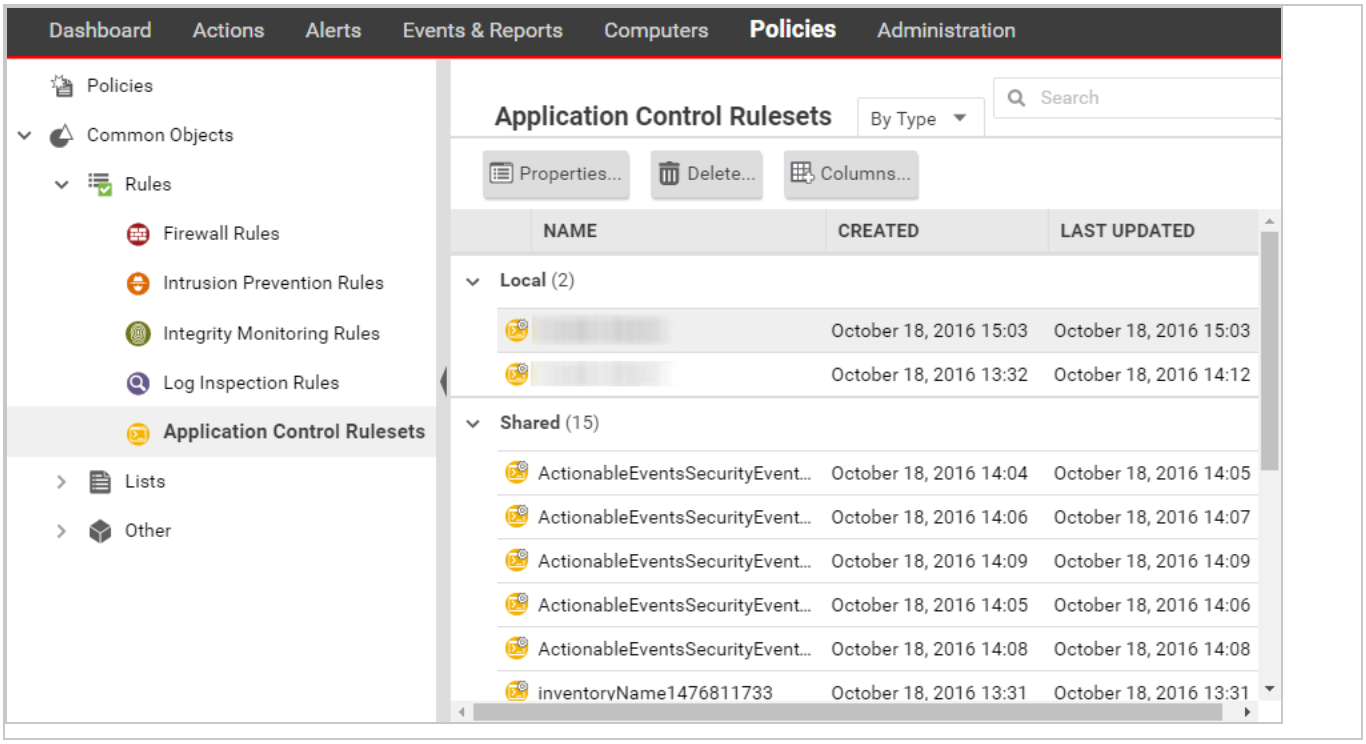
- "Change the action for an Application Control rule" on page 556 if a software file should no longer be allowed/blocked.
- "Delete an individual Application Control rule" on page 557 if the software has been removed and isn't likely to return.

- "Delete an Application Control ruleset" on page 558 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.

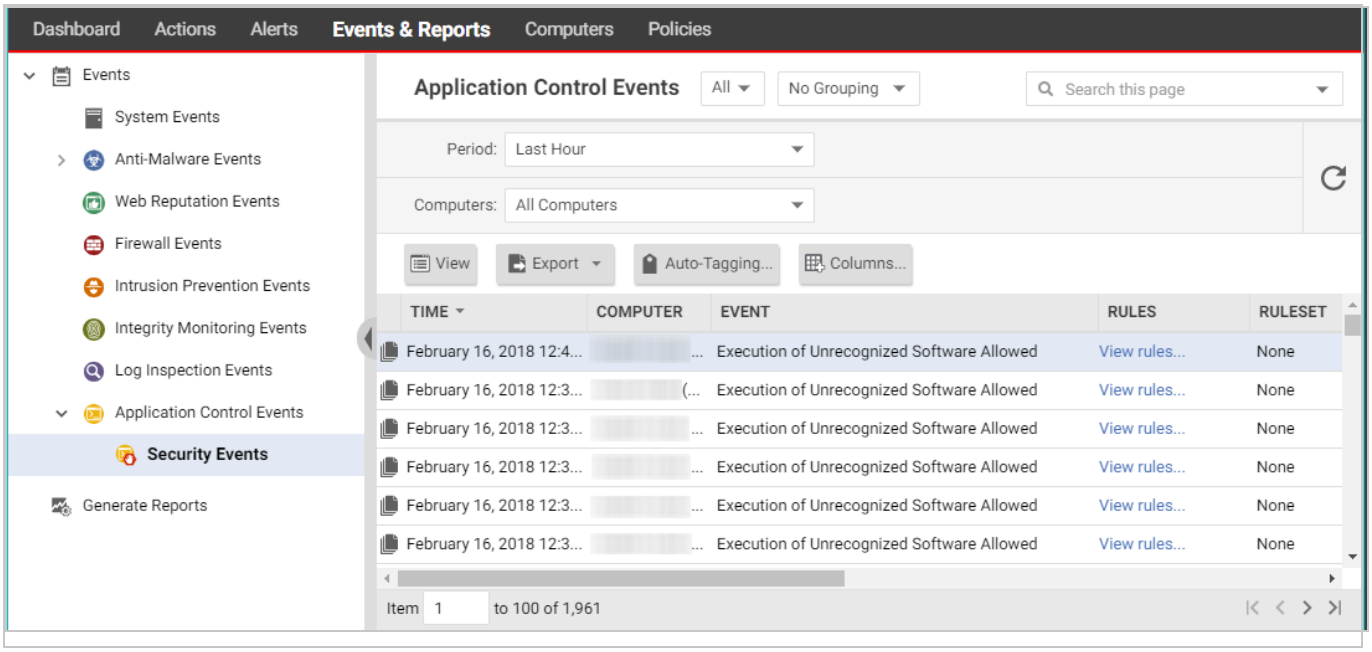
View Application Control rulesets

To view the list of Application Control rulesets, go to **Policies > Common Objects > Rules > Application Control Rulesets**.



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" on the next page.)

Security Events



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 763.

For each event (except aggregated events), you can click **View rules** to change the rule from Allow to Block or vice versa.

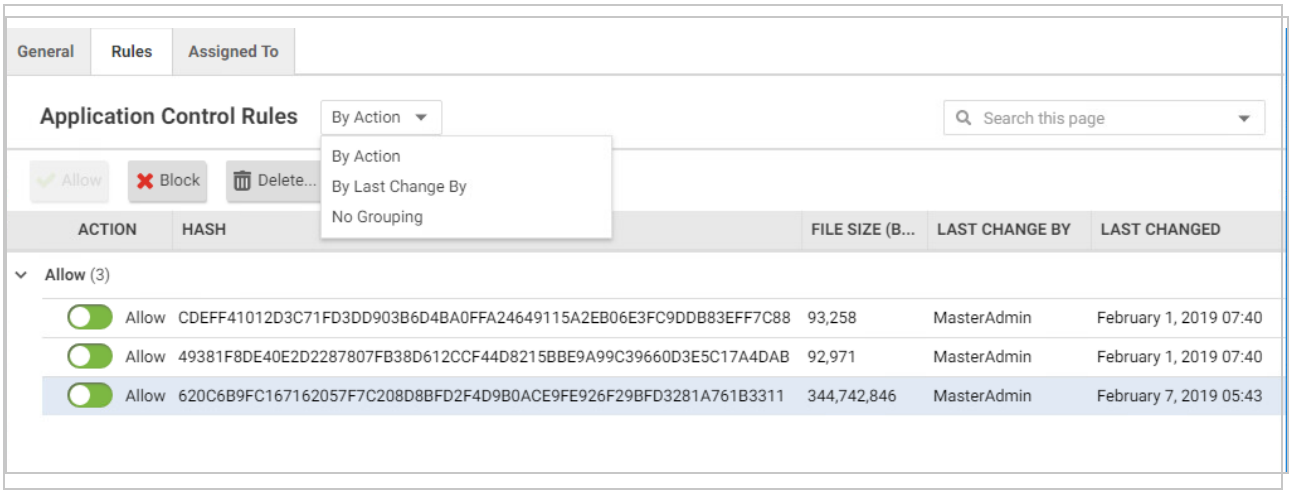
Deep Security Agent 10.2 or later includes event aggregation logic to reduce the volume of logs when the same event occurs repeatedly. (See "Interpret aggregated security events" on page 552.)

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.



   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**.

Reset Application Control after too much software change

For an overview of Application Control, see "About Application Control" on page 537.

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 548).
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.

Use the API to create shared and global rulesets

For an overview of Application Control, see "About Application Control" on page 537. For initial configuration instructions, see "Set up Application Control" on page 543.

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

[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).

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, it can only contain hash-based rules (rules that compare only a file's hash and size). If you created a shared ruleset using an earlier version of Deep Security, 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 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

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 554.

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.

   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] 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 **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.

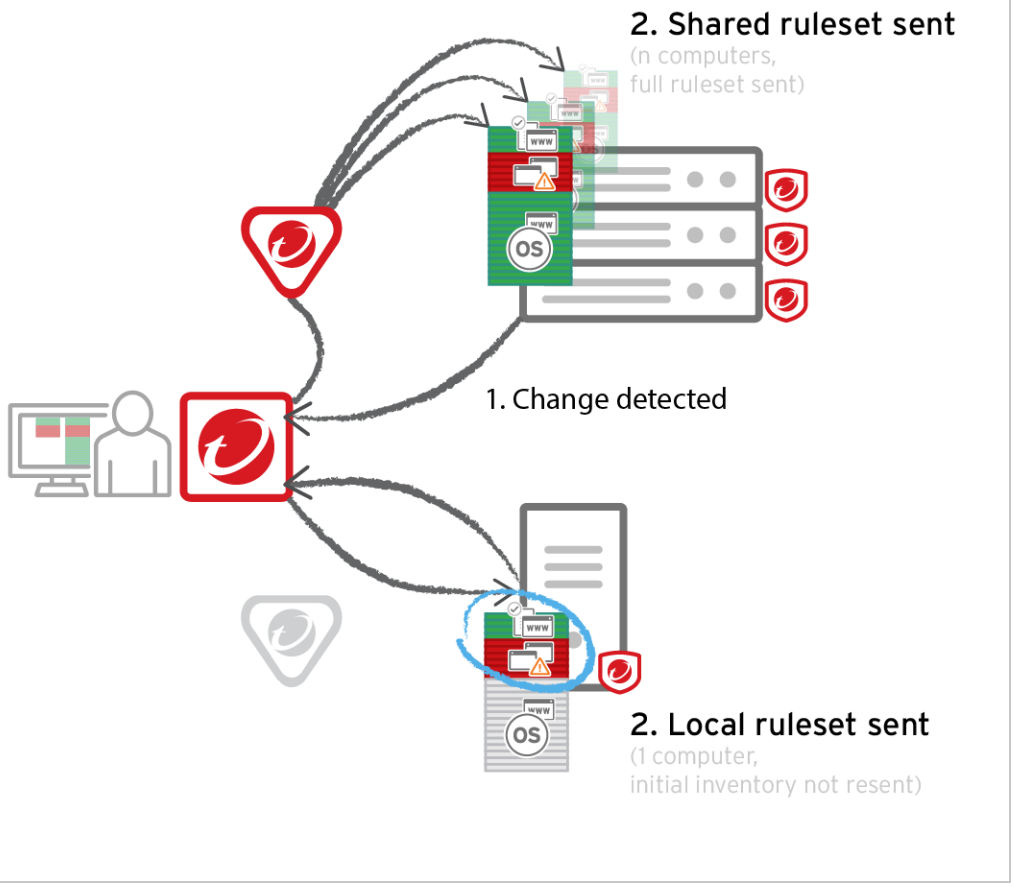
Using Deep Security Relays can solve this problem. (For information on configuring relays, see "Deploy additional relays" on page 816.)

Steps vary depending whether or not you have a multi-tenant deployment.

Single tenant deployments

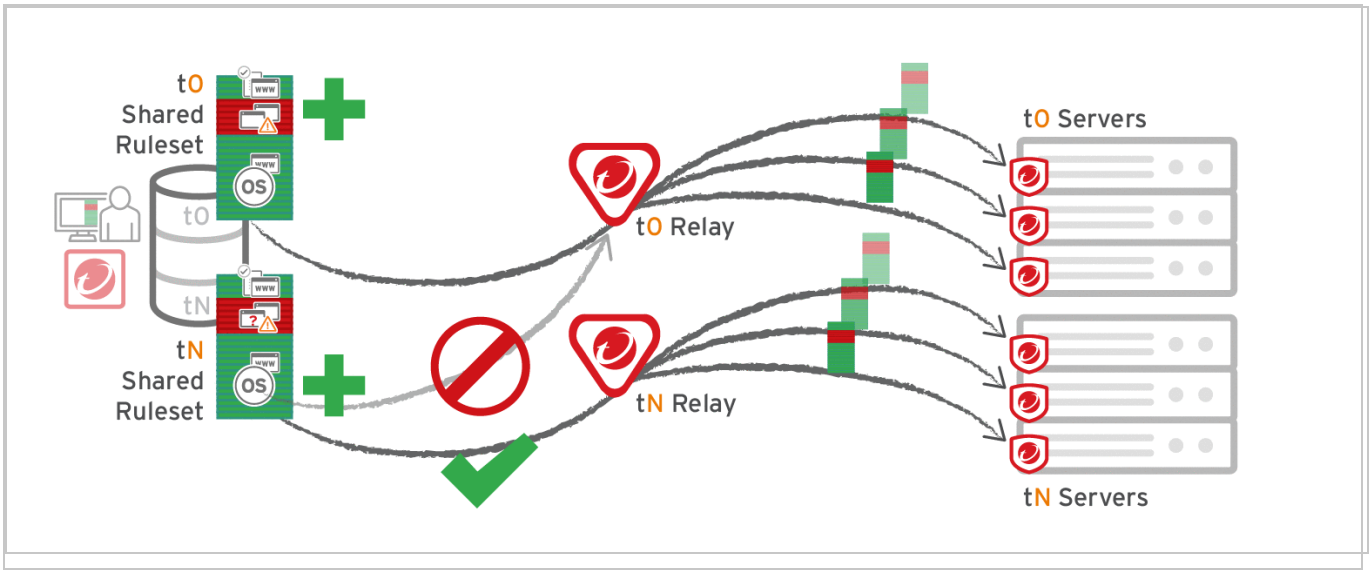
Go to **Administration > System Settings > Advanced** and then select **Serve Application Control rulesets from relays**.

[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).



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 (including Deep Security as a Service), 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?

As of May 15, 2017, Deep Security as a Service retains security events for 32 days and system events for 13 weeks. Customers requiring a longer event retention period should consider exporting events to an external SIEM. For more information, see "Forward Deep Security events to a Syslog or SIEM server" on page 583.

Event history is retained for:

- Anti-Malware events
- Application Control events
- Firewall events
- Integrity Monitoring events
- Intrusion Prevention events
- Log Inspection events
- Web Reputation events
- System events

[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).

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 717.

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 765
- "View and restore identified malware" on page 350
- "Application Control events" on page 763
- "Firewall events" on page 767
- "Integrity monitoring events" on page 780
- "Intrusion prevention events" on page 776
- "Log inspection events" on page 784
- "Web reputation events" on page 785

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 767.

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.

---

[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).

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.
- **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.

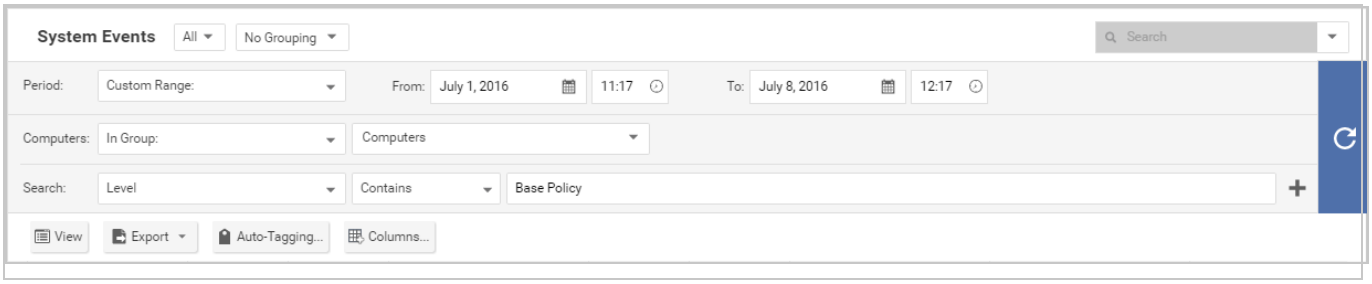
The **Tags** tab displays tags that have been attached to this event. For more information on event tagging, see **Policies > Common Objects > Other > Tags**, and "Apply tags to identify and group events" on page 573.

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.



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.

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**. 2. Make sure a Malware Scan configuration is assigned to the Scheduled scan. 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 > General**. 2. Make sure the Anti-Malware state is "On" or "Inherited (On)." 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**. 2. If the Anti-Malware Status is "Anti-Malware Engine Offline," follow the procedure to solve the "Error: Anti-Malware Engine Offline" on page 792 issue. 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 792 issue. 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**. 2. Rerun the scan.

Event reason	Reason ID *	Description	Recommended action
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. 2. If yes, either wait for the current scan task to complete or right-click the target computer and go to **Actions > Cancel Malware Scan**. 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 and logs" on page 1075. 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.	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**. 2. Make sure the Anti-Malware

Event reason	Reason ID *	Description	Recommended action
			state is "On" or "Inherited (On)." 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**. 2. Make sure the Anti-Malware state is "On" or "Inherited (On)." 3. Rerun the scan. 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 and logs" on page 1075. 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**.

Note: 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 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 576 lets you auto-tag integrity monitoring events based on their similarity to known-good events from a trusted source.

Note: 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

Note: 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 will result 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 above example, "authentication_success" would be "Authentication Success", "account_changed" would be "Account Changed". When this checkbox is set, 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

Note: 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 either:

1. A **local trusted computer**,
2. The **Trend Micro Certified Safe Software Service**, or
3. 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 that will be used as a "model" computer that you know will 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.

How does Deep Security determine whether an event on a target computer matches an event on a trusted source computer?

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.

Note: 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.

Note: Trusted source computers must be scanned for malware before applying trusted source event tagging.

Note: 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 computer(s) 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.

Note: 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.

Note: When an integrity monitoring baseline is generated for a computer, Deep Security will first check if that computer is part of a trusted common baseline group. If it is, it will include the computer's baseline data 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**.

Delete a tag

1. In an events list, right-click the events with the tag you want to delete, and select **Remove Tag(s)**.
2. Select the tag you'd like to remove. Choose to remove the tag from **The Selected [Event Type] Event** or to **Apply to selected similar [Event Type] Events.** Click **Next**.
3. Enter some optional 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.

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 Invalid Flags Invalid Sequence Invalid ACK Unsolicited UDP Unsolicited ICMP Out Of Allowed Policy Dropped Retransmit
Stateful, Normalization, and Frag Suppression	Out Of Connection Invalid Flags Invalid Sequence Invalid ACK Unsolicited UDP Unsolicited ICMP Out Of Allowed Policy CE Flags Invalid IP Invalid IP Datagram Length Fragmented Invalid Fragment Offset First Fragment Too Small Fragment Out Of Bounds Fragment Offset Too Small IPv6 Packet Max Incoming Connections Max Outgoing Connections Max SYN Sent License Expired IP Version Unknown Invalid Packet Info Maximum ACK Retransmit

[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	Ignored Events
	Packet on Closed Connection Dropped Retransmit
Stateful, Frag, and Verifier Suppression	Out Of Connection Invalid Flags Invalid Sequence Invalid ACK Unsolicited UDP Unsolicited ICMP Out Of Allowed Policy CE Flags Invalid IP Invalid IP Datagram Length Fragmented Invalid Fragment Offset First Fragment Too Small Fragment Out Of Bounds Fragment Offset Too Small IPv6 Packet Max Incoming Connections Max Outgoing Connections Max SYN Sent License Expired IP Version Unknown Invalid Packet Info Invalid Data Offset No IP Header Unreadable Ethernet Header Undefined Same Source and Destination IP Invalid TCP Header Length Unreadable Protocol Header Unreadable IPv4 Header Unknown IP Version Maximum ACK Retransmit Packet on Closed Connection Dropped Retransmit
Tap Mode	Out Of Connection Invalid Flags Invalid Sequence Invalid ACK Maximum ACK Retransmit Packet on Closed Connection 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.

Tip: Alternatively, if you want to publish events to Amazon SNS, see "Set up Amazon SNS" on page 645.

Basic steps include:

1. "Allow event forwarding network traffic" below
2. "Request a client certificate" below
3. "Define a Syslog configuration" below
4. "Forward system events" on page 587 and/or "Forward security events" on page 588

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 106. Your Syslog server must be accessible via the Internet and its domain name must be globally DNS-resolvable. See also "Deep Security as a Service IP addresses" on page 113.

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 will use 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).

Note: 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 called 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:

- **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's usually port 6514. See also "Port numbers, URLs, and IP addresses" on page 106.
- **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.

  > **Note:**
  > 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 589

  > **Note:** LEEF format requires that you set **Agents should forward logs** to **Via the Deep Security Manager** (indirectly).

> **Note:** 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.

  > **Note:** Full dates require that you set **Agents should forward logs** to **Via the Deep Security Manager** (indirectly).

- **Facility:** Type of process that events will be associated with. Syslog servers may prioritize or filter based upon 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.

  > **Note:** 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 584), then on the **Credentials** tab, configure:

   - **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 which events to forward. See "Forward system events" below and/or "Forward security events" on the next page.

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 select **New**. For details, see "Define a Syslog configuration" on page 584.
3. Click **Save**.

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.

Like other policy settings, you can override event forwarding settings for specific policies or computers. See "Policies, inheritance, and overrides" on page 216.

1. Go to **Policies**.
2. Double-click the policy used by the computers.
3. Select **Settings** and then the **Event Forwarding** tab.
4. From **Period between sending of events**, select how often to forward events.
5. From **Anti-Malware Syslog Configuration** and other protection modules' drop-down 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 584.
6. 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 870.

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:

- Splunk 6.5.1
- 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.

Tip: If you are using Splunk, you can use the Deep Security app for Splunk to get dashboards and saved searches.

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 GUI 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 the Deep Security Agent or Manager and which feature created the log message.

Note: If your syslog messages are being truncated, it may be because you're 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 584.

Note: 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 will still read " 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 the Deep Security Manager or a 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 that don't have an in-guest agent, will still be 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: • 4,000,000 - Anti-Malware - Real-Time Scan • 4,000,001 - Anti-Malware - Manual Scan • 4,000,002 - Anti-Malware - Scheduled Scan • 4,000,003 - Anti-Malware - Quick Scan • 4,000,010 - Anti-Spyware - Real-Time Scan • 4,000,011 - Anti-Spyware - Manual Scan • 4,000,012 - Anti-Spyware - Scheduled Scan • 4,000,013 - Anti-Spyware - Quick Scan • 4,000,020 - Suspicious Activity - Real-Time Scan • 4,000,030 - Unauthorized Change - Real-Time Scan
5,000,000-5,999,999	Web Reputation events. Currently, only these signature IDs are used: • 5,000,000 - Web Reputation - Blocked • 5,000,001 - Web Reputation - Detect Only
6,000,000-6,999,999	Application Control events. Currently, only these signature IDs are used:

Signature IDs	Description
	• 6,001,100 - Application Control - Detect Only, in block list • 6,001,200 - Application Control - Detect Only, not in allow list • 6,002,100 - Application Control - Blocked, in block list • 6,002,200 - Application Control - Blocked, not in allow list

Note: Log entries don't always have all CEF extensions described in the event log format tables below. 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.

Note: 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

Note: 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 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 contain a verbose description of the event.	msg=User password incorrect for username MasterAdmin on an attempt to sign in from 127.0.0.1 msg=A Scan for Recommendations on computer (localhost) has completed...
TrendMicroDsTags	TrendMicroDsTags	Event Tags	Deep Security	TrendMicroDsTags=suspicious

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			event tags assigned to the event	
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 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
cn2	cn2	File Size	The size of the quarantine file.	cn2=100

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			This extension is included only when the "direct forward" from agent/appliance is selected.	
cn2Label	cn2Label	File Size	The name label for the field cn2.	cn2Label=Quarantine File Size
cs3	cs3	InfectedResource	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	InfectedResource	The name label for the field	cs3Label=Infected Resource

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			cs3. This field is only for spyware detection events.	
cs4	cs4	Resource Type	Resource Type values: 10=Files and Directories 11=System Registry 12=Internet Cookies 13=Internet URL Shortcut 14=Pr	cs4=10

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			ograms in Memory 15=Program Startup Areas 16=Browser Helper Object 17=Layered Service Provider 18=Hosts File 19=Windows Policy Settings 20=Browser 23=Wi	

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			ndows Shell Setting 24=IE Downloaded Program Files 25=Add/Remove Programs 26=Services other=Other For example, if there's a spyware file named spy.exe that create	

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			s a registry run key to keep its persistence after system reboot, there will be two items in the spyware report: the item for spy.exe has cs4=10 (Files and Directories), and the item	

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			This field is only for spyware detection events.	
cs4Label	cd4Label	Resource Type	The name label for the field cs4. This field is only for spyware detection events.	cs4Label=Resource Type
cs5	cs5	Risk Level	Risk level values: 0=Very Low 25=Low 50=Me	cs5=25

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			dium 75=High 100=Very High This field is only for spyware detection events.	
cs5Label	cs5Label	Risk Level	The name label for the field cs5. This field is only for spyware detection events.	cs5Label=Risk Level
cs6	cs6	Container	The image name of the Docke	cs6=ContainerImageName | ContainerName | ContainerID

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			r container, container name, and container ID where the malware was detected.	
cs6Label	cs6Label	Container	The name label for the field cs6.	cs6Label=Container
filePath	filePath	File Path	The location of the malware file.	filePath=C:\\Users\\Mei\\Desktop\\virus.exe
act	act	Action	The action performed by the Anti-Malware engine. Possible values are: Deny	act=Clean act=Pass

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			Access, Quarantine, Delete, Pass, Clean, Terminate, and Unspecified.	
msg	msg	Message	The type of scan. Possible values are: Realtime, Scheduled, and Manual.	msg=Realtime msg=Scheduled
dvc	dvc	Device address	The IPv4 address for cn1. Does not appear if the source is an IPv6 addres	dvc=10.1.144.199

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			s or hostname. (Uses dvchost instead.)	
dvchost	dvchost	Device hostname	The hostname or IPv6 address for cn1. Does not appear if the source is an IPv4 address. (Uses dvc field instead.)	dvchost=www.example.com dvchost=fe80::f018:a3c6:20f9:afa6%5
TrendMicroDsBehaviorRuleID	TrendMicroDsBehaviorRuleID	Behavior monitoring rule	The behavior monitoring rule ID	BehaviorRuleID=CS913

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
		ID	for internal malware case tracking.	
TrendMicroDsBehaviorType	TrendMicroDsBehaviorType	Behavior Monitoring type	The type of behavior monitoring event detected.	BehaviorType=Threat-Detection
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	TrendMicroDsMalwareTarget=N/A TrendMicroDsMalwareTarget=C:\\Windows\\System32\\cmd.exe TrendMicroDsMalwareTarget=HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings TrendMicroDsMalwareTarget=Multiple

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			(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." Only suspicious activity monitoring and unauthorized	

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			change monitoring have values for this field.	
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 Windows registry.	TrendMicroDsMalwareTargetType=N/A TrendMicroDsMalwareTargetType=Exploit TrendMicroDsMalwareTargetType=File System TrendMicroDsMalwareTargetType=Process TrendMicroDsMalwareTargetType=Registry

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			Only suspicious activity monitoring and unauthorized change monitoring have values for this field.	
TrendMicroDsProcess	TrendMicroDsProcess	Process	Process Name	TrendMicroDsProcess= abc.exe
TrendMicroDsFileMD5	TrendMicroDsFileMD5	FileMD5	The MD5 hash of the file	TrendMicroDsFileMD5=1947A1BC0982C5871FA3768CD025453E
TrendMicroDsFileSHA1	TrendMicroDsFileSHA1	FileSHA1	The SHA1 hash of the file	TrendMicroDsFileSHA1=5AD084DDCD8F80FBF2EE3F0E4F812E812DEE60C1
TrendMicroDsFileSHA256	TrendMicroDsFileSHA256	FileSHA256	The SHA256 hash of the file	TrendMicroDsFileSHA256=25F231556700749F8F0394CAABDED83C2882317669DA2C01299B45173482FA6E
TrendMicroDsDetectionConfide	TrendMicroDsDetectionConfide	Threat	Indicates	TrendMicroDsDetectionConfidence=95

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
nce	nce	Probability	how closely (in %) the file matched the malware model	
TrendMicroDsRelevantDetectionNames	TrendMicroDsRelevantDetectionNames	Probable Threat Type	Indicates the most likely type of threat contained in the file after Predictive Machine Learning compared the analysis to other known threats (separate by semicolon";")	TrendMicroDsRelevantDetectionNames=Ransom_CERBER.BZC;Ransom_CERBER.C;Ransom_CRYPNISCA.SM
None	sev	Severity	The severity of the event. 1 is	sev=6

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			the least severe; 10 is the most severe.	
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

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 unique identifier.	cn1=2
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	cs1=notWhitelisted

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			was configured to block unrecognized software).	
cs1Label	cs1Label		The name label for the field cs1.	cs1Label=actionReason
cs2	cs2		If it was calculated, the SHA-1 hash of the file.	cs2=156F4CB711FDBD668943711F853FB6DA89581AAD
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	act=blocked

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			are: Blocked, Allowed.	
dvc	dvc	Device address	The IPv4 address for cn1. Does not appear if the source is an IPv6 address or hostname. (Uses dvchost instead.)	dvc=10.1.1.10
dvchost	dvchost	Device host name	The hostname or IPv6 address for cn1. Does not appear if the source is an IPv4 address. (Uses dvc field instead.)	dvchost=www.example.com dvchost=2001:db8::5
suid	suid	User ID	The account ID number of the user	suid=0

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			name.	
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
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	AggregationType	An integer that indicates how the event is	aggregationType=2

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			aggregated: • 0: The event is not aggregated • 1: The event is aggregated based on filename, path, an	

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			d event type. • 2: The event is aggregated based on event type. For information, about event aggregation, see "View Application Control	

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			event logs" on page 552.	
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 more.	repeatCount=4
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	desc=blocked

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			Control uses the action as the description.	

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 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

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
cnt	cnt	Repeat Count	The number of times this event was sequentially repeated.	cnt=8
cs2	cs2	TCP Flags		cs2=0x10 ACK 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 cs3=MF 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 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 destination computer's network	dmac= 00:0C:29:2F:09:B3

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			interface.	
dpt	dstPort	Destination Port	(For TCP and UDP protocol only) Port number of the destination computer's connection or session.	dpt=80 dpt=135
dst	dst	Destination IP Address	IP address of the destination computer.	dst=192.168.1.102 dst=10.30.128.2
in	in	Inbound Bytes Read	(For inbound connections only) Number of inbound bytes read.	in=137 in=21
out	out	Outbound Bytes Read	(For outbound connections only) Number of outbound bytes read.	out=216 out=13
proto	proto	Transport protocol	Name of the transport protocol used.	proto=tcp proto=udp proto=icmp
smac	srcMAC	Source MAC Address	MAC address of the	smac= 00:0E:04:2C:02:B3

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			source computer's network interface.	
spt	srcPort	Source Port	(For TCP and UDP protocol only) Port number of the source computer's connection or session.	spt=1032 spt=443
src	src	Source IP Address	The packet's source IP address at this event.	src=192.168.1.105 src=10.10.251.231
TrendMicroDsFrameType	TrendMicroDsFrameType	Ethernet frame type	Connection ethernet frame type.	TrendMicroDsFrameType=IP TrendMicroDsFrameType=ARP TrendMicroDsFrameType=RevARP TrendMicroDsFrameType=NetBEUI
TrendMicroDsPacketData	TrendMicroDsPacketData	Packet data	The packet data, represented in Base64.	TrendMicroDsPacketData=AFB...
dvc	dvc	Device address	The IPv4 address for cn1. Does not appear if	dvc=10.1.144.199

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			the source is an IPv6 address or hostname. (Uses dvchost instead.)	
dvchost	dvchost	Device host name	The hostname or IPv6 address for cn1. Does not appear if the source is an IPv4 address. (Uses dvc field instead.)	dvchost=exch01.example.com 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	TrendMicroDsTenant=Primary
TrendMicroDsTenantId	TrendMicroDsTenantId	Tenant ID	Deep Security tenant ID	TrendMicroDsTenantId=0
None	sev	Severity	The severity of the	sev=5

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			event. 1 is the least severe; 10 is the most severe.	
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 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
suser	suser	Source User	Deep Security Manager administrator's account.	suser=MasterAdmin
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	msg=lastModified,sha1,size

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			names. If "Relay via Manager" is selected, all event action types include a full description.	
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. Does not appear if the source is an IPv6 address or hostname.	dvc=10.1.144.199

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			(Uses dvchost instead.)	
dvchost	dvchost	Device host name	The hostname or IPv6 address for cn1. Does not appear if the source is an IPv4 address. (Uses dvc field instead.)	dvchost=www.example.com 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

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
None	desc	Description	Event description. Integrity Monitoring uses the event name as the description.	desc=Microsoft Windows - System file modified

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	cn1Label=Host ID

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			label for 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	cs1=Drop_data

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			converted to underscores. If it contains 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 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 cs3=MF cs3=DF MF
cs3Label	cs3Label	Fragmenta	The	cs3Label=Fragmentation Bits

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
		tion Bits	name label for the field cs3.	
cs4	cs4	ICMP Type and Code	(For the ICMP protocol only) The ICMP type and code stored in their respective order delimited by a space.	cs4=11 0 cs4=8 0
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 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: 1 - Data truncated - Data	The following example would be a summed combination of 1 (Data truncated) and 8 (Have Data): cs6=9

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			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.	
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	dpt=80 dpt=135

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			computer connection port.	
dst	dst	Destination IP Address	Destination computer IP Address.	dst=192.168.1.102 dst=10.30.128.2
xff	xff	X-Forwarded-For	The IP address of the last hub in the X-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.	xff=192.168.137.1
in	in	Inbound Bytes Read	(For inbound	in=137 in=21

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			connections only) Number of inbound bytes read.	
out	out	Outbound Bytes Read	(For outbound connections only) Number of outbound bytes read.	out=216 out=13
proto	proto	Transport protocol	Name of the connection transport protocol used.	proto=tcp proto=udp proto=icmp
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 spt=443
src	src	Source IP Address	Source computer IP Address. This is the IP of the last proxy server, if	src=192.168.1.105 src=10.10.251.231

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			it exists, or the client IP. See also the xff field.	
TrendMicroDsFrameType	TrendMicroDsFrameType	Ethernet frame type	Connection ethernet frame type.	TrendMicroDsFrameType=IP TrendMicroDsFrameType=ARP TrendMicroDsFrameType=RevARP TrendMicroDsFrameType=NetBEUI
TrendMicroDsPacketData	TrendMicroDsPacketData	Packet data	The packet data, represented in Base64.	TrendMicroDsPacketData=R0VUIC9zP3...
dvc	dvc	Device address	The IPv4 address for cn1. 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.	dvchost=www.example.com dvchost=2001:db8::5

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			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 name	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=10
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	desc=Sun Java RunTime Environment Multiple Buffer Overflow Vulnerabilities

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			use the event name as the description.	

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	cs1=Multiple Windows audit failure events

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			this event.	
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) 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 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 Address	Source computer IP address.	src=192.168.1.105 src=10.10.251.231
dvc	dvc	Device address	The IPv4 address for cn1.	dvc=10.1.144.199

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			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. Does not appear if the source is an IPv4 address. (Uses dvc field instead.)	dvchost=www.example.com 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	msg=Realtime

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
			of action. Possible values are: Realtime, Scheduled, and Manual.	msg=Scheduled
dvc	dvc	Device address	The IPv4 address for cn1. 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. Does not appear if the source is an IPv4 address. (Uses dvc field instead.)	dvchost=www.example.com dvchost=2001:db8::5
TrendMicroDsTag	TrendMicroDsTag	Events	Deep	TrendMicroDsTags=suspicious

CEF Extension Field	LEEF Extension Field	Name	Description	Examples
s	s	tags	Security event tags assigned to the event	
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=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

Configure Red Hat Enterprise Linux to receive event logs

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:
   `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:
   - On Red Hat Enterprise Linux 6: `service rsyslog restart`
   - On Red Hat Enterprise Linux 7: `systemctl restart rsyslog`

When Syslog is functioning you will see logs 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 to receive logs from Deep Security.

1. Log in as root
2. Execute:
   `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:
   `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: `/etc/init.d/syslog restart`

When Syslog is functioning you will see logs populated in: `/var/log/DSM.log`

Access events with Amazon SNS

Set up Amazon SNS

If you have an AWS account, you can take advantage of the Amazon Simple Notification Service (SNS) to publish notifications about Deep Security events and deliver them to subscribers. For details about SNS, see https://aws.amazon.com/sns/.

To set up Amazon SNS:

1. "Create an AWS user" on the next page.
2. "Create an Amazon SNS topic" on the next page.
3. "Enable SNS" on the next page.
4. "Create subscriptions" on page 647.

See the sections below for details on how to perform these tasks.

Create an AWS user

In order to use Amazon SNS with Deep Security, you need to create an AWS user with the appropriate permissions for SNS. Note the access key and secret key for the user, because you will need that information for step 3, below.

The AWS user will need the "sns:Publish" permission on all SNS topics that Deep Security will publish to. This 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 Special Information for Amazon SNS Policies in the Amazon AWS documentation.

Create an Amazon SNS topic

In AWS, create an SNS topic where the events will be published. For instructions on how to create an Amazon SNS topic, see "Create a Topic" in the Amazon SNS documentation. Note the SNS Topic ARN because you will need this information in step 3, below.

Enable SNS

1. In the 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. Enter this information:
   - **Access Key:** The access key of the AWS user you created in section 1.
   - **Secret Key:** The secret key of the AWS user you created in section 1.
   - **SNS Topic ARN:** The SNS Topic ARN that events will be sent to. This is the ARN that you noted in section 2.
4. Select the types of events that you want to forward to SNS.

   Selecting the events automatically generates a JSON SNS configuration.

5. (Optional) 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" below.

   Note: If you edit the JSON, the event check boxes will become unavailable. If you want to select or deselect any of the event check boxes, you can click **Revert to basic SNS configuration**, but any customizations you have made to the JSON SNS configuration will be discarded.

6. 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: 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 662.

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 663). 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 the next page.

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 686.

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 647.

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)
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 show what would have happened if the rule had been enabled. 0=Unknown, 1=Deny, 6=Log Only, 0x81=Detect Only: Deny.	Firewall events
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
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	Application Control

Property Name	Data Type	Description	Applies To Event Type(s)
		Control event occurred repeatedly. If "AggregationType" is not "0", 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	events
ApplicationType	String	Name of the network application type associated with the Intrusion Prevention rule, if available.	Intrusion Prevention 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
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 the event occurred.	Anti-Malware events, Intrusion Prevention events, Firewall events

Property Name	Data Type	Description	Applies To Event Type(s)
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, 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	Firewall

Property Name	Data Type	Description	Applies To Event Type(s)
		string.	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
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	All event types

Property Name	Data Type	Description	Applies To Event Type(s)
		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.	
EventType	String (enum)	The type of the event. One of: "SystemEvent", "PacketLog", "PayloadLog", "AntiMalwareEvent", "WebReputationEvent", "IntegrityEvent", "LogInspectionEvent", "AppControlEvent".	All event types
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
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
Frame	Integer (enum)	Frame type. -1=Unknown, 2048=IP, 2054=ARP, 32821=REVARP, 33169=NETBEUI, 0x86DD=IPv6	Firewall events, Intrusion Prevention

Property Name	Data Type	Description	Applies To Event Type(s)
			events
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.	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.	Application Control events
HostAssetValue	Integer	The asset value assigned to the computer at the time the event was generated.	Anti-Malware events, Web Reputation

Property Name	Data Type	Description	Applies To Event Type(s)
			events, Integrity Monitoring events, Log Inspection events, Firewall events, Intrusion Prevention events, Application Control events
HostGroupID	Integer	The unique identifier of the Computer Group of the computer where the event was detected.	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.	Anti-Malware events, Web Reputation events, Integrity Monitoring events, Log Inspection events, Firewall events,

Property Name	Data Type	Description	Applies To Event Type(s)
			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.	Anti-Malware events, Web Reputation events, Integrity Monitoring events, Log Inspection events, Firewall events, Intrusion Prevention events
Hostname	String	Hostname of the computer on which the event was generated.	Anti-Malware events,

Property Name	Data Type	Description	Applies To Event Type(s)
			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, 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.	Anti-Malware events, Web Reputation events, Integrity Monitoring

Property Name	Data Type	Description	Applies To Event Type(s)
			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
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,

Property Name	Data Type	Description	Applies To Event Type(s)
			Application Control events
HostVCUUID	String	The vCenter UUID of the computer the event applies to, if known.	Anti-Malware events, Web Reputation events, Integrity Monitoring events, Log Inspection events, Firewall events, Intrusion Prevention events
ImageDigest	String	A unique digest that identifies the container image.	Intrusion Prevention events, Firewall events
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

Property Name	Data Type	Description	Applies To Event Type(s)
			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, IPS, etc.), the time is when the event was recorded by the agent, not when the event was received by Deep Security Manager.	All event types
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

Property Name	Data Type	Description	Applies To Event Type(s)
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
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
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

Property Name	Data Type	Description	Applies To Event Type(s)
OSSEC_Data	String	OSSEC data	Log Inspection events
OSSEC_Description	String	OSSEC description	Log Inspection events
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

Property Name	Data Type	Description	Applies To Event Type(s)
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
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

Property Name	Data Type	Description	Applies To Event Type(s)
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
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

Property Name	Data Type	Description	Applies To Event Type(s)
			events
ProcessID	Integer	The identifier (PID) of the process that generated the event, if available.	Application Control events, Intrusion Prevention events, Firewall events
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
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

Property Name	Data Type	Description	Applies To Event Type(s)
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 was not triggered by a rule. For Application Control, "Reason" may be "None"; see "BlockReason" instead.	Firewall, Intrusion Prevention, integrity monitoring, 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

Property Name	Data Type	Description	Applies To Event Type(s)
ScanResultAction1	Integer	Scan result action 1.	Anti-Malware events
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

Property Name	Data Type	Description	Applies To Event Type(s)
SHA1	String	The SHA-1 checksum (hash) of the software, if any.	Application Control events
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
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, 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	Integrity

Property Name	Data Type	Description	Applies To Event Type(s)
		of an integrity monitoring event, if known.	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	The user name, if any, of the user account that tried to start the software, such as "root".	Application Control events

Data types of event properties

Events forwarded as JSON usually use strings to encode other data types.

Data Type	Description
Boolean	JSON `true` or `false`.
Integer	JSON `int`. Deep Security does not output floating point numbers in events. **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.

Data Type	Description
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:u
s-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" :         "[
                        {
                          "AMTargetTypeString":"N/A",
                          "ATSEDetectionLevel":0,
                          "CreationTime":"2018-12-
04T15:57:18.000Z",
                          "EngineType":1207959848,
                          "EngineVersion":"10.0.0.1040",
```

```
                            "ErrorCode":0,
                            "EventID":1,
                            "EventType":"AntiMalwareEvent",
                            "HostAgentGUID":"4A5BF25A-4446-DD8B-
DFB7-564C275F5F6B",
                            "HostAgentVersion":"11.1.0.163",
                            "HostID":1,
                            "HostOS":"Amazon Linux (64 bit)
(4.14.62-65.117.amzn1.x86_64)",
                            "HostSecurityPolicyID":3,
                            "HostSecurityPolicyName":"PolicyA",
                            "Hostname":"ec2-12-123-123-123.us-west-
2.compute.amazonaws.com",
                            "InfectedFilePath":"/tmp/eicar_
1543939038890.txt",
                            "LogDate":"2018-12-04T15:57:19.000Z",
                            "MajorVirusType":2,
                            "MajorVirusTypeString":"Virus",
                            "MalwareName":"Eicar_test_file",
                            "MalwareType":1,
                            "ModificationTime":"2018-12-
04T15:57:18.000Z",
                            "Origin":0,
                            "OriginString":"Agent",
                            "PatternVersion":"14.665.00",
                            "Protocol":0,
                            "Reason":"Default Real-Time Scan
Configuration",
                            "ScanAction1":4,
                            "ScanAction2":3,
                            "ScanResultAction1":-81,
                            "ScanResultAction2":0,
                            "ScanResultString":"Quarantined",
```

```
                            "ScanType":0,
                            "ScanTypeString":"Real Time",
                            "Tags":"\",
                            "TenantID":123,
                            "TenantName":"Umbrella Corp."},
                           {
                            "AMTargetTypeString":"N/A",
                            "ATSEDetectionLevel":0,
                            "CreationTime":"2018-12-
04T15:57:21.000Z",
                            ...},
                           {
                            "AMTargetTypeString":"N/A",
                            "ATSEDetectionLevel":0,
                            "CreationTime":"2018-12-
04T15:57:29.000Z",
                            ...
                           }
                         ]",
  "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:u
s-west-2:123456:DS_Events:123abc-123-123-123-123abc"
}
```


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 699). 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" below).
- You can get an email notification when an alert is triggered (see "Set up email notification for alerts" on the next page.)
- You can generate alert reports (see "Generate reports about alerts and other activity" on page 695).

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.

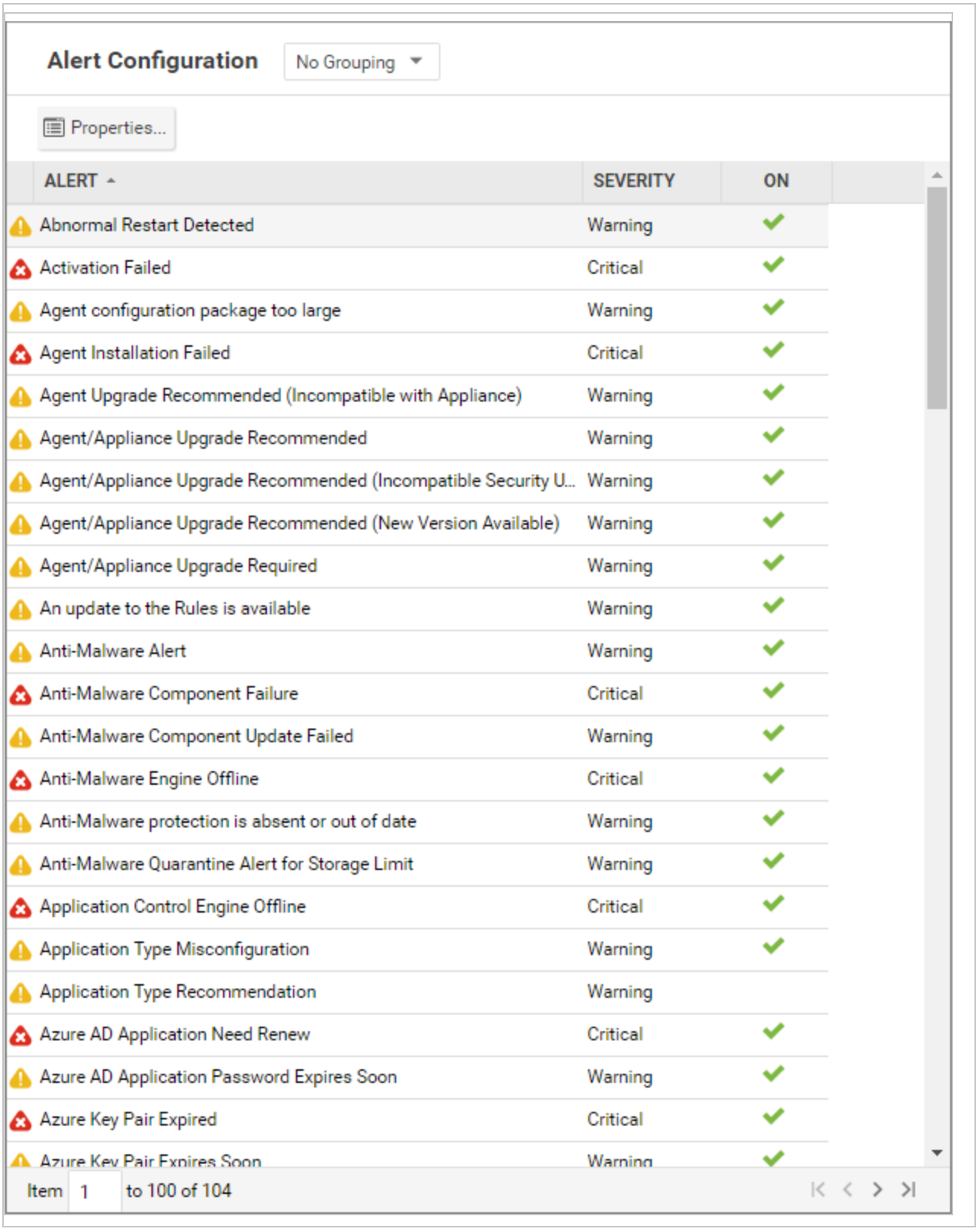
Set up email notification for alerts

Deep Security Manager can send emails to specific users when selected alerts are triggered.

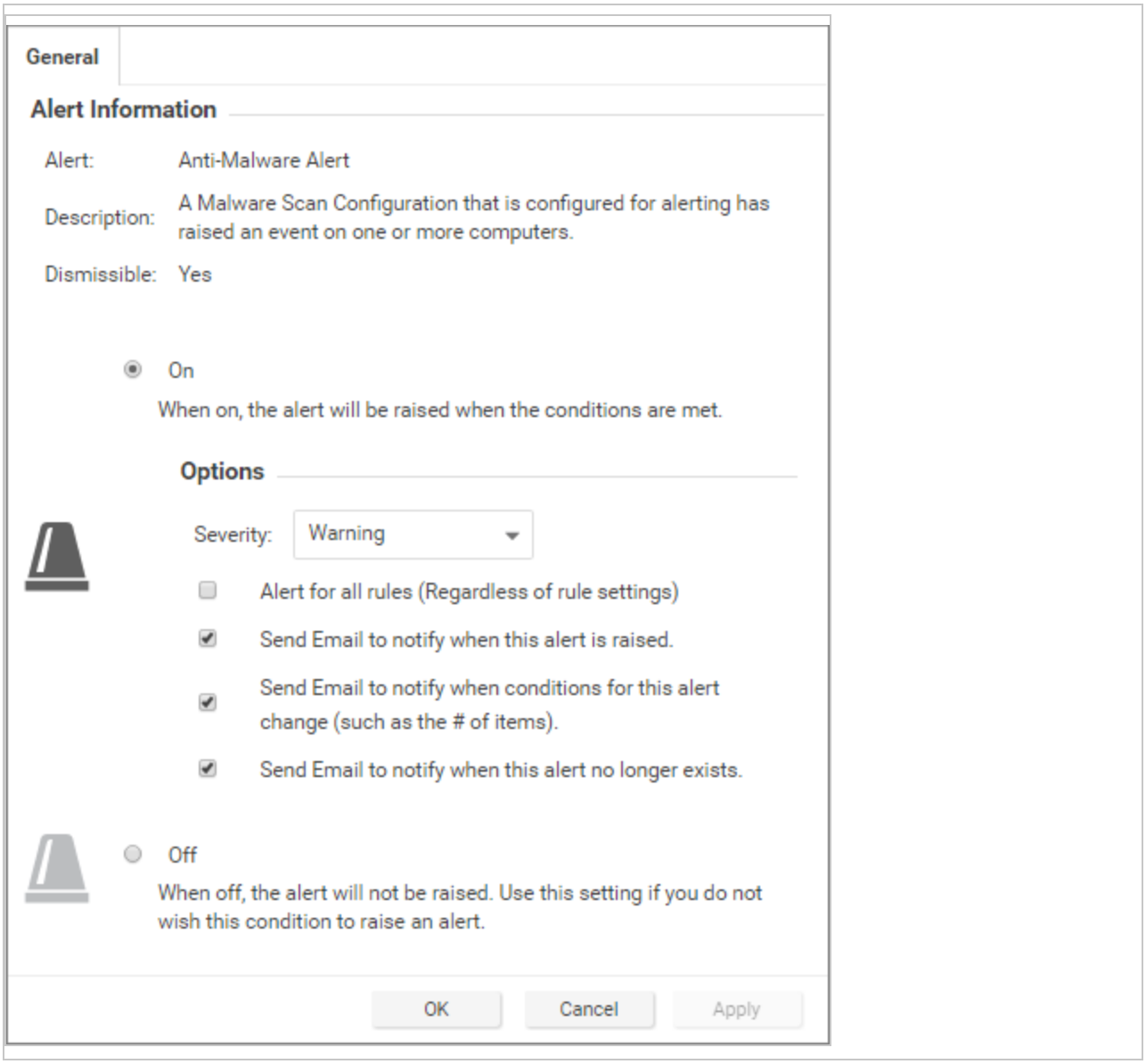
To enable email notifications:

Turn alert emails on or off

1. Go to the **Alerts** page and click **Configure Alerts** to display the list of alerts.



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.



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.

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 will be disabled for reports to which they don't 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 698).

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, these 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. For details about what's included, 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 Computers 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:** Baseline of the computer(s) 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
- **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
- **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. (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.
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 tag(s).

   Note: 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. 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:** 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 the signed in User has view access right to.
   - **In Group:** The computers in a Deep Security group.
   - **Using Policy:** The computers using a specific protection Policy.
   - **Computer:** A single computer.

   Note: 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.

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 (this feature used to be named "Recurring Reports").

To set up a scheduled report, go to the **Events & Reports** tab and then in the left pane, click **Generate Reports > Scheduled Reports**. Click **New**. The New Scheduled Task wizard opens and will step you through the configuration process. Most of the options are identical to those for single reports, with the exception of Time Filter:

- **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.

Note: 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 991.

Lists of events and alerts

Predefined alerts

Alert	Default Severity	Dismissible	Description
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 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.

Alert	Default Severity	Dismissible	Description
			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.
Account Balance Depleted	Critical	No	Your pre-paid account balance has been depleted. You will no longer receive updates, including security updates, until your account is replenished. To ensure your security is maintained, please contact your sales representative to add credit to your account.
Account Balance Low	Warning	No	Your pre-paid account balance is running low. To ensure uninterrupted service, please contact your sales representative to add more credit to your account.
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 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. This may indicate a problem with 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).

Alert	Default Severity	Dismissible	Description
			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/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.
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.

[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
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, 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 543.) 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

Alert	Default Severity	Dismissible	Description
			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.
AWS Contract License Exceeded	Critical	No	AWS Contract License expired or AWS Contract entitlements have been exceeded.
Azure AD Application Needs Renew	Critical	No	The Azure AD 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 AD Application Expires Soon	Warning	No	The Azure AD application password will expire soon. You can remove this alert by renewing 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.
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. Refer to "Warning: Census, Good File Reputation, and Predictive Machine Learning Service Disconnected" on page 803 for troubleshooting tips.

Alert	Default Severity	Dismissible	Description
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.
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.

Alert	Default Severity	Dismissible	Description
Configuration Required	Warning	No	One or more computers are using a policy that defines multiple interface types where not all interfaces have been mapped.
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.
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 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.
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

Alert	Default Severity	Dismissible	Description
			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.
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 805.
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 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

Alert	Default Severity	Dismissible	Description
			'Integrity 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.
Legacy Agent Software Detected	Warning	Yes	We have detected software whose version is less than 9.5, and is no longer supported. Please import the latest software to replace it. For details, see "Get Deep Security Agent software" on page 144.
License Expired	Critical	No	Your Deep Security as a Service license has expired. You will no longer receive updates, including security updates, until your license is

Alert	Default Severity	Dismissible	Description
			renewed. To ensure your security is maintained, please contact your sales representative to renew your license.
License Expiring Soon	Warning	No	Your Deep Security as a Service license will expire soon. Please contact your sales representative to renew your license.
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.
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 accidentally added to the ruleset.
Network Engine Mode Incompatibility	Warning	No	Setting "Network Engine Mode" to "Tap" is only available on agent versions 5.2 or higher. 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

Alert	Default Severity	Dismissible	Description
			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.
Newer Versions of Software Available	Warning	No	New software is available. Software can be downloaded from the Download Center.
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 the computer's events to see the details of the probe and see "Warning: Reconnaissance Detected" on page 805.
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 805.
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.

[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
			Check the computer's events to see the details of the probe and see "Warning: Reconnaissance Detected" on page 805.
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 805.
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 805.
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) expire 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 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

Alert	Default Severity	Dismissible	Description
			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.
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. 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

[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
			one or more users have passwords that will expire within the next 7 days.
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, and billed at a lower hourly rate, if you are using hourly billing.

Agent events

ID	Severity	Event	Notes
Special Events			
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	Warning	Upgrading Driver	
1006	Error	Driver Upgrade Requires Reboot	
1007	Warning	Driver Upgrade Succeeded	
1008	Error	Kernel Unsupported	
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	

ID	Severity	Event	Notes
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	
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	

ID	Severity	Event	Notes
3002	Warning	Too Many Interfaces	
3003	Error	Unable To Run External Command	
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	

ID	Severity	Event	Notes
5007	Info	Appliance Protection 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. For details, see Linux Secure Boot support for agents.
5111	Error	Secure Boot 'On' Not Supported	Deep Security Agent does not support this OS with Secure Boot enabled. For details, see Linux Secure Boot support for agents.
5200	Info	File Backup Completed	
5201	Error	Failure to Backup File	
Logging-Related Events			
6000	Info	Log Device Open Error	

ID	Severity	Event	Notes
6001	Info	Log File Open Error	
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 805.
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	
9110	Error	Anti-Malware license is	

ID	Severity	Event	Notes
		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 787.
9301	Info	Smart Protection Server Connected for Web Reputation	See "Troubleshoot "Smart Protection Server disconnected" errors" on page 787.
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 to record individual events and whether 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 won't appear under the **Events & Reports** tab (or anywhere in Deep Security Manager) and it won't be forwarded either.

Depending on whether it's a system configuration change or security incident, each log will appear in either the **System Events** sub-menu, or the sub-menu 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	
102	Info	Trend Micro Deep Security Customer Account Changed	
103	Warning	Check For Updates Failed	
104	Warning	Automatic Software Download Failed	
105	Warning	Scheduled Rule Update Download and Apply Failed	
106	Info	Scheduled Rule Update Downloaded and Applied	
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	
113	Warning	Scheduled Rule Update Download Failed	
114	Info	Scheduled Rule	

ID	Severity	Event	Description or Solution
		Update Downloaded	
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	
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	
131	Warning	Credential Generation Failed	
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	

ID	Severity	Event	Description or Solution
152	Info	Software Deleted	
153	Info	Software Updated	
154	Info	Software Exported	
155	Info	Software Platforms Changed	
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: <detailed_message> Please contact Trend Micro support for more help. See "Check digital signatures on software packages" on page 136 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	
165	Error	Security Update Failed	
166	Info	Check for New Software Success	
167	Error	Check for New Software Failed	
168	Info	Manual Security Update Successful	
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.
171	Info	Anti-Malware Spyware Item Exported	
172	Info	Web Reputation Events Exported	
173	Info	Anti-Malware Identified Files List	

ID	Severity	Event	Description or Solution
		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.
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	
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	

ID	Severity	Event	Description or Solution
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	
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

ID	Severity	Event	Description or Solution
			"Automatically upgrade agents on activation" on page 853.
278	Info	Software Update: Reboot to Complete Agent Software Upgrade	
280	Info	Computers Exported	
281	Info	Computers Imported	
286	Info	Computer Log Exported	
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	
296	Info	Interface IP 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 Requested	
302	Info	Agent Software Removal Requested	
303	Info	Computer Renamed	
305	Info	Scan for Integrity Requested	
306	Info	Rebuild Baseline Requested	

ID	Severity	Event	Description or Solution
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	
320	Info	Directory Synchronization	
321	Info	Directory Synchronization Finished	
322	Error	Directory Synchronization Failed	
323	Info	Directory Synchronization Requested	
324	Info	Directory Synchronization Cancelled	
325	Info	User Synchronization	Synchronization of the user accounts with Microsoft Active Directory has been started.
326	Info	User Synchronization Finished	Synchronization of the user accounts with Microsoft Active Directory has completed.
327	Error	User Synchronization Failed	
328	Info	User Synchronization Requested	
329	Info	User Synchronization Cancelled	
330	Info	SSL Configuration Created	
331	Info	SSL Configuration Deleted	
332	Info	SSL Configuration	

ID	Severity	Event	Description or Solution
		Updated	
333	Info	Host Merge Finished	
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. For details, see Linux Secure Boot support for agents.
357	Error	Secure Boot 'On' Not Supported	Deep Security Agent does not support this OS with Secure Boot enabled. For details, see Linux Secure Boot support for agents.
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 104.
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	

ID	Severity	Event	Description or Solution
411	Info	Firewall Rule 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	

ID	Severity	Event	Description or Solution
		Prevention Rule 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	

ID	Severity	Event	Description or Solution
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	
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	
565	Info	Backup Finished	

ID	Severity	Event	Description or Solution
566	Error	Backup Failed	
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.
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	

ID	Severity	Event	Description or Solution
		Require Configuration Resolved	
586	Warning	Log Inspection Rules Require Configuration	
587	Info	Log Inspection Rules Require Configuration Resolved	
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.

ID	Severity	Event	Description or Solution
610	Info	User Session Validated	
611	Info	User Viewed Firewall Event	
613	Info	User Viewed Intrusion Prevention Event	
615	Info	User Viewed System Event	
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	

ID	Severity	Event	Description or Solution
		Updated	
633	Info	Syslog Configuration Exported	
634	Info	Syslog Configuration Imported	
650	Info	User Created	
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	
663	Info	Roles Imported	
664	Info	Roles Exported	
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	
676	Error	API Key Made Invalid Request	
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	

ID	Severity	Event	Description or Solution
		Key Expired	
700	Info	Agent Software Installed	
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 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	This can occur if agent self-protection is enabled. 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).

ID	Severity	Event	Description or Solution
		Removal Failed	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.
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 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 805.
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 normally caused by a network interruption while events are being transferred. Clear the error and run a "Get Events Now" to retry the operation.

[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).

ID	Severity	Event	Description or Solution
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 1064.
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	
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 794.
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	The Agent is having problems communicating its status to

[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
		Problem	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	
750	Warning	Last Automatic Retry	
755	Info	Deep Security Manager Version Compatibility 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. 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 Update (s))	Each security module rule (such as Firewall, Anti-Malware, and the others) has a specific minimum Deep Security Agent or Deep Security Virtual Appliance version that's required in order for the rule to run.

ID	Severity	Event	Description or Solution
			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 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 786.
780	Info	Recommendation Scan Failure Resolved	
781	Warning	Recommendation Scan Failure	See "Troubleshooting: Recommendation Scan Failure" on page 231.
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	

ID	Severity	Event	Description or Solution
		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 failed. See also "Anti-Malware scan failures and cancellations" on page 570.
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 570.
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	

ID	Severity	Event	Description or Solution
		Failed to Compile	
850	Warning	Reconnaissance Detected: Computer OS Fingerprint Probe	See "Warning: Reconnaissance Detected" on page 805
851	Warning	Reconnaissance Detected: Network or Port Scan	See "Warning: Reconnaissance Detected" on page 805
852	Warning	Reconnaissance Detected: TCP Null Scan	See "Warning: Reconnaissance Detected" on page 805
853	Warning	Reconnaissance Detected: TCP SYNFIN Scan	See "Warning: Reconnaissance Detected" on page 805
854	Warning	Reconnaissance Detected: TCP Xmas Scan	See "Warning: Reconnaissance Detected" on page 805
900	Info	Deep Security Manager Audit Started	
901	Info	Deep Security Manager Audit Shutdown	
902	Info	Deep Security Manager Installed	
903	Warning	License Related Configuration Change	
904	Info	Diagnostic Logging Enabled	
905	Info	Diagnostic Logging Completed	
910	Info	Diagnostic Package Generated	
911	Info	Diagnostic Package Exported	
912	Info	Diagnostic Package Uploaded	
913	Error	Automatic Diagnostic Package Error	
914	Info	Identified File Deletion	

ID	Severity	Event	Description or Solution
		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	
920	Info	Usage Information Generated	
921	Info	Usage Information Package Exported	
922	Info	Usage Information Package Uploaded	
923	Error	Usage Information Package Error	
924	Warning	File cannot be analyzed or quarantined (VM maximum disk space used to store identified files exceeded)	The Anti-Malware module was unable to analyze or quarantine a file because the VM 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.
925	Warning	File cannot be analyzed or quarantined (maximum disk space used to store identified files exceeded)	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.
926	Warning	Smart Protection Server Disconnected for Smart Scan	See "Troubleshoot "Smart Protection Server disconnected" errors" on page 787.
927	Info	Smart Protection Server Connected for Smart Scan	
928	Info	Identified File Restoration	

ID	Severity	Event	Description or Solution
		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 787.
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 1068
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	

ID	Severity	Event	Description or Solution
		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 Utility Started	
978	Info	Command Line Utility Failed	
979	Info	Command Line Utility Shutdown	Deep Security Manager was manually stopped.
980	Info	System Information Exported	
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	

ID	Severity	Event	Description or Solution
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 "Deep Security Agent Linux kernel support" on page 88.
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	

ID	Severity	Event	Description or Solution
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	
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 570.
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 570.

ID	Severity	Event	Description or Solution
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-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 570.
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 570.
1544	Info	Quick Malware Scan Resumed	
1545	Info	Files could not be scanned for	Anti-malware could not scan a file because its file path exceeded the maximum number of characters. Maximum file

ID	Severity	Event	Description or Solution
		malware	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 Updated	
1553	Info	Log Inspection Configuration Updated	
1554	Info	Firewall Stateful Configuration Updated	
1555	Info	Intrusion Prevention Configuration Updated	
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	

ID	Severity	Event	Description or Solution
		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	
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	

ID	Severity	Event	Description or Solution
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 Back to Normal	
1900	Info	Cloud Account Added	
1901	Info	Cloud Account Removed	
1902	Info	Cloud Account Updated	
1903	Info	Cloud Account Synchronization In Progress	
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	

ID	Severity	Event	Description or Solution
		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	
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	

ID	Severity	Event	Description or Solution
1928	Warning	AWS Account Update Failed	
1929	Info	Upgrade Connector to AWS Account Finished	
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	
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	

ID	Severity	Event	Description or Solution
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 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

ID	Severity	Event	Description or Solution
			executing an AWS billing job. If the problem persists, contact your support provider.
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	
2206	Info	Security Update: Pattern Update on Agents/Appliances Skipped	
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	
2400	Info	Software Update:	

ID	Severity	Event	Description or Solution
		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	
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	
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	

ID	Severity	Event	Description or Solution
		Download Successful	
2700	Info	Software Update: Log Inspection Module Installation 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	

ID	Severity	Event	Description or Solution
2902	Warning	Software Update: Relay Module Installation Failed	
2903	Info	Software Update: Relay Module 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	

ID	Severity	Event	Description or Solution
		Failed	
2926	Warning	Submission to Deep Discovery Analyzer queued	
2930	Info	File back up pending	
2931	Info	Smart Folder 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	
2936	Info	Inactive User Deleted	
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	
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	

ID	Severity	Event	Description or Solution
		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 Cleanup Completed Successfully	Inactive agent cleanup removed computers that have 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 860.
2954	Warning	Dropped events recorded in the future	
2970	Info	GCP Account Added	GCP Account: <GCPaccountname> successfully added. For details, see "Add a Google Cloud Platform account" on page 199.
2971	Info	GCP Account Removed	GCP Account: <GCPaccountname> successfully removed. For details, see "Remove a GCP account" on page 202.
2972	Info	GCP Account Updated	GCP Account: <GCPaccountname> successfully updated. For details, see "Add a Google Cloud Platform account" on page 199.
2973	Info	GCP Account Synchronization Finished	Synchronize computers completed for GCP Account: <GCPaccountname> For details, see "Synchronize a GCP account" on page 203.
2974	Error	GCP Account Synchronization Failed	Deep Security Manager was unable to synchronize computers with GCP Account: <GCPaccountname> *<detailed_message>* For example: Root URL is not valid For details, see "Synchronize a GCP account" on page 203.
2975	Info	GCP Account Synchronization Requested	A request has been made to synchronize computers with GCP Account: <GCPaccountname> For details, see "Synchronize a GCP account" on page 203.

ID	Severity	Event	Description or Solution
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: *<detailed_message>* For example: Project <GCPprojectname>: 403 Required 'compute.machineTypes.list' permission for 'projects/<GCPprojectname>' For details, see "Synchronize a GCP account" on page 203.
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	
2996	Warning	XDR Certificate Update 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 Module Installation Started	The agent received a policy from Deep Security Manager where application control was selected, but detected that it did not have the application control engine installed or needed to update it, so it began to download it. This is

ID	Severity	Event	Description or Solution
			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	Either an administrator sent or the legacy REST

ID	Severity	Event	Description or Solution
		Control 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	An administrator applied a new ruleset, but some of the

ID	Severity	Event	Description or Solution
		some running processes on restart	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, 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 543.) 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 543.)
7042	Info	Application Control Software Inventory Deleted	
7043	Info	A computer reboot is required to complete Application Control protection	

Application Control events

For general best practices related to events, see "About Deep Security event logging" on page 566.

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 717.

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 566.

To see the anti-malware events captured by Deep Security, go to **Events & Reports** > **Events** > **Anti-Malware Events**.

What information is displayed for anti-malware events?

These columns can be displayed on the Anti-Malware 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".)
- **Infected File(s):** The location and name of the infected file.
- **Tag(s):** Event tags associated with this event.
- **Malware:** The name of the malware that was found.
- **Action Taken:** Displays the results of the actions specified in the malware scan configuration associated with the event.
  - **Cleaned:**Deep Security successfully terminated processes or deleted registries, files, cookies, or shortcuts, depending on the type of malware.
  - **Clean Failed:** Malware could not be cleaned for a variety of possible reasons.
  - **Deleted:** An infected file was deleted.
  - **Delete Failed:** An infected file could not be deleted for a variety of possible reasons. For example, the file may be 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.
  - **Quarantined:** An infected file was moved to the identified files folder.
  - **Quarantine Failed:** An infected file could not be quarantined for a variety of possible reasons. For example, the file may be 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/Computer Editor > Anti-Malware > Advanced** tab) has been exceeded.

- **Access Denied:** Deep Security has prevented the infected file from being accessed without removing the file from the system.
- **Passed:** 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. Possible values are: Joke, Trojan, Virus, Test, Spyware, Packer, Generic, or Other. For information on these types of malware, see the anti-malware event details or see "About Anti-Malware" on page 312
- **Target(s):** 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."
- **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:** Image name of the Docker container where the malware was found.
- **Container Name:** Name of the Docker container where the malware was found.
- **File MD5:** The MD5 hash of the file.

List of all 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
9010	Error	File cannot be analyzed or quarantined (VM maximum disk space used to store identified files exceeded)
9011	Error	File cannot be analyzed or quarantined (maximum disk space used to store

ID	Severity	Event
		identified files exceeded)
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

Firewall events

For general best practices related to events, see "About Deep Security event logging" on page 566.

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. "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 403.)
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	

ID	Event	Notes
	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). A packet is dropped with this event when the packet header has the following configuration: • Fragment Offset = 0 (The fragment is the first in the packet) • Total length (maximum combined header length) < 120 bytes (the default allowed minimum fragment size) 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 239.)
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 239.)
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 443.
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 443.
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 443.
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 stateful has been enabled (in firewall stateful configuration) and an

ID	Event	Notes
	ICMP	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.
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.) 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:

ID	Event	Notes
		• "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 retransmitted packet in the sequenced data stream. Otherwise, the note is "prev-part". • "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 803.
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.

ID	Event	Notes
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.
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.

ID	Event	Notes
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 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	Double decoding exploit attempt (%25xx, %25%xxd, etc).

ID	Event	Notes
	Decoding Exploit	
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 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	

Intrusion prevention events

For general best practices related to events, see "About Deep Security event logging" on page 566.

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.

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

ID	Event	Notes
		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 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.
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	A client attempted to rollback to an earlier version of the SSL protocol than

ID	Event	Notes
	Attempted to Rollback	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 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.
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	Double decoding exploit attempt (%25xx, %25%xxd, etc).

ID	Event	Notes
	Exploit	
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 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	

Integrity monitoring events

For general best practices related to events, see "About Deep Security event logging" on page 566.

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

ID	Severity	Event	Notes
			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 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".

ID	Severity	Event	Notes
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 Monitoring Rule	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 (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	

ID	Severity	Event	Notes
		wildcard was used.	

Log inspection events

For general best practices related to events, see "About Deep Security event logging" on page 566.

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 717.

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 566.

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").
- **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 969.

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 863.

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:

- "Activation Failed - Protocol Error" below
- "Activation Failed - Unable to resolve hostname" on the next page
- "Activation Failed - No agent/appliance" on the next page
- "Activation Failed - Blocked port" on the next page
- "Activation Failed - Maximum five protected computers" on page 791

Activation Failed - 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.

Agent-initiated communication

When the agent uses agent-initiated communication, you need to activate the agent from the agent computer. (See "Activate an agent" on page 986.)

When using Deep Security as a Service, agent-initiated communication is the recommended communication directionality.

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 106 and "Create a firewall rule" on page 422.)

Activation Failed - 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 are a Deep Security as a Service user or 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 852.

Activation Failed - No agent/appliance

This error message indicates that the agent software has not been installed on the computer that you would like to protect.

Review "Deploy agents to your Amazon EC2 instances and WorkSpaces" on page 155.

Activation Failed - 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::AgentEventWriteHaveL
ock | 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
Agent-initiated communication	Deep Security Agent / Ephemeral port	Deep Security as a Service / 443
Manager-initiated communication	Deep Security Manager or Deep Security as a Service / 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, or Deep Security as a Service on 443.
- Allow inbound access to Deep Security Agent on port 4118 if you're using Manager-initiated communication.

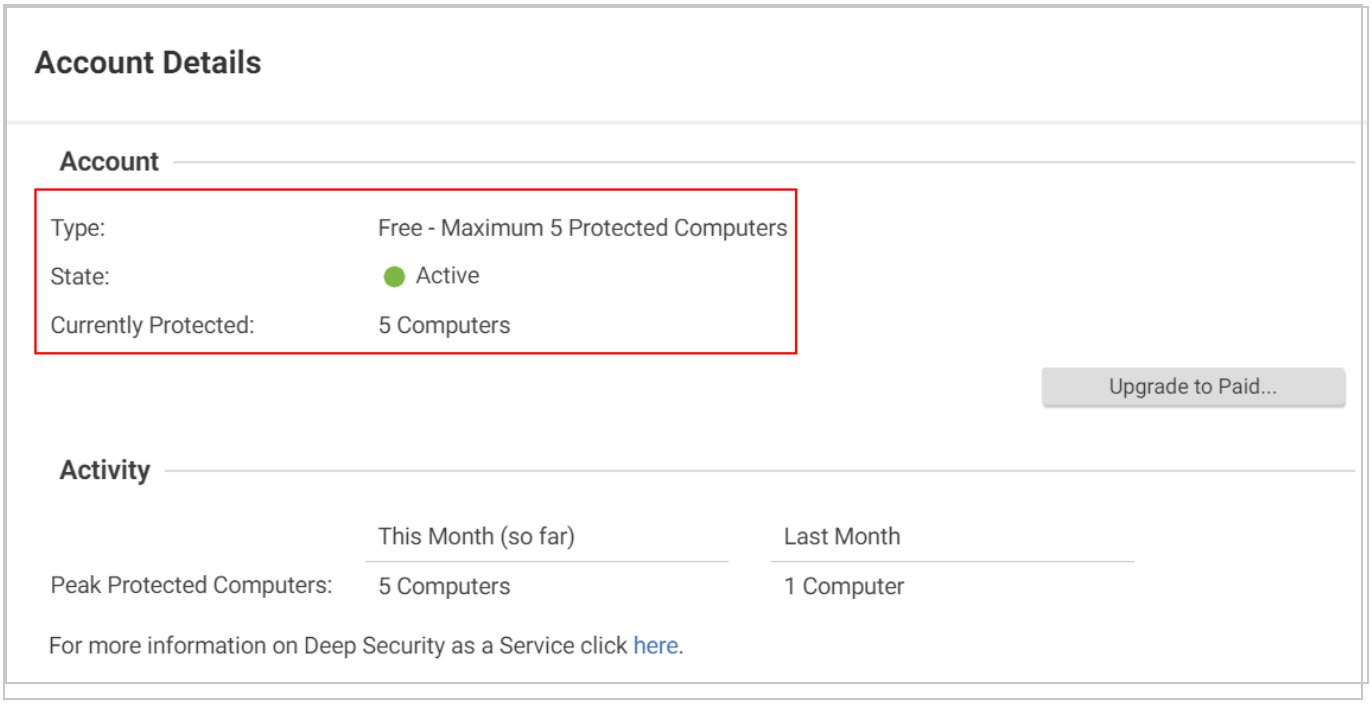
For details on ports, see "Port numbers, URLs, and IP addresses" on page 106.

Activation Failed - Maximum five protected computers

After your 30-day free trial for Deep Security as a Service is over, your account only supports five protected computers while it's in free status.

To confirm how many protected computers you already have:

1. Go to Your **Account Name > Account Details**.
2. Your status is displayed next to **Type** and the amount of **Currently Protected** computers.



To successfully activate another Deep Security Agent:

- Upgrade to a paid Deep Security as a Service account. See "Sign up for Deep Security as a Service" on page 120 for more information.
- Deactivate protected computers from the Deep Security Manager. Go to **Computers > Actions > Deactivate**.
- Delete your unused protected computers from the Deep Security Manger. Go to **Computers > Delete**.
- Shutdown your unused protected computers.

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 962.

Error: Anti-Malware Engine Offline

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" below
- "Agentless protection" on the next page

For an overview of the Anti-Malware module, see "About Anti-Malware" on page 312.

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 319.)
4. Deactivate and uninstall the agent before reinstalling and re-activating it. See "Uninstall Deep Security" on page 969 and "Activate the agent" on page 164 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 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:
   - `# sc query AMSP`
   - `# 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 following 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're using a Linux server, your kernel might not be supported. For more information, see "Error: Module installation failed (Linux)" on page 799.

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 and logs" on page 1075.

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 and logs" on page 1075.
   - Diagnostic package from the Deep Security Virtual Appliance.
   - vCenter support bundle for the effected VMs.

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. Unless you are using Deep Security as a Service, 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 106.
- 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. To confirm 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**.

Re-check 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 above steps, troubleshoot the issue with the solutions below:

- "Apply Intrusion Prevention best practices" below
- "Manage rules" below
- "Unassign application types from a single port" on the next page

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 406.

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:

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've 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**.

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 eight application types.

To resolve the issue, remove an assigned application type from a port:

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**.

[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).

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.

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**[3] **or Policy editor**[4] **> 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**.

---

[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).

3. View the results on the **General** tab of the protection module in the **Computer**[1] or **Policy editor**[2].

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 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 "Deep Security Agent Linux kernel support" on page 88.

Error: There are one or more application type conflicts on this computer

This 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]
```

[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).

```
[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, you will see the following message in the Events tab: *The Application Type Port List Misconfiguration has been resolved.*

Consolidate ports

1. Log on to Deep Security Manager and go to **Policies > Rules > Intrusion Prevention Rules**.
2. Search for **Web Server Common** in the search box in the 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**.

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 click to clear **Inherit** .
4. Click **OK**.

Check the IPS rule 1000128.

1. Right-click **Application Type Properties**.
2. Click to clear **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 852.

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 449.

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 216.
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: 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
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 848 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**.
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.
- 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.

---

[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).

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.

[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).

- 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**[1], 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.

For more information on reconnaissance scans, see "Firewall settings" on page 436.

Configure proxies

Configure proxies

You can configure proxies between various Trend Micro servers and services.

In this topic:

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.

---

[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 the **Proxy Protocol**, select either **HTTP**, **SOCKS4**, or **SOCKS5**. Not all protocols are supported by all components. See "Supported proxy protocols" below for details.
5. In the **Address** and **Port** fields, enter the IP address or URL of the proxy as well its port (by default 8080 or 80 for HTTP; 3128 for the Squid HTTP proxy; 443 for HTTPS; 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 table lists the proxy protocols supported by the Trend Micro services and clients. You'll need this information when registering a proxy, and when configuring 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
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

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 called Active Update).

Note: The **agents and appliances**[1] will only use the proxy if their assigned relay is not available, and they've been granted explicit permission to access the primary update source.

1. Make sure you're using Deep Security Agent 10.0 or later. Only 10.0 and later supports connections through a proxy.
2. "Register a proxy in the manager" on page 807.
3. In Deep Security Manager, click the **Administration > System Settings > Proxies** tab.

[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.

4. 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.
5. Click **Save**.
6. Restart the agents.

Connect to Deep Security Manager via proxy

Agents connect to Deep Security as a Service during agent activation and heartbeats. There are two methods to connect an agent to Deep Security as a Service via a proxy.

Connect an agent to the manager via a proxy using a deployment script

1. Make sure you're using Deep Security Agent 10.0 or later. Only 10.0 and later supports connections through a proxy.
2. "Register a proxy in the manager" on page 807.
3. In the top right-hand corner of Deep Security as a Service, 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:

```
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:

```
/opt/ds_agent/dsa_control -u myUserName:MTPassw0rd

/opt/ds_agent/dsa_control -x dsm_proxy://squid.example.com:443
```

Notes:

- Make sure the proxy uses a supported protocol. See "Supported proxy protocols" on page 808.
- For details on `dsa_control` and its `-u` and `-x` options, see "dsa_control" on page 973.
- Repeat these commands on each agent that needs to connect through a proxy to the manager.
- Run the following 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 methods 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're using Deep Security Agent 10.0 or later. Only 10.0 and later supports connections through a proxy.
2. "Register a proxy in the manager" on page 807
3. In the top right-hand corner 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 these 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:

```
/opt/ds_agent/dsa_control -w myUserName:MTPassw0rd

/opt/ds_agent/dsa_control -y relay_proxy://squid.example.com:443
```

Notes:

- Make sure the proxy uses a supported protocol. See "Supported proxy protocols" on page 808.
- For details on `dsa_control` and its `-w` and `-y` options, see "dsa_control" on page 973.
- Repeat these commands on each agent that needs to connect through a proxy to the manager.
- Run the following 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 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 807.
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 215.

Your agents now connect to the Smart Protection Network through a proxy.

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 1013.

  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 973.

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 807.

Proxy server use

To view and edit the list of available proxies, go to **Administration > System Settings > Proxies**.

- **Primary Security Update Proxy used by Agents, Appliances, and Relays:** For information on this setting, see "Connect to the 'primary security update source' via proxy" on page 808.

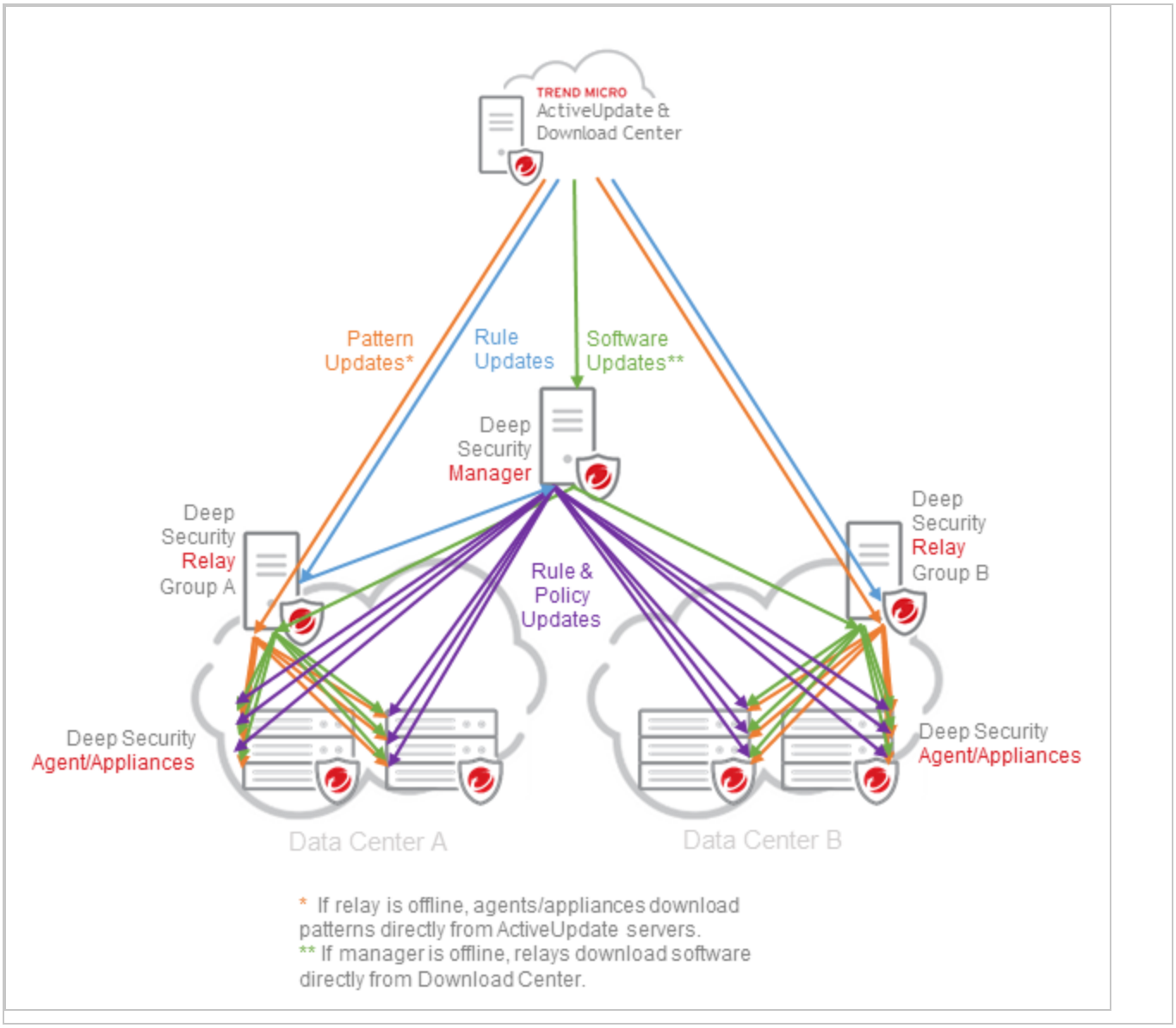
Configure relays

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.



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 821.

Deploy additional relays

Under most circumstances, the Deep Security-provided relays should be enough; however, there are some circumstances that might require you to install additional ones.

When deploying relays, you must:

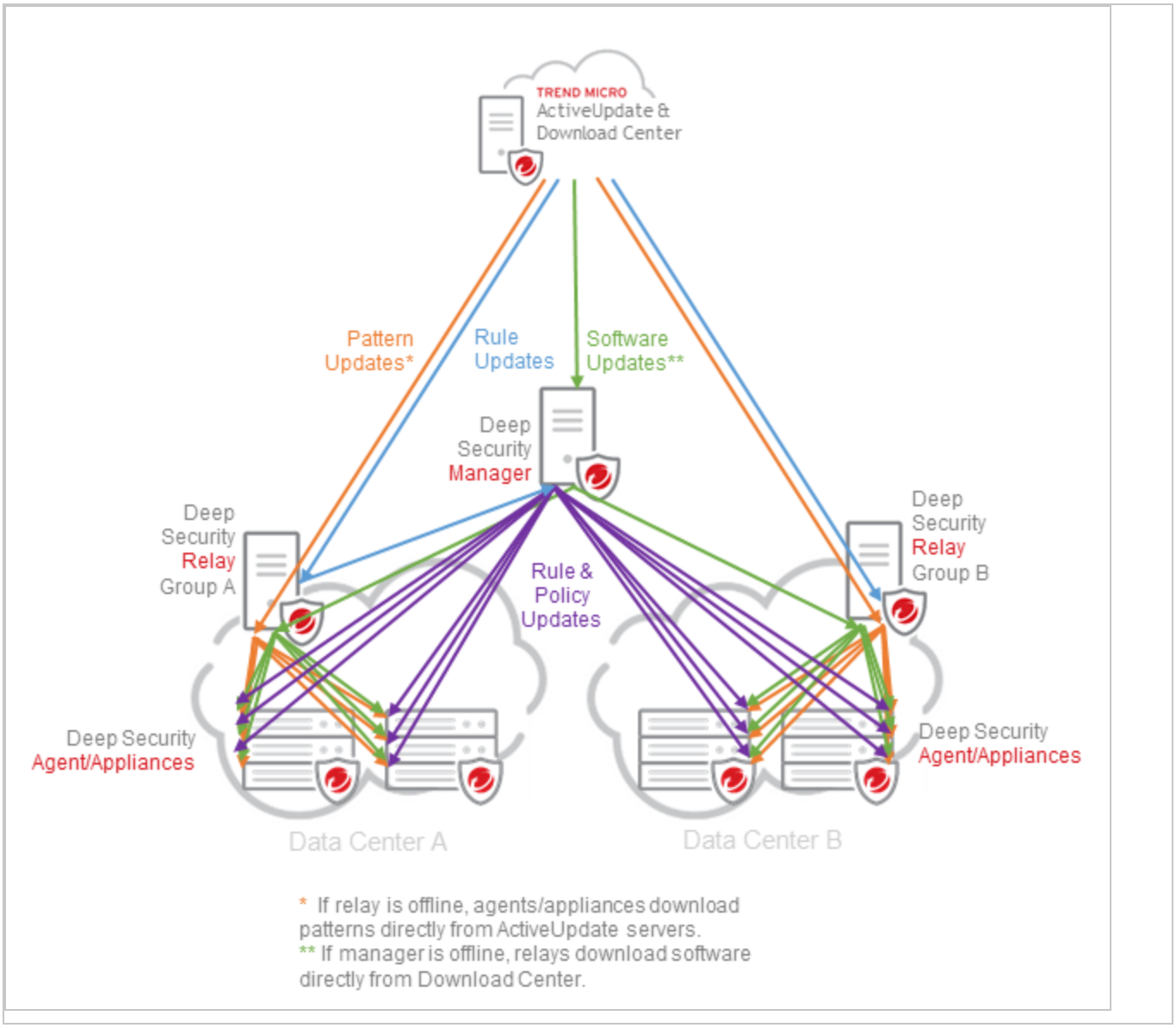
1. "Plan the best number and location of relays" on the next page
2. "Configure the update source" on page 819
3. "Configure relays" on page 820

Warning: Too many relays on your network will *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 normal Deep Security Agent. See "Remove relay functionality from an agent" on page 823.

Plan the best number and location of relays

The optimal number and placement of relays depends on:

- "Geographic region and distance" on the next page
- "Network architecture and bandwidth limits" on the next page
- "Usage of Application Control shared rulesets through a proxy connection" on page 819



Geographic region and distance

Ideally, each geographic region should have its own relay group with at least 2 relays.

Agents should use local relays in their **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 2 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 1 "parent" relay group might use the Internet connection; sub-groups 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 (instead of more relays on shared servers). See "Deep Security Agent and Relay sizing" on page 105.

Usage of Application Control shared rulesets through a proxy connection

If you will use shared Application Control rulesets and agents connect through a proxy, you might want to **add more relays to handle large rulesets** and improve performance. See Deploy Application Control rulesets via relays and "Deep Security Agent and Relay sizing" on page 105.

Configure the update source

Before you set up relays, you should 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. Don't 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. Usually, 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:

- **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. Usually, Deep Security as a Service provides relays. But if you don't want to use them, deselect **Use the Primary Tenant Relay Group as my Default Relay Group**.

   > **Note:** If this option is deselected, when you click **Administration > Updates > Relay Groups**, then the relay group name will be "Default Relay Group", not "Primary Tenant Relay Group".

5. Configure an **Alternate software update distribution server(s) to replace Deep Security Relays** to specify an alternative source for *software* updates, noting that *security* updates will 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
   - the address and port of the relays hosted by Deep Security as a Service, namely `https://relay.deepsecurity.trendmicro.com:443`. These relays will act as your software update source, while your own relays must act as the security update source.

Configure relays

After determining where and how many relays you should have, and what update sources they should use, you can:

1. "Create relay groups" on the next page
2. "Enable relays" on page 822
3. "Assign agents to a relay group" on page 822
4. "Connect agents to a relay's private IP address" on page 823

Create relay groups

Relays must be organized into relay groups. The relay groups themselves can be further organized into hierarchies.

Relays for Deep Security as a Service are in a relay group named "Primary Tenant Relay Group." To use it, verify that your computers can connect to the listening port number on Deep Security as a Service. If you need more relay groups (see "Plan the best number and location of relays" on page 817), you can create more.

Tip: To minimize latency and external/Internet bandwidth usage, create a relay group for each geographic region and/or network segment.

1. Go to **Administration > Updates > Relay Management**. A **Relay Group Properties** pane appears on the right.
2. Click **New Relay Group**.
3. Type a **Name** for the relay group.
4. In **Update Source**, select either Primary Security Update Source or, if this will be a sub-group (child), the name of the parent relay group.

   Note: The Default Relay Group is not included in the list of update sources, and therefore cannot be configured as a parent.

   Tip: Select 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 the **Update Source Proxy**. For details, see "Connect to the 'primary security update source' via proxy" on page 808.

   Unlike other relay groups, "Default Relay Group" uses the same proxy as Deep Security Manager, and cannot be configured. Deep Security as a Service provides relays in the "Primary Tenant Relay Group" which acts as your default relay group. You cannot configure an update source proxy for the relays provided by Deep Security as a Service.

> **Note:** If this relay group usually connects to a parent relay group, then the sub-group **won't** 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 819.

Enable relays

1. Make sure the relay computer meets the requirements. See "Deep Security Agent and Relay sizing" on page 105 and "Deep Security Relay requirements" on page 105.
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 107.
3. If the relay must connect through a proxy, see "Connect to the 'primary security update source' via proxy" on page 808.
4. Deploy an agent on the chosen computer. See "Get Deep Security Agent software" on page 144 and "Install the agent" on page 146.
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. Select the relay group into which the relay will be placed. If a relay group does not exist, create one.
   e. Click **Add Relay**.
   f. In **Available Computers**, select the agent you just deployed.
   g. Click **Enable Relay and Add to Group**.

   The agent is enabled as a relay and is displayed with a relay icon ().

1. > **Tip:** To minimize latency and external/Internet bandwidth usage, group together relays that are in the same geographic region and/or 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.

> **Tip:** 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**.

> **Note:** If your relay group's private IP changes, you must manually update this setting. It will not be updated 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" below 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 826.

For a list of the events, see "Agent events" on page 712 and " System events" on page 717.

Also on this page:

- "Computer errors" on page 830
- "Protection module status" on page 831
- "Perform other actions on your computers" on page 832
- "Computers icons" on page 835
- "Status information for different types of computers" on page 835

Status column - computer states

State	Description
Activated	The agent is activated. See "Perform other actions on your computers" on page 832.
Discovered	Computer has been added to the computers list via the discovery process. (See "Discover computers" on page 170.)

State	Description
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**. 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. Verify that firewall settings allow the required port numbers, and that the computer is powered on. If you use Deep Security as a Service, also see "Activate and protect agents using agent-initiated activation and communication" on page 852.
Online	The agent is online and operating as expected.
Unknown	No attempt has been made to determine whether an agent is present.

[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).

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 Paused	A baseline rebuild has been 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

State	Description
	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 In Progress	The instruction to cancel a manually-initiated Malware Scan has been sent.
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	The instruction to perform a manually-initiated Malware Scan has not yet

State	Description
Scan Pending	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 Pending (Offline)	The agent is currently offline. The manager will initiate the cancellation of a quick malware scan when communication is reestablished.
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.

State	Description
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 Configuration Pending (Heartbeat)	An instruction to update the configuration to match the policy changes will 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	An instruction to perform a software upgrade is queued to be sent.

State	Description
(Pending)	
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. 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 Required	The agent is currently activated by another Deep Security Manager.
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	Software changes detected on the file system exceeded the maximum amount.

State	Description
change limit reached	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. See "Reset Application Control after too much software change" on page 558.

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.
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 164
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. **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 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 954.
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.

Action	Description
Clear Warnings/Errors	Use this command to clear all warnings and errors for the computer. This command is useful in these situations: • If the agent for the computer has been reset locally • 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 951).
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 221.
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. **Note:** This action will not un-assign any rules that were assigned 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" on page 322.
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. **Note:** Quick Scan is only available on-demand. You cannot

Action	Description
	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**. **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. **Note:** New 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 449.
Rebuild Integrity	Rebuilds a baseline for Integrity Monitoring on this 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).

[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
Baseline	
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 582.
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

 Docker host (physical computer)

 Azure virtual machine with Docker

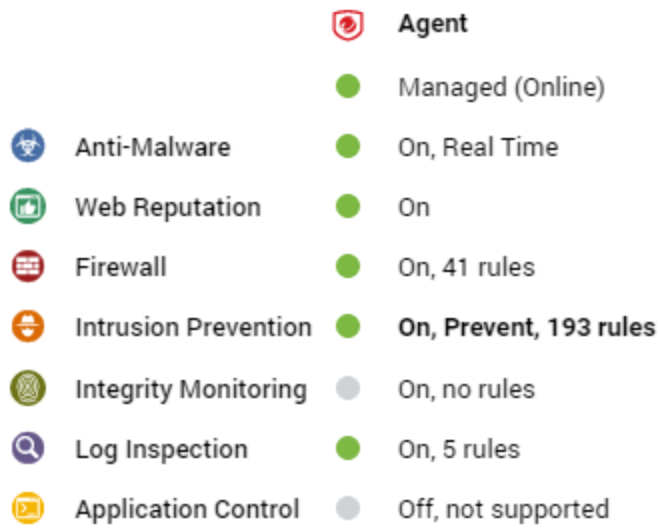
 Amazon EC2 with Docker

 Amazon WorkSpace (started)

Status information for different types of computers

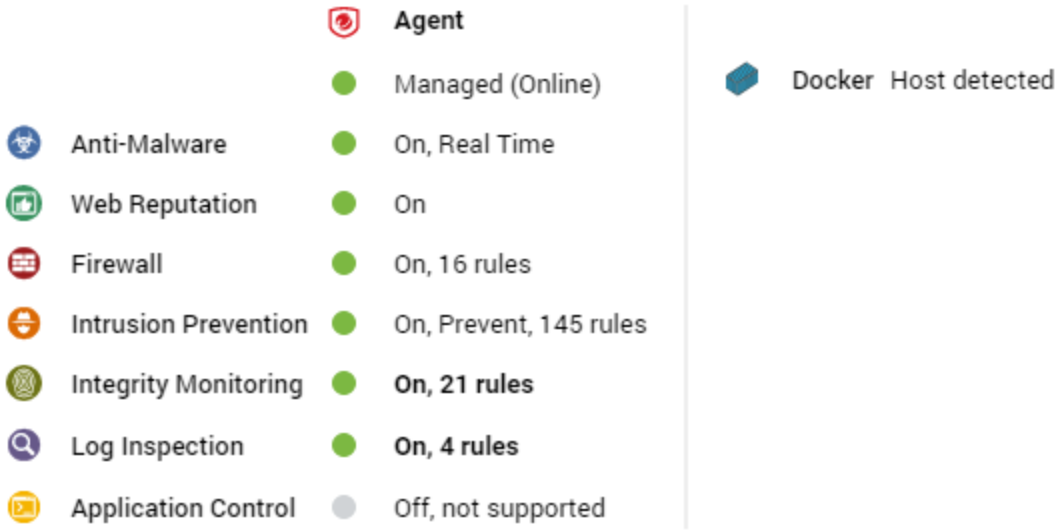
Ordinary computer

The preview pane for an ordinary computer displays the presence of an agent, it status, and the status of the protection modules.



Docker hosts

The preview pane for a Docker host displays the presence of an agent and its status, the status of the protection modules, and the Docker status.



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 (in a Deep Security as a Service environment, for example) 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. Go to Deep Security Manager.
2. Click **Administration** at the top.
3. On the left, expand **Updates > Software > Agent Version Control**.

   All the agent platforms appear in the main pane.

4. (Optional) Use the **Show/Hide Platforms** section on the right to restrict the agent platforms that are visible.
5. 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 1013.

Column	Description
PLATFORM	This column lists the platforms for which Deep Security Agent software is available.

Column	Description
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: • **Latest**: Indicates to use the latest agent software build , 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 life cycle policy" on page 60. • **Latest LTS**: (default) Indicates to use the latest long-term support (LTS) software build . Latest LTS can be the original LTS release, or can be an update to the original LTS release. Any FRs 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 life cycle policy" on page 60. • *<agent_version>* for example, `11.0.0.760`: Indicates to use a specific agent version. Other agents are ignored. **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 63.

Column	Description
RESULTING AGENT	This column shows the agent that will be deployed based on your selection under **VERSION CONTROL**. If the column shows an **N/A (Removed from inventory)** message, it's because Trend Micro deemed the agent unsuitable for deployment and removed it.

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 1023.

Agent version control FAQs

Do I need to update my deployment scripts to use this feature?

Yes.

To update your deployment scripts:

1. In Deep Security as a Service, go to **Support > Deployment Scripts** and generate new deployment scripts. For instructions, see "Use deployment scripts to add and protect computers" on page 1013.
2. Re-distribute and re-run the new scripts as necessary.

The latest deployment scripts pass additional information to Deep Security as a Service (for example, 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 LTS**. 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 965.

- 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

A 'heartbeat' is a periodic communication between the Deep Security Manager and agent. During a heartbeat, the manager collects this information:

- the status of the drivers (on- or off-line)
- the status of the agent (including clock time)
- 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 sub-policy, or on an individual computer.

You can configure the following properties of the heartbeat:

- **Heartbeat Interval:** How much time 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 three causes the manager to trigger an alert on the fourth missed heartbeat.)

  Note: 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 setting should be set to "unlimited".

- **Maximum change (in minutes) of the local system time on the computer between heartbeats before an alert is raised:** For agents that are capable of detecting changes to the system clock (Windows agents only) these events are reported to the manager as 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: Once a **Computer-Clock-Changed** alert is triggered, it must be dismissed manually.

- **Raise Offline Errors For Inactive Virtual Machines:** Sets whether an offline error is raised if the virtual machine is stopped.

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: For Deep Security as a Service, agent-initiated communication is enabled by default and we strongly recommend that you do not change this setting.

---

[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).

Configure whether the agent or the manager initiates communication. 'Communication' includes the heartbeat and all other communications. The following options are available:

Bidirectional: The agent normally 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 107.) 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.
- **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 agent heartbeats. (See "Deep Security port numbers" on page 107.) 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 852.

Note: 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 will accept 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 these settings:

action: force allow or bypass
priority: 4 - highest
packet's direction: incoming

frame type: IP
protocol: TCP
packet's destination port: agent's listening port number for heartbeat connections from the manager, or a list that includes the port number. (See agent listening port number.)

While these settings are in effect, the new rule will replace the hidden rule. You can then type packet source information for IP or MAC addresses, or both, to restrict traffic to the computer.

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", or "Bidirectional"), or choose "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** to apply the changes.

Note: 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. If you need to know the cipher suites supported by the Deep Security Manager, contact Trend Micro.

The cipher suites consist of a key exchange asymmetric algorithm, a symmetric data encryption algorithm and a hash function.

[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).

Deep Security Agent 9.5 cipher suites

Deep Security Agent 9.5 (without SPs, patches, or updates) supports these TLS 1.0 cipher suites:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

Deep Security Agent 9.5 SP1 - 9.5 SP1 Patch 3 Update 2 supports these cipher suites:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

Deep Security Agent 9.5 SP1 Patch 3 Update 3 - 8 supports these cipher suites:

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

Deep Security Agent 9.6 cipher suites

Deep Security Agent 9.6 (without SPs, patches, or updates) - 9.6 Patch 1 supports these TLS 1.0 cipher suites:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

Deep Security Agent 9.6 Patch 2 - 9.6 SP1 Patch 1 Update 4 supports these cipher suites:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

Deep Security Agent 9.6 SP1 Patch 1 Updates 5 - 21 supports these cipher suites:

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- 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 up to Update 15 supports these TLS 1.2 cipher suites:

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256

Deep Security Agent 10.0 Update 16 and later updates supports these TLS 1.2 cipher suites, out-of-box:

- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256

Deep Security Agent 11.0 cipher suites

Deep Security Agent 11.0 up to Update 4 supports these cipher suites:

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256

Deep Security Agent 11.0 Update 6 and later updates supports these TLS 1.2 cipher suites:

- 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 12.0 and Deep Security Agent 20 cipher suites

- 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

Configure agents that have no internet access

If your agents or relays don't have access to the internet (also called "air-gapped agents"), then they won't be able to access several 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 features.

The Trend Micro Smart Protection Network security services are:

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 the above services, the agent and relay-enabled agent also 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 can't reach the services above, you have several solutions, described below.

Solutions

- Solution 1: "Use a proxy" below
- Solution 2: "Install a Smart Protection Server locally " below
- Solution 3: "Disable the features that use Trend Micro security services" on the next page

Use a proxy

If your agents or relay-enabled agents can't 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.

Note: 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 807

Install a Smart Protection Server locally

If your agents and relay-enabled agents can't connect to the internet, you can install a Smart Protection Server in your local area network (LAN) to which they *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 disseminated to your agents and relay-enabled agents.

If you decide to use this solution, remember that:

- Only the Smart Scan and Web Reputation features are supported with a local Smart Protection Server.
- Use the proxy solution if you need the behavior monitoring, predictive machine learning, and process memory scanning features. See "Use a proxy" above 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 on disabling these features, see "Disable the features that use Trend Micro security services" on the next page

To deploy a Smart Protection Server:

- install it manually. See the Smart Protection Server documentation for details.
  OR
- if your agents or relay-enabled agents are inside AWS, install it using an AWS CloudFormation template created by Trend Micro. See "Integrate with Smart Protection Server" on page 1049 for details.

Disable the features that use Trend Micro security services

You can disable the 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.

---

[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. From the **Configuration** drop-down 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, click the **Smart Feedback** tab.
  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 both options, namely, **Detect suspicious activity and unauthorized changes (incl. ransomware)** and **Back up and restore ransomware-encrypted files**.
  c. Click **OK**.

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 (443).

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: If you are using Deep Security as a Service, agent-initiated communication is enabled by default.

Enable agent-initiated activation and communication

Proceed with the following steps:

1. "Create or modify policies with agent-initiated communication enabled" below.
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 863.

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 1013 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 158). 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. Go to **Administration > System Settings > Agents**.
2. 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**.
3. 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 717 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. The event details list the existing agent version and the attempted upgrade version, along with the reason the upgrade failed. The reasons can be: • 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. • 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. • The agent was not upgraded automatically because a required Linux kernel support file was not found. • 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 146.
706	Software Update: Agent Software Upgraded	The upgrade was successful.
707	Software Update: Agent Software Upgrade	The upgrade was not successful. Refer to the event details for more information about why it was not successful.

ID	Event	Description
	Failed	

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 requires certain iptables rules, as described below.

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" on the next page 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 842.)
- 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 816.)

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 106.

Prevent Deep Security from automatically adding iptables rules

You can prevent 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 Agent:

```
/etc/do_not_open_ports_on_iptables
```

Enable Managed Detection and Response

This feature is now GA and being rolled out to Deep Security as a Service customers. If it's not available in your account yet, it will be soon.

Trend Micro Managed Detection and Response (MDR) detects and responds to threats across email, servers, cloud workloads and networks. Deep Security can send server activity metadata and Integrity Monitoring data to the MDR server for correlation and visibility across physical, virtual, and cloud workloads. For more information about MDR, see XDR - Managed Detection and Response Service.

To enable Managed Detection and Response:

1. Obtain the following information from your Threat Investigation Center administrator:
   - Threat Investigation Center Server URL
   - Company GUID
   - Data Source GUID
   - (Optional) Proxy server address
2. Go to **Deep Security Manager > Administration > Managed Detection and Response**.
3. Click **Enable the MDR service** and fill in the following information:
   - **Server URL (for example: "https://[server]/")**: The Threat Investigation Center Server URL
   - **Company GUID**
   - **Data Source GUID**
4. If required, you can choose to use a proxy to access MDR. Select **When accessing MDR server, use proxy** and click **Edit** to specify the proxy server address provided by your Threat Investigation Center administrator.
5. Before saving, click **Test Connection** to make sure the Deep Security Manager is connected to TIC. If the connection fails, double-check that all the information entered is correct. If the connection passes, click **Save**.

Enable or disable agent self-protection

Note: The agent self-protection feature is only available for agents on Windows. It is not available on Linux.

Agent self-protection prevents local users from tampering with the agent. When enabled, if a user tries to tamper with the agent, a message such as "Removal or modification of this application is prohibited by its security settings" will be displayed.

To update or uninstall Deep Security Agent or Relay, or to create a diagnostic package for support (see "Create a diagnostic package and logs" on page 1075), you must temporarily disable agent self-protection.

Note: Anti-Malware protection must be "On" to prevent users from stopping the agent, and from modifying agent-related files and Windows registry entries. It isn't required, however, to prevent uninstalling the agent.

You can configure agent self-protection using either the 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. Click **Settings > General**.
3. In the **Agent Self-Protection** section, for **Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent**, select **Yes**.
4. For **Local override requires password**, select **Yes** and type an authentication password. The authentication password is highly recommended because it prevents unauthorized use of the dsa_control command. After specifying the password here, it must be entered with the dsa_control command using the `-p` or `--passwd=` option whenever a command is run on the agent.
5. Click **Save**.
6. To disable the setting, select **No**. 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).

Configure self-protection using the command line

You can enable and disable self-protection using the command line. The command line has one limitation: you cannot specify an authentication password. You'll need to use Deep Security Manager for that. See "Configure self-protection through Deep Security Manager" on the previous page for details.

1. Log in to the Windows agent locally.
2. Open the Command Prompt (`cmd.exe`) as Administrator.
3. Change the current directory to the Deep Security Agent installation folder. (The default install folder is shown below.)

   ```
   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 specified previously in Deep Security Manager. For details on this password, see "Configure self-protection through Deep Security Manager" on the previous page.

Are "Offline" agents still protected by Deep Security?

Agents showing as "Offline" in the Deep Security Manager are still being protected according to their last known configuration. However, they will not 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 1064.

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 171, "Add a Microsoft Azure account to Deep Security" on page 187, or "Add a Google Cloud Platform account" on page 199). 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 weeks 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" on the next page (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" on the next page (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:

---

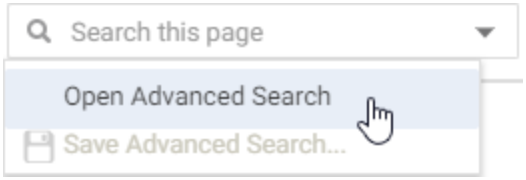
[1] You can change these settings for a policy or for a specific computer. To change the settings for a policy, go to the Polices page and double-click the policy that you want to edit (or select the policy and click Details). To change the settings for a computer, go to the Computers page and double-click the computer that you want to edit (or select the computer and click Details).

- "2953 - Inactive Agent Cleanup Completed Successfully" below
- "251 - Computer Deleted" below
- "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. 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.

Agent-initiated activation (AIA)

In addition to activating new agents on Deep Security Manager (such as via a cloud connector or manually adding a new computer on **Computers**), but you can also (or instead) allow agents to automatically activate themselves. See also "Activate and protect agents using agent-initiated activation and communication" on page 852.

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.

- **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 via 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 via **Computers > Add Account**.

- **Reactivate unknown Agents:** Reactivate deleted (but previously activated) computers as new computers if they connect again; do not assign the original computer's assigned policies or rules. 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 860.

  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 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 853.

Inactive Agent Cleanup

If you have many offline computers (that is, they are not communicating with Deep Security Manager), and they don't need to manage them anymore, you can automatically remove them from **Computers** via 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 860.

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 Data Collection Notice.

Note: This feature is supported with Deep Security Agent 12.5.0.1001 or later.

Deep Security Notifier

The Deep Security Notifier is a Windows System Tray application that communicates the state of the Deep Security Agent and Deep Security Relay to client machines. The notifier displays popup user notifications when the Deep Security Agent begins a scan, or blocks malware or 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 system tray. 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.

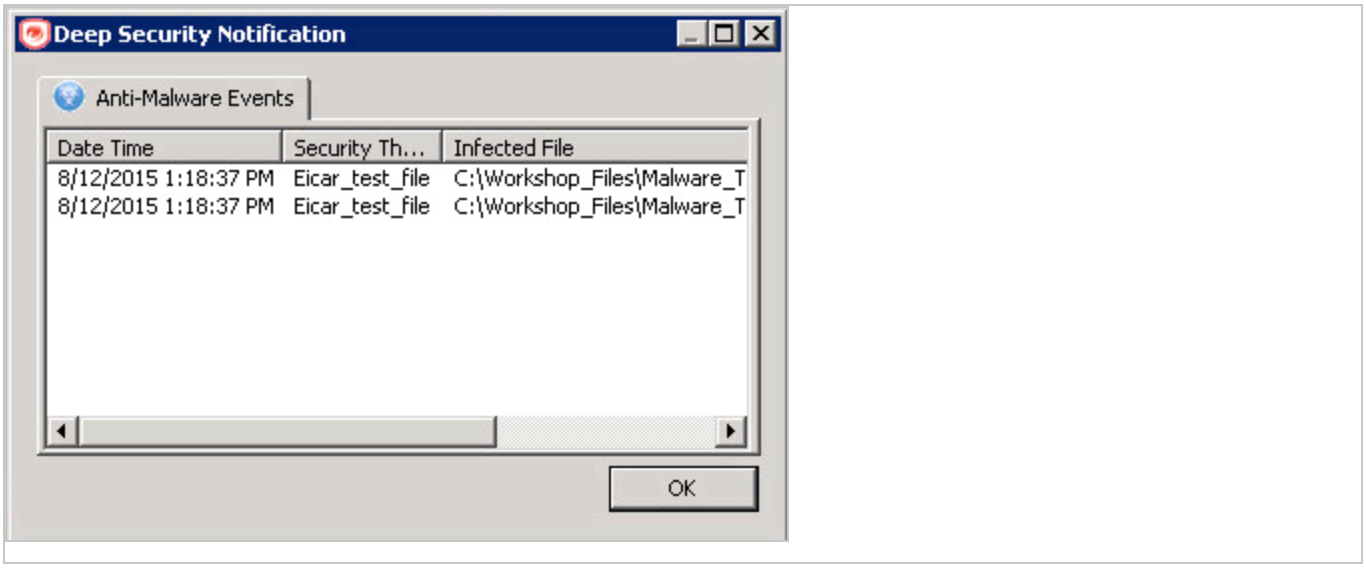
Note: On computers running a relay-enabled agent, the notifier displays the components that are being distributed to agents or appliances, *not* which components are in effect on the local computer.

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 system tray.

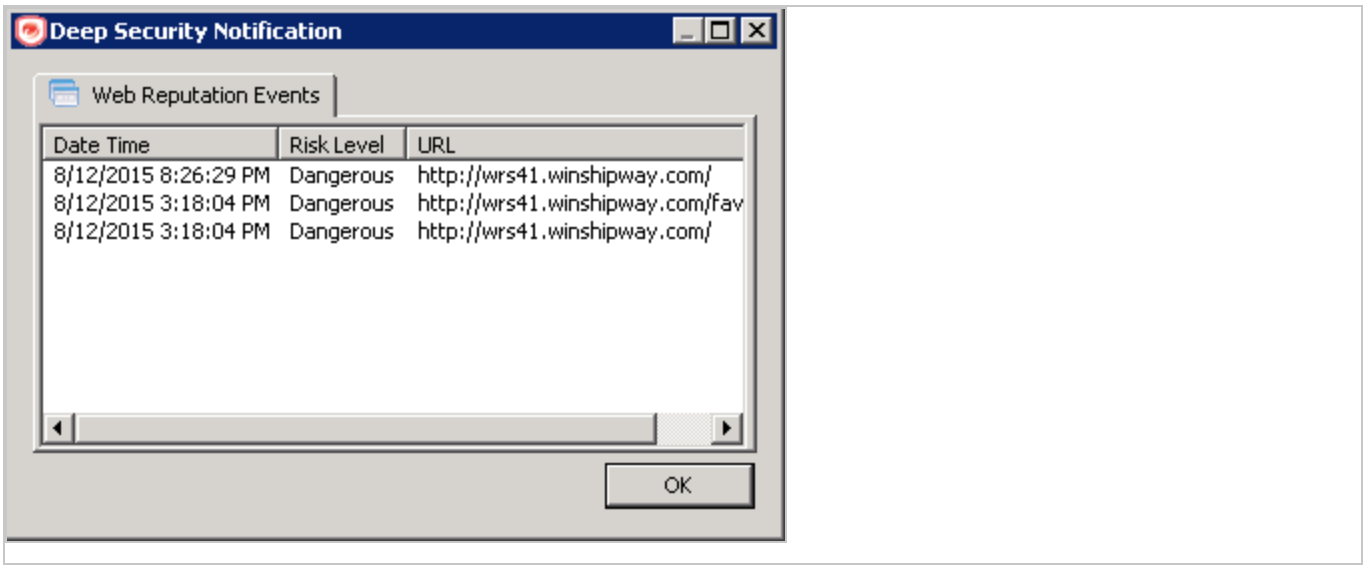
If malware is detected, the notifier displays a message in a system tray popup similar to the following:

If the user clicks on the message, a dialog box with detailed information about anti-malware events is displayed:

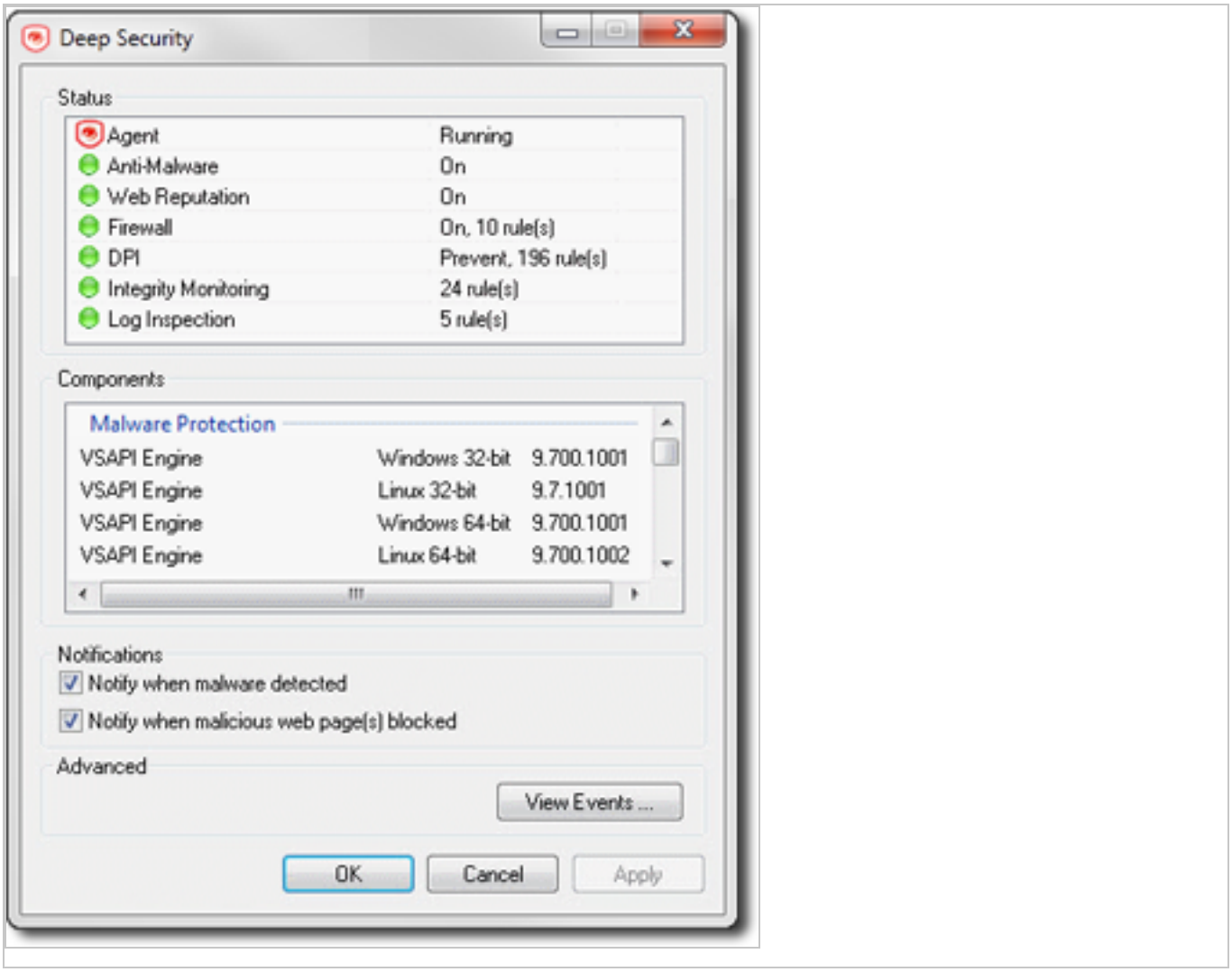


When a malicious web page is blocked, the notifier displays a message in a system tray popup similar to the following:

If the user clicks on the message, a dialog box with detailed information about web reputation events is displayed:

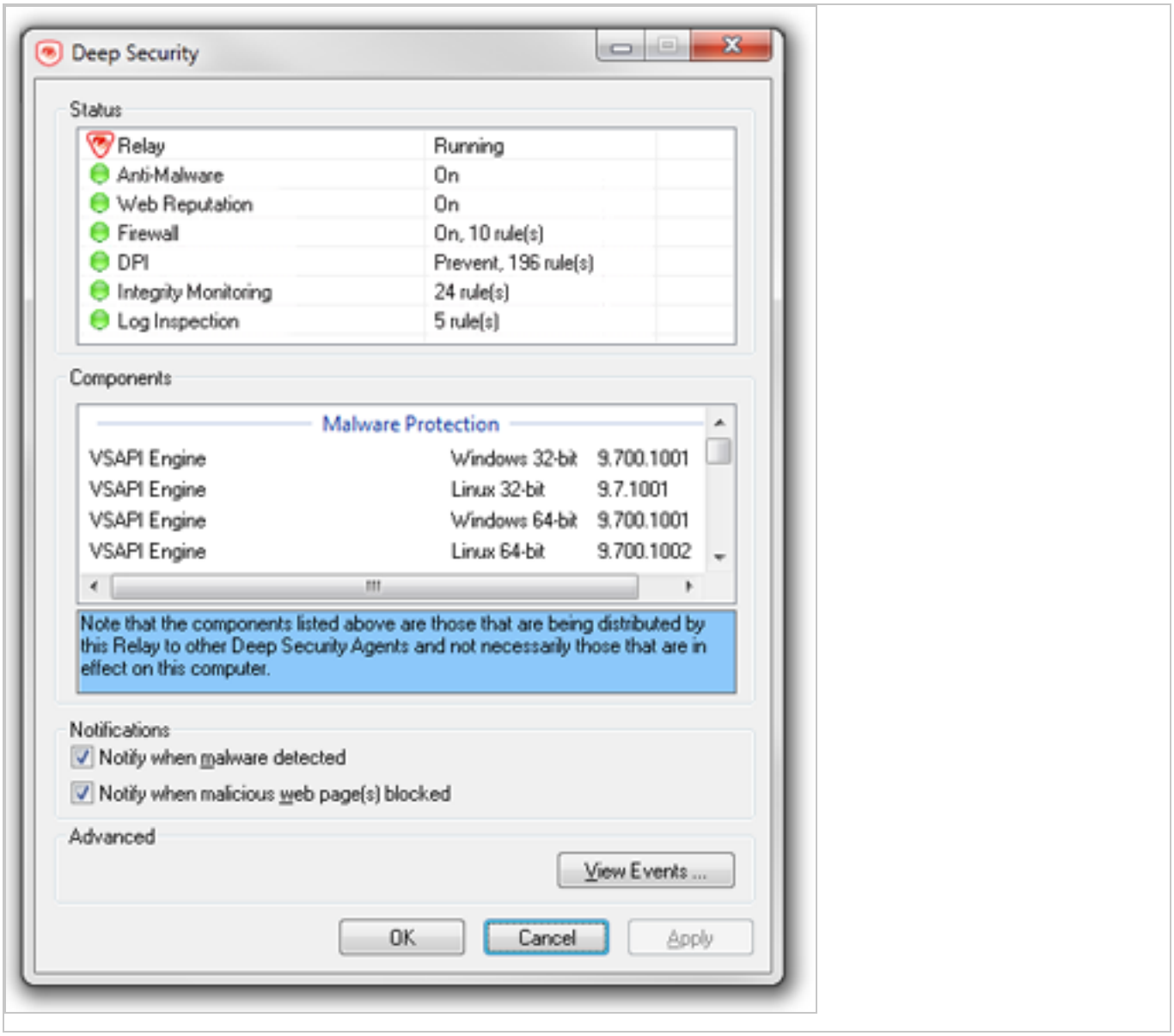


The notifier also provides a console utility for viewing the current protection status and component information, including pattern versions. The console utility allows the user to turn on and off the popup notifications and access detailed event information.



Tip: 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.



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 "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 874.
- **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 890.

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 943).
   - **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**.

     Note: The Deep Security Manager comes 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 943

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 944.
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:

   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 List view or Summary view.
   - **Computers List:** How often to refresh the data on the Computers page.

     Note: The **Last Successful Update** column value will not be 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 Tag(s). 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 computer(s). 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 computer(s). 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 will determine if the search results are kept if you navigate away from and return to the page.
- **Number of items to show on a single page:** Screens that display lists of items will 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 the 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 will appear at the top of the display informing you that only a portion of the results are being displayed.

Note: Increasing these values will affect Deep Security Manager performance.

Reports

- **Enable PDF Encryption:** When this option is selected, reports exported in PDF format will be 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 892.

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**.

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 comes preconfigured with two 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.

Note: Depending on the level of access granted, controls in Deep Security Manager will be either visible and changeable, visible but disabled, or 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 882.

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 and itemize what Deep Security objects those roles will require access to and what the nature of that access will be (viewing, editing, creating, and so on). Once you have created your roles, you can then begin 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.

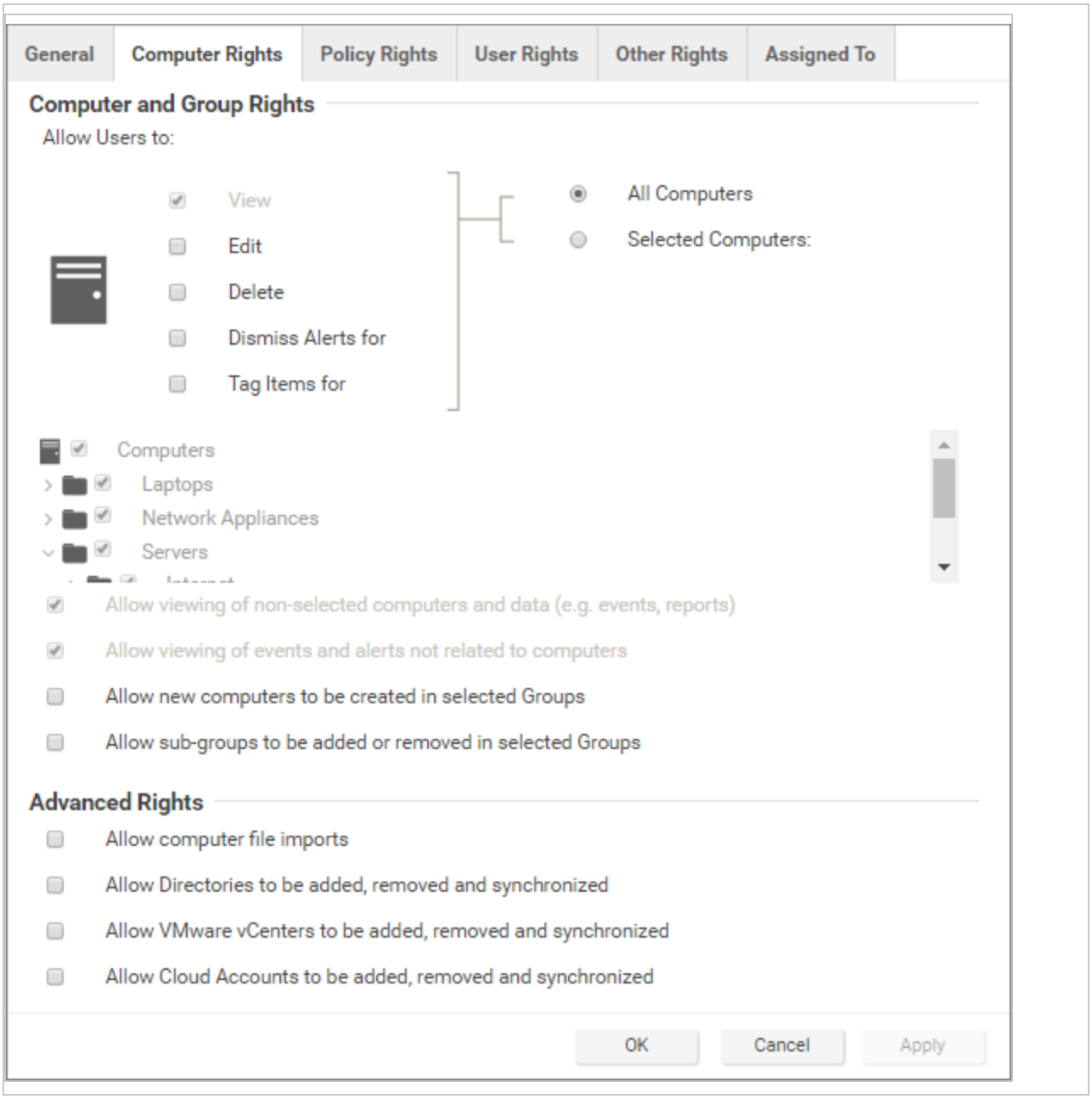
Clicking **New** () or **Properties** () displays the **Role properties window** with six tabs (**General, Computer Rights, Policy Rights, User Rights, Other Rights,** and **Assigned To**).

Add or edit a role

1. In Deep Security Manager go to **Administration > User Management > Roles**.
2. Click **New** to add a new role or double-click an existing role to edits its settings.
3. Specify the general properties for the role, including:
   - **Name:** The name of the role, which will appear on the Roles page and in the list of available roles when adding a user.
   - **Description:** (Optional) A description of the role.
   - **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), or both.

     Note: To enable the legacy SOAP and REST Web service APIs, go to **Administration > System Settings > Advanced > SOAP Web Service API**.

4. Use the **Computer Rights** pane to confer viewing, editing, deleting, alert-dismissal, and event tagging rights to users in a role. These rights can apply to all computers and computer groups or they can be restricted to only certain computers. If you wish to restrict access, select the **Selected Computers** radio button and put a check next to the computer groups and computers that users in this role will have access to.
5. **Note:** These rights restrictions will affect not only the user's access to computers in Deep Security Manager, but also what information is visible, including events and alerts. As well, email notifications will only be sent if they relate to data that the user has access rights to.



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)

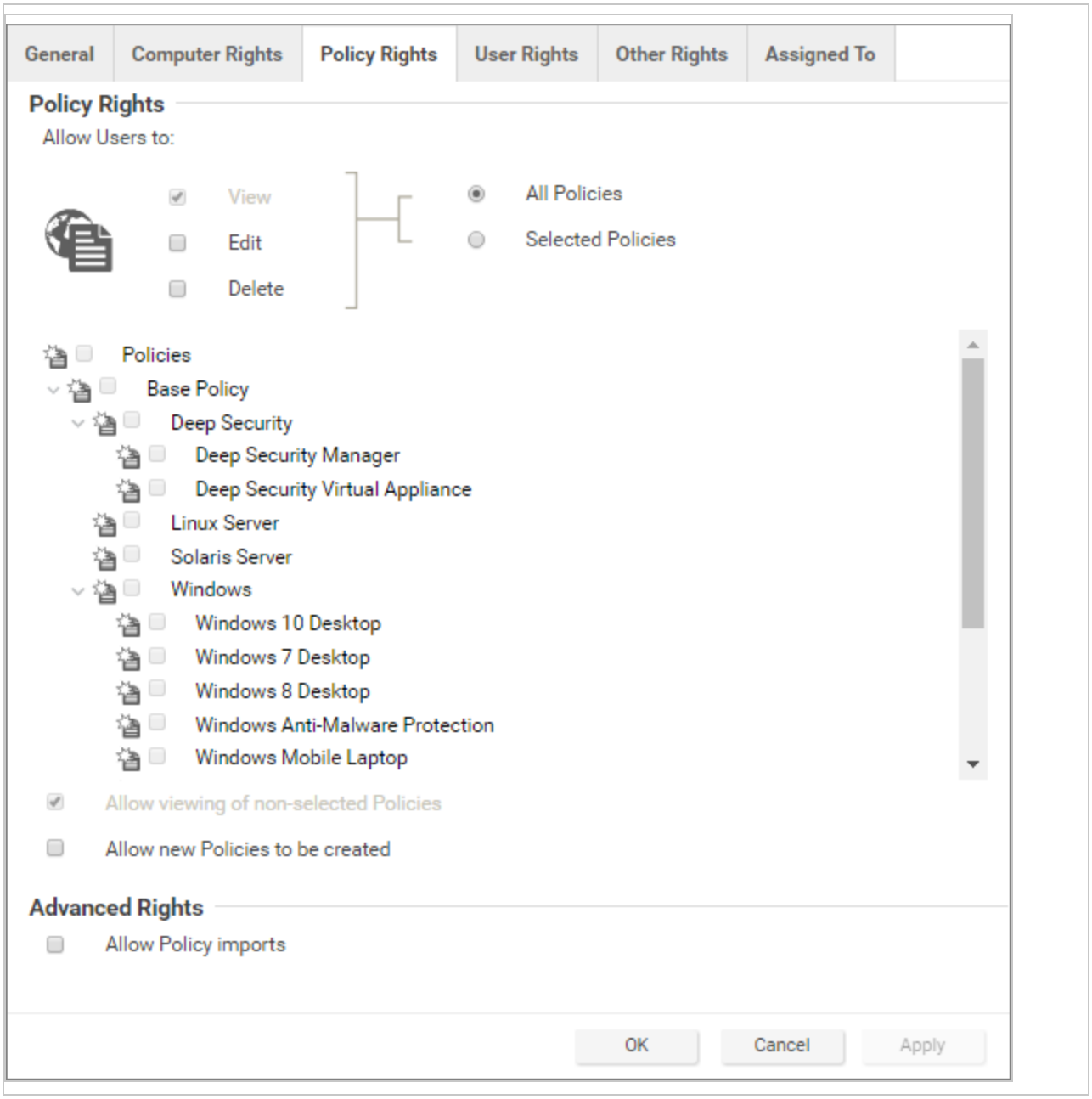
> **Note:** The previous two settings affect the data that users have access to. Although the ability of a user to make changes to computers have been restricted, these two settings control whether they can see information relating to computers they don't otherwise have access to. This includes receiving 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 they have access to.

You can also enabled 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. (Not available with Deep Security as a Service)
- **Allow Cloud Providers to be added, removed, and synchronized:** Allow Users in this Role to add, remove, and synchronize Cloud Providers. (Not available with Deep Security as a Service)

6. 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 a check mark next to the policies that users in this role will have access to.



When you allow rights to a policy that has "child" policies, users automatically get rights to the child policies as well.

Two basic options are available:

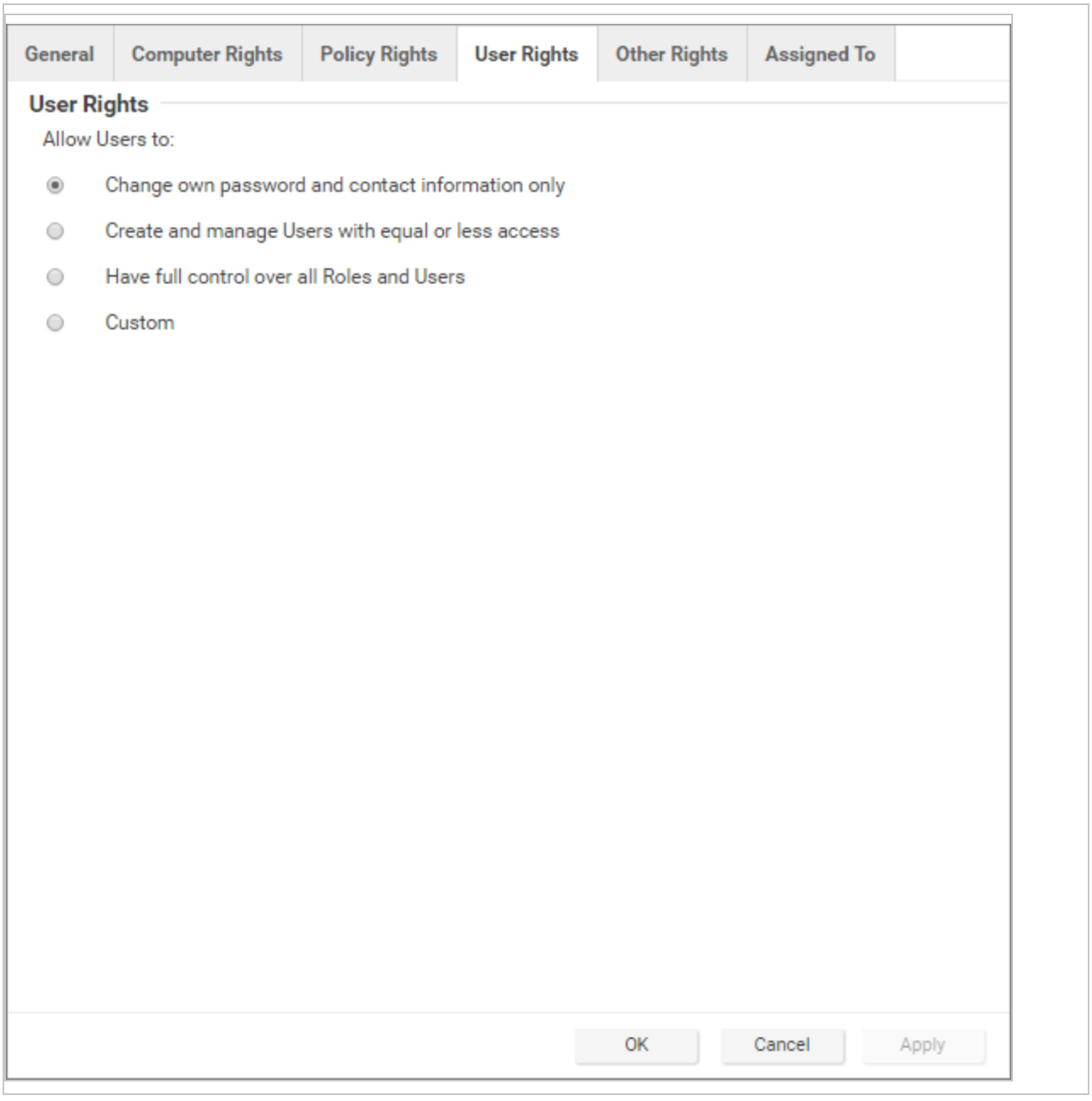
- **Allow viewing of non-selected Policies:** If users in this role have restricted edit or delete rights, you can still allow them to view but not change information about other policies by checking this box.

- **Allow new Policies to be created:** Set this option to allow users in this role to create new policies.

You can also enabled this 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.

7. The options on the **User Rights** tab allow you to define permissions for administrator accounts.



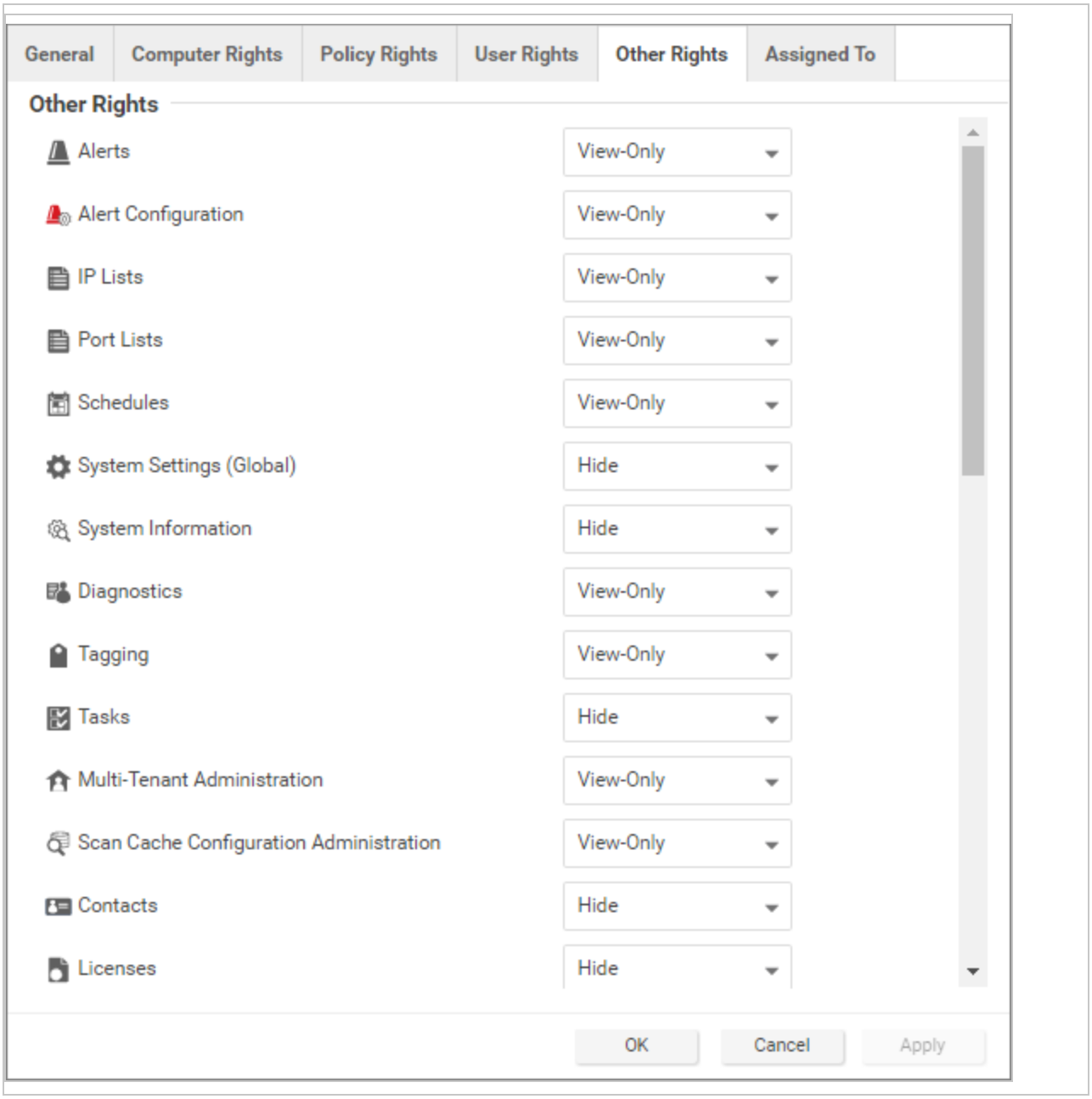
- **Change own password and contact information only:** Users in this role can change their own password and contact information only.
- **Create and manage Users with equal or less access:** Users in this role can create and manage any users who do not have any privileges greater than theirs. If there 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.

8. 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.



9. 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
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	Allowed	Allowed	Allowed,

RIGHTS	SETTINGS BY ROLE		
non-selected computers and data (e.g. events, reports)			All Computers
Allow viewing of events and alerts not related to computers	Allowed	Allowed	Allowed, All Computers
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,	Not allowed,

RIGHTS	SETTINGS BY ROLE		
		All Policies	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
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

RIGHTS	SETTINGS BY ROLE		
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))	View-Only	Hide
Diagnostics	Full (Can Create Diagnostic Packages)	View-Only	View-Only
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)	View-Only	Hide
Multi-Tenant Administration	Full	Hide	View-Only
Scan Cache Configuration Administration	Full	View-Only	View-Only
Contacts	Full (Can View, Create, Edit, Delete Contacts)	View-Only	Hide
Licenses	Full (Can View, Change License)	View-Only	Hide
Updates	Full (Can Add, Edit, Delete Software; Can	View-Only	Hide

RIGHTS	SETTINGS BY ROLE		
	View Update For Components; Can Download, Import, Apply Update Components; Can Delete Deep Security Rule Updates)		
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
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

RIGHTS	SETTINGS BY ROLE		
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 Rulesets	Full (Can Create, View, Edit, or Delete Application Control rulesets)	Hide	Hide
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 corresponding to "Change own password and contact information only" option	
Users	
Can View Users	Not allowed
Can Create New Users	Not allowed

Custom settings corresponding to "Change own password and contact information only" option	
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	
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 corresponding to "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	

Custom settings corresponding to "Create and manage Users with equal or less access" option	
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 corresponding to "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

Custom settings corresponding to "Have full control over all Roles and Users" option	
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 990 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 874 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)**.

Note: If all of your administrative users are locked out, please contact Trend Micro Support for assistance.

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**.

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 894 or "Configure SAML single sign-on with Azure Active Directory" on page 900.

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** with one another.

> **Note:** At this time, 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

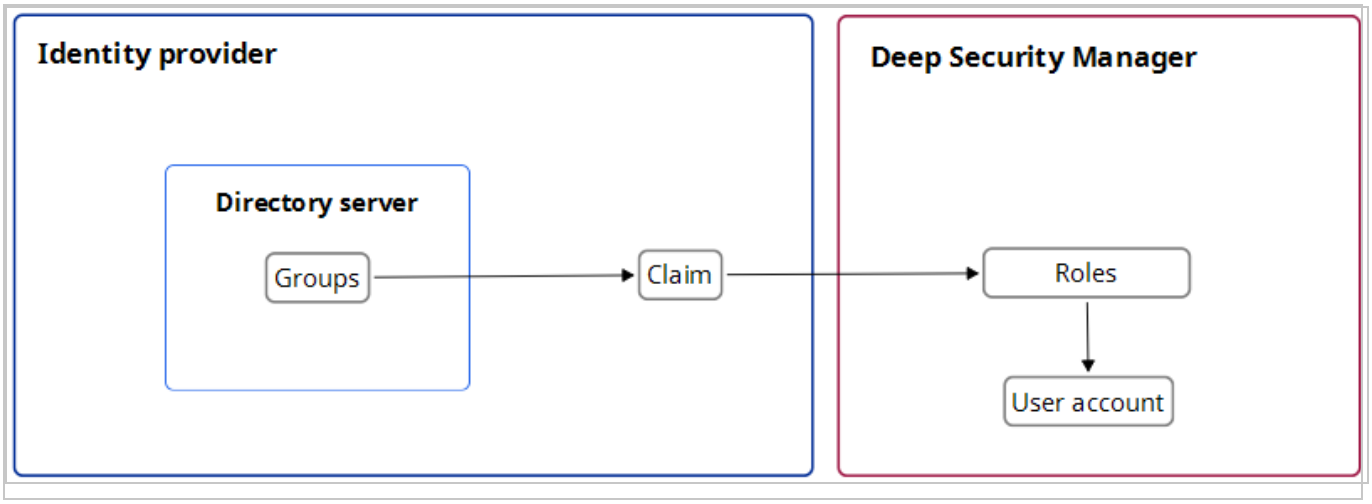
Once Deep Security and the identity provider have exchanged SAML metadata documents and established a trust relationship, Deep Security can access the user identities on the identity provider's directory server. However, before Deep Security can actually create accounts from the user identities, account 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 that a Deep Security user account will have. 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.

> **Tip:** Learn more about the "SAML claims structure" on page 897 required by Deep Security.

Below is a representation of 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 detailed explanation of Deep Security's implementation of the SAML standard, see "About SAML single sign-on (SSO)" on page 892. If you are using Azure Active Directory as your identity provider, see "Configure SAML single sign-on with Azure Active Directory" on page 900.

Note: At this time, 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 will need to do the following:

1. "Configure pre-set up requirements" below
2. "Configure SAML in Deep Security" below
3. "Provide information for your identity provider administrator" on the next page
4. "SAML claims structure" on page 897
5. "Test SAML single sign-on" on page 899
6. "Service and identity provider settings" on page 900

Configure pre-set up 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
- Azure Active Directory

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 874.

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 the next page
- "Preferred language (optional)" on page 899

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/RoleSessionNam
e">
        <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.

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/SessionDuratio
n">
        <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)
- `zh-CN` (Simplified Chinese)

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-set up requirements" on page 895 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 support case

1. Click **Support** in the top right-hand corner of the Deep Security Manager.
2. From the drop-down menu, click **Contact Support**.
3. Create a case and click **Submit**.

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 Azure Active Directory

For a detailed explanation of Deep Security's implementation of the SAML standard, see "About SAML single sign-on (SSO)" on page 892. For instructions on configuring it with other identity providers, see "Configure SAML single sign-on" on page 894.

Note:

- At this time, 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 Azure Active Directory for SAML single sign-on (SSO): a Deep Security administrator and an Azure Active Directory 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.

These are the steps required to set up SAML single sign-on with Deep Security using Azure Active Directory, and the person who performs each step:

Step	Performed by
"Download the Deep Security service provider SAML metadata document" below	Deep Security administrator
"Configure Azure Active Directory" below	Azure Active Directory administrator
"Configure SAML in Deep Security" on the next page	Deep Security administrator
"Define a role in Azure Active Directory" on page 903	Azure Active Directory administrator

Download the Deep Security service provider SAML metadata document

In Deep Security as a Service, go to **Administration > User Management > Identity Providers > SAML** and click **Download**. The file is downloaded as `ServiceProviderMetadata.xml`. Send the file to your Azure Active Directory administrator.

Configure Azure Active Directory

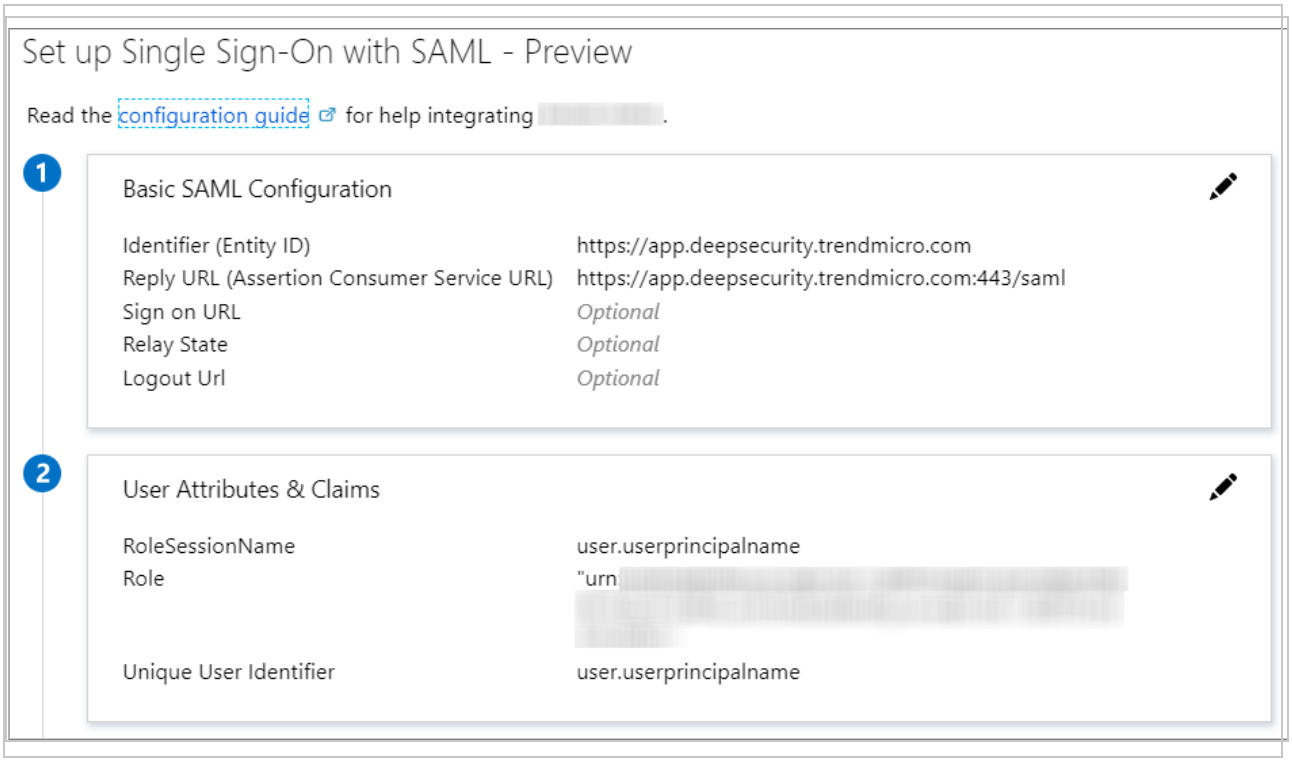
The steps in this section are performed by an Azure Active Directory administrator.

Refer to Configure single sign-on to non-gallery applications in Azure Active Directory for details on how to perform the steps below.

1. In the Azure Active Directory portal, add a new non-gallery application.
2. Configure single sign-on for the application. We recommend that you upload the metadata file, `ServiceProviderMetadata.xml`, that was downloaded from Deep Security as a Service. Alternatively, you can enter a reply URL (the Deep Security Manager URL + `/saml`).
3. Configure SAML claims. Deep Security requires these two:
   - `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 Azure Active Directory" on the next page.

You can also configure other optional claims, as described in "SAML claims structure" on page 904.



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 Azure Active Directory metadata document

1. In Deep Security as a Service, 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 Azure Active Directory 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 874. Each Deep Security role requires a corresponding Azure Active Directory application.

Get URNs

In Deep Security Manager, gather this information, which you will need to provide to your Azure Active Directory 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 Azure Active Directory 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 Azure Active application.

Define a role in Azure Active Directory

The steps in this section must be performed by an Azure Active Directory administrator.

In Azure Active Directory, use the identity provider URN and role URN identified in the previous section to define the "role" attribute in the Azure application. This must be in the format “IDP URN,Role URN”. See "Deep Security user role (required)" in the "SAML claims structure" on the next page section.

Use the Validate button in Azure Active Directory 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)" below
- "Deep Security user role (required)" below
- "Maximum session duration (optional)" on the next page
- "Preferred language (optional)" on page 906

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/RoleSessionNam
e">
        <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.

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/SessionDuratio
n">
        <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)
- `zh-CN` (Simplified Chinese)

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>
```

Manage your billing account

Check your billing and usage

If you are using AWS or Azure subscription billing, you can check your billing charges and usage levels through AWS or Azure. You can also export a usage report through Deep Security as a Service.

Note: For details on AWS and Azure subscription billing, see "About billing and pricing" on page 74.

Check billing and usage in AWS

If you're using AWS subscription billing, you can check your current costs and usage from the AWS Billing and Cost Management console. For instructions on viewing or downloading your bills, see the AWS documentation on Viewing Your Monthly Charges. If you are new to using the AWS Billing and Cost Management console, see the AWS Getting Started documentation.

If you want a more detailed look at your costs and usage, you can enable the AWS Billing Cost Explorer feature. Cost Explorer can show you a daily breakdown of your costs and usage and forecast what your costs might be over the coming months.

Check billing and usage in Azure

If you're using Azure subscription billing, you can check your current costs and usage from the Cost Management + Billing section of the Azure portal.

If you are new to using the Azure Cost Management solution, see the Azure cost management documentation.

Check billing and usage in the manager

If you are using AWS or Azure subscription billing, you can check your billing and usage in Deep Security as a Service:

1. In Deep Security as a Service, go to **Events & Reports > Generate Reports > Single Report**.
2. From the **Report** list, select **AWS Metered Billing Report** or **Azure Metered Billing Report**.
3. Select the period of time for which you want to view usage data from the **Time Filter** area.
4. Click **Generate**.

For more information on generating reports from the manager, see "Generate reports about alerts and other activity" on page 695.

Change your billing method

With Deep Security as a Service, you can change from your current billing method to another one. For details on billing methods, see "About billing and pricing" on page 74.

To change, follow one of these sets of instructions:

- "Change from BYOL billing " below
- "Change from credit card billing" below
- "Change from prepaid credit" on the next page
- "Change from AWS subscription billing" on the next page
- "Change from Azure subscription billing" on page 910

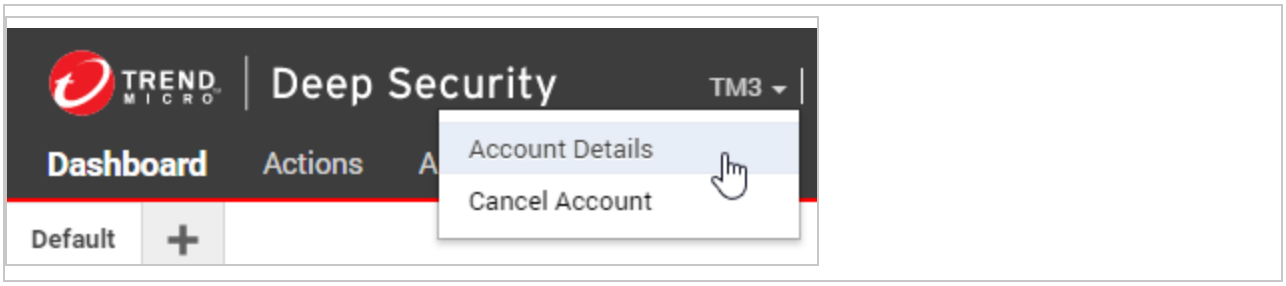
Change from BYOL billing

To change from bring-your-own-license (BYOL) billing to another method, simply sign up for the other method. For instructions, see "Sign up for Deep Security as a Service" on page 120

Change from credit card billing

First, cancel credit card billing:

1. Log in to Deep Security as a Service.
2. In the top middle of the page, click your account name (as shown below) and select **Account Details** from the list.



3. Click **Cancel Subscription**.
4. Select **I have read and understood the above information** and then click **Cancel My Subscription**.

   Your Deep Security as a Service account will change state to allow for 5 free protected instances. However, all of your existing instances will continue to be protected.

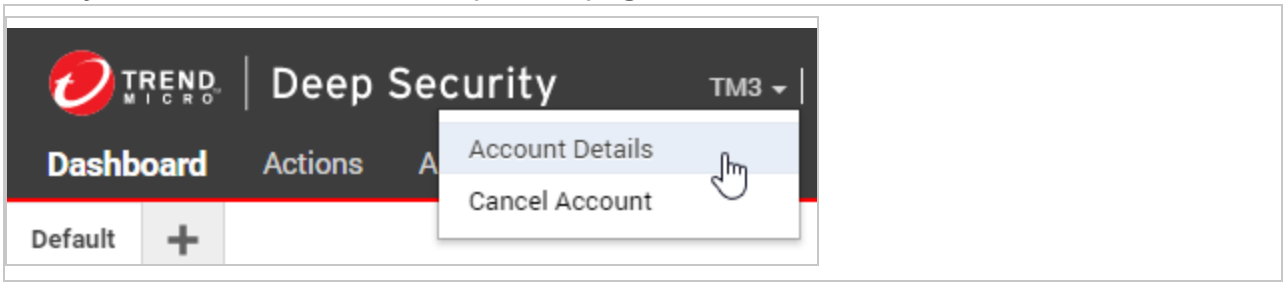
Next, sign up for another billing method. For instructions, see "Sign up for Deep Security as a Service" on page 120

Change from prepaid credit

First, make sure you have used all remaining prepaid credits so you don't lose them.

Next, update your license:

1. Click your account name at the top of the page and select **Account Details** from the list.



2. Click **Update License**.

Next, sign up for another billing method. For instructions, see "Sign up for Deep Security as a Service" on page 120

Change from AWS subscription billing

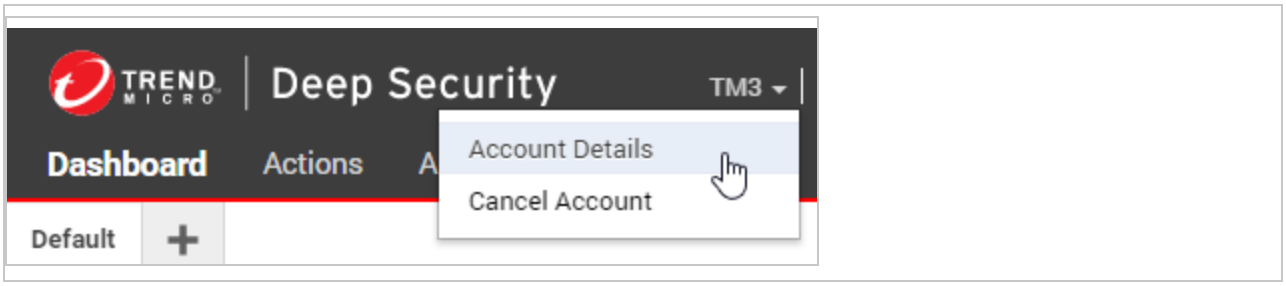
First, cancel your current AWS subscription billing:

1. Log in to your AWS Marketplace account.
2. Click **Your Software**.
3. Under the Trend MicroDeep Security as a Service product, click **Cancel Subscription**, and then **Yes, Cancel Subscription**.

> **Note:** It may take up to two hours for your cancellation to be processed.

Next, unlink your AWS Marketplace account from your Deep Security as a Service account:

1. Sign in to your Deep Security as a Service account.
2. At the top of the page, click your account name (as shown below) and select **Account Details**.



3. On the **Type** field, check that your Deep Security as a Service account now shows **Free - Maximum of 5 Protected Computers**.
4. Click **Unlink AWS Account**.

Finally, sign up for another billing method. For instructions, see "Sign up for Deep Security as a Service" on page 120

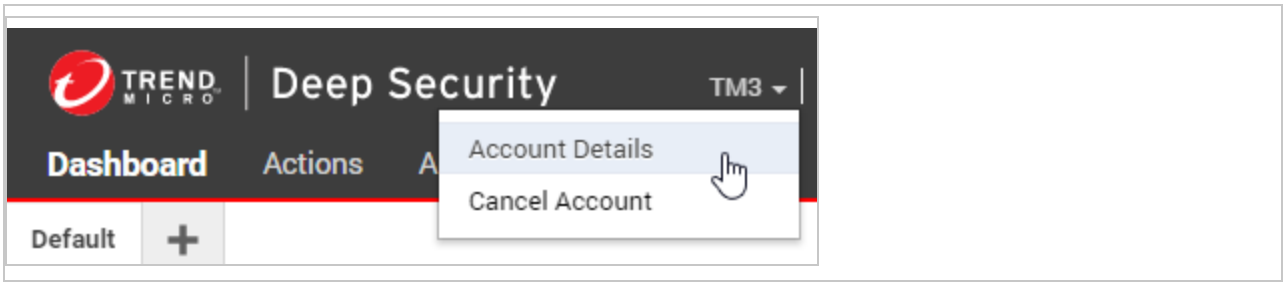
Change from Azure subscription billing

First, cancel your current Azure subscription billing:

1. Log in to the Azure portal.
2. Use the search bar at the top to navigate to the **Software as a Service (SaaS)** page.
3. Select the name of your account (example: `Example Inc - Deep Security as a Service`) and click **Delete**.

Next, check that Azure billing has been removed from your Deep Security as a Service account:

1. Log out of Deep Security as a Service if you're not already.
2. Log in.
3. At the top of the page, click your account name (as shown below) and select **Account Details**.



4. On the **Type** field, check that your Deep Security as a Service account now shows **Free - Maximum of 5 Protected Computers**. This indicates that your Deep Security as a Service account has been unlinked from Azure subscription billing.

Finally, sign up for another billing method. For instructions, see "Sign up for Deep Security as a Service" on page 120

Change your subscription account

If you're using AWS or Azure subscription billing, you can change the AWS or Azure account associated with your Deep Security as a Service account. For details on subscription billing, see "About billing and pricing" on page 74.

Change an AWS subscription account

First, cancel AWS subscription billing:

1. Log in to the current AWS Marketplace account.
2. Click **Your Software**.
3. Under the Trend Micro Deep Security as a Service product, click **Cancel Subscription**, and then **Yes, Cancel Subscription**.

   Note: It may take up to two hours for your cancellation to be processed.

Next, sign up for Deep Security as a Service with another AWS account. See "Sign up for Deep Security as a Service" on page 120

Change an Azure subscription account

First, cancel Azure subscription billing:

1. Log in to the Azure portal.
2. Use the search bar at the top to navigate to the **Software as a Service (SaaS)** page.
3. Select the name of your account (example: `Example Inc - Deep Security as a Service`) and click **Delete**.

Next, sign up for Deep Security as a Service with another Azure account. See "Sign up for Deep Security as a Service" on page 120

Change your credit card information

You can change your Deep Security as a Service credit card information. For details on credit card billing, see "About billing and pricing" on page 74.

To change your credit card information:

1. In the Deep Security Manager, click your account name and select **Account Details**.
2. In the **Activity** section, click the link next to **Credit Card Details**.
3. When the payment options page opens, update and save your credit card information.

Note: If you need to change the address or email associated with your credit card or would like copies of previous invoices, contact Cleverbridge customer support.

Cancel your account

Topics in this section:

Cancel your account

To cancel your Deep Security as a Service account, you have to:

1. (Optional but strongly recommended) Deactivate and uninstall your Deep Security Agents. For instructions, see "Uninstall Deep Security" on page 969.
2. If you signed up for AWS subscription billing, cancel AWS subscription billing.
3. if you signed up for Azure subscription billing, cancel Azure subscription billing.
4. "Cancel your Deep Security as a Service account" on the next page.

For details on billing, see "About billing and pricing" on page 74.

Cancel AWS subscription billing

1. Log in to your AWS Marketplace account.
2. Click **Your Software**.
3. Under the Trend Micro Deep Security as a Service product, click **Cancel Subscription**, and then **Yes, Cancel Subscription**.

Cancel Azure subscription billing

1. Log in to the Azure portal.
2. Use the search bar at the top to navigate to the **Software as a Service (SaaS)** page.
3. Select the name of your account (example: `Example Inc - Deep Security as a Service`) and click **Delete**.

Cancel your Deep Security as a Service account

1. Sign in to your Deep Security as a Service account.
2. Click your account name and select **Cancel Account**.
3. Select the **I have read and understood the above information** check box, and then click **Cancel My Account**.

What happens when I cancel my account?

Upon receiving your request to cancel your account, the account is immediately put into a suspended state where it is no longer accessible to you. At the end of each month we start a 30-day timer on any suspended accounts. If you canceled your account in error, it can be restored at any point before the 30-day timer reaches zero. Once the 30-day timer reaches zero, your data is permanently deleted. To restore your account, contact Trend Micro Business Support. Alternatively, you can sign up again.

Other effects of canceling your account are:

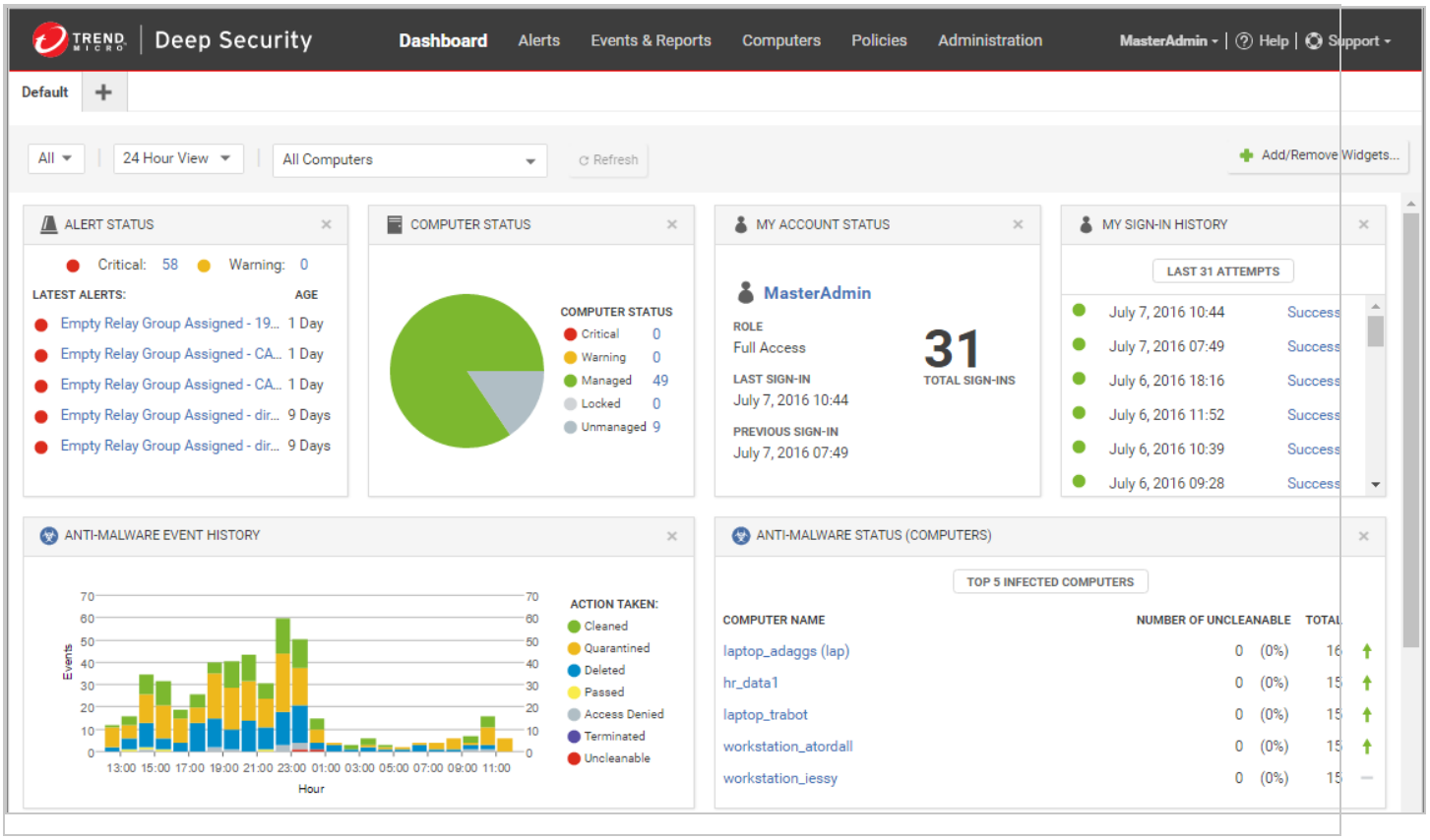
- If you opted for metered billing, it stops immediately. Your last monthly bill shows the usage up to the point when you canceled.
- If you chose AWS subscription billing with the Annual + Pay as you Go option, the annual fee remains in effect. To stop the annual charge, you must "Cancel AWS subscription billing" on the previous page.
- If you chose prepaid credit billing, your prepaid credits are not returned. We advise that you use up your prepaid credits before canceling your account.
- Since you no longer have access to Deep Security as a Service, you will no longer be able to view or manage agents that may still be running in your environment. We therefore strongly recommend that you deactivate and uninstall your agents prior to canceling your account.
- Any computers that have agents still running on them remain protected; however, agents no longer receive security updates (pattern updates) and software updates, so security will degrade over time.

Navigate and customize Deep Security Manager

Customize the dashboard

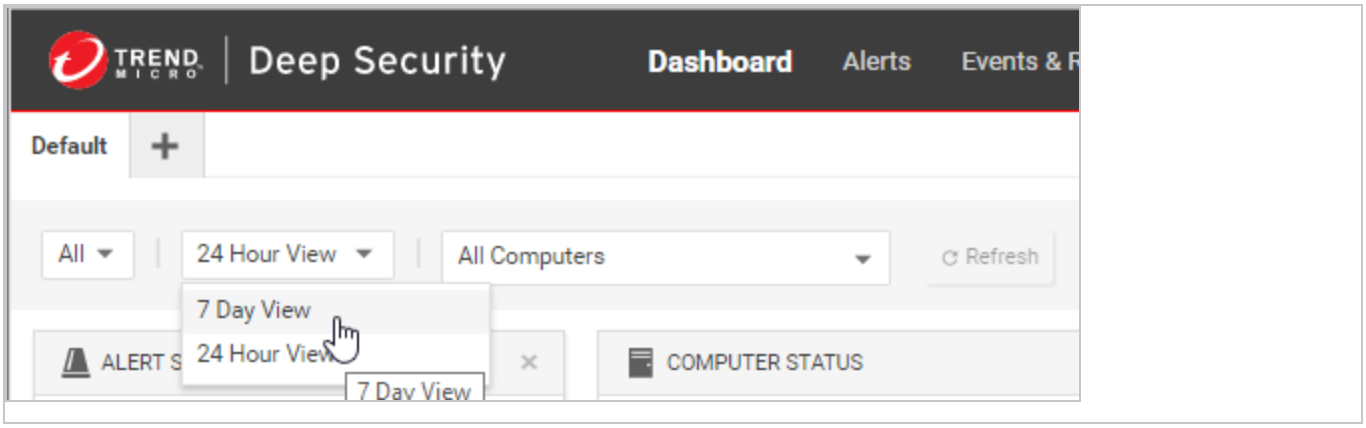
The dashboard is the first page that appears after you log into Deep Security Manager.

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.



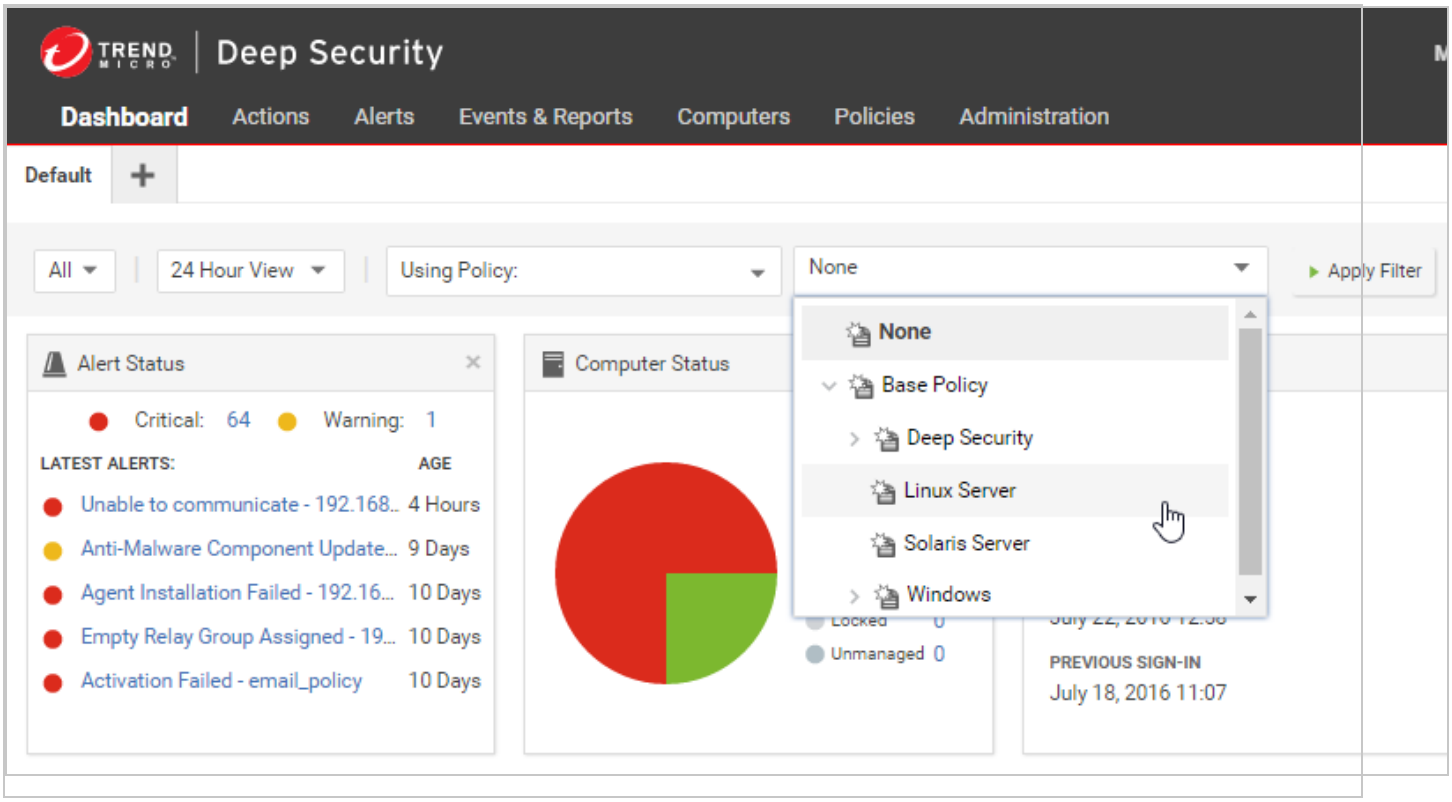
Date and time range

The dashboard can display data from either the last 24 hours, or the last seven days.



Computers and computer groups

Use the **Computer** menu to filter the displayed data to display only data from specific computers. For example, only those using the **Linux Server** security policy:

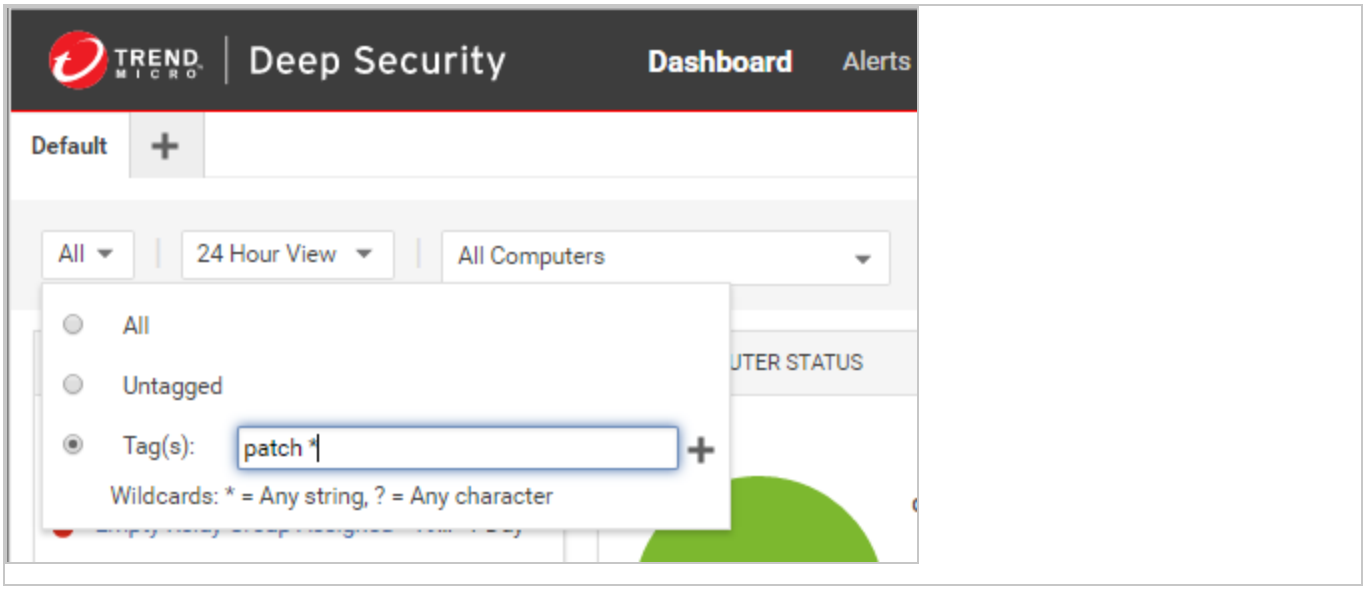


Filter by tags

In Deep Security, a **Tag** is a unit of meta-data 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 in order 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.

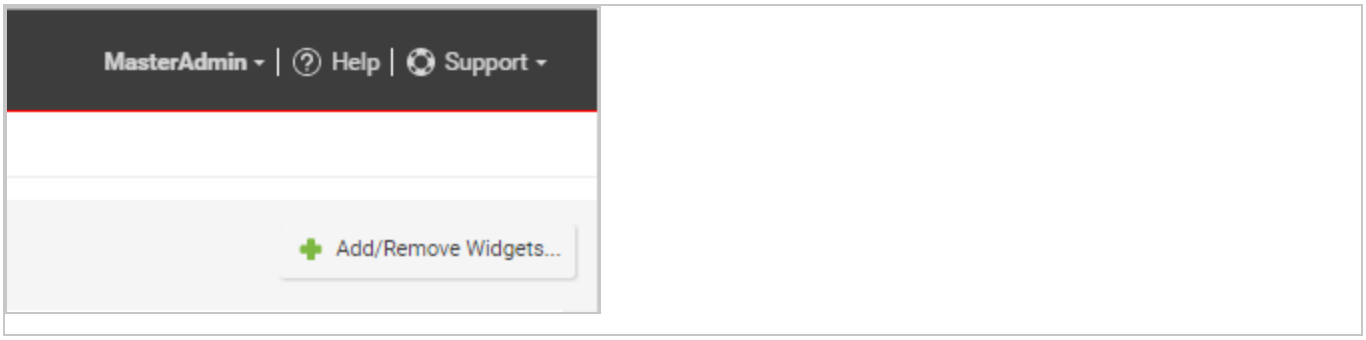
The data displayed in the Dashboard can be filtered by tags:



For more information on tagging see "Apply tags to identify and group events" on page 573.

Select dashboard widgets

Click **Add/Remove Widgets** to display the widget selection window and choose which widgets to display.



Note: 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]**: Displays 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.
- **License Information**: Displays license information, including the number of protected computers.
- **Security Update Status**: Displays the update status of computers, including the number of computers that are up-to-date, out-of-date, and unknown.

System:

- **My Sign-in History**: Displays the last 50 sign-in attempts and whether or not they were successful.
- **My User Summary [2x1]**: Displays a summary of the user, including name, role, and sign-in information.
- **Software Updates**: Displays out-of-date computers.
- **System Event History [2x1]**: Displays recent system event history, including the number of events that are categorized as info, warning, or error.

Ransomware:

- **Ransomware Event History [3x1]**: Displays recent ransomware event history, including the event type.
- **Ransomware Status**: Displays 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]**: Displays recent Anti-Malware event history, including the action taken for the events.
- **Anti-Malware Protection Status**: Displays 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]**: Displays the top five infected computers, including the amount of uncleanable files and the total number of files affected.
- **Anti-Malware Status (Malware) [2x1]**: Displays the top five detected malware, including their name, amount of uncleanable files, and number of times it was triggered.
- **Malware scan Status [2x1]**: Displays the top five appliances with incomplete scheduled malware scans.

Web Reputation:

- **Web Reputation Computer Activity**: Displays the top five computers with Web Reputation events, including the number of events.
- **Web Reputation Event History [2x1]**: Displays recent Web Reputation event history, including the events severity.
- **Web Reputation URL Activity**: Displays the top five URLs that triggered Web Reputation events, including the number of times they were accessed.

Firewall:

- **Firewall Activity (Detected)**: Displays the top five reasons packets were detected, including the number of times.
- **Firewall Activity (Prevented)**: Displays the top five reasons packets were prevented, including the number of times.
- **Firewall Computer Activity (Detected)**: Displays the top five computers that generated detected Firewall events and the number of times they occurred.
- **Firewall Computer Activity (Prevented)**: Displays the top five computers that generated prevented Firewall events and the number of times they occurred.
- **Firewall Event History [2x1]**: Displays recent Firewall event history, including if the events were detected or prevented.
- **Firewall IP Activity (Detected)**: Displays the top five source IPs that generated detected Firewall events and the number of times they occurred.
- **Firewall IP Activity (Prevented)**: Displays the top five source IPs that generated prevented Firewall events and the number of times they occurred.
- **Firewall Port Activity (Detected)**: Displays the top five destination ports for detected Firewall events and the number of times they occurred.
- **Firewall Port Activity (Prevented)**: Displays the top five computers that generated prevented Firewall events and the number of times they occurred.

- **Reconnaissance Scan Activity**: Displays the top five detected reconnaissance scans, including the number of times they occurred.
- **Reconnaissance Scan Computers**: Displays the top five computers where reconnaissance scans occurred and the number of times they occurred.
- **Reconnaissance Scan History [2x1]**: Displays recent reconnaissance scan history, including the type of scan that occurred.

Intrusion Prevention:

- **Application Type Activity (Detected)**: Displays the top five detected application types, including the number of times they were triggered.
- **Application Type Activity (Prevented)**: Displays the top five prevented application types, including the number of times they were triggered.
- **Application Type Treemap (Detected) [2x2]**: Displays 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]**: Displays 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):** Displays the top five reasons Intrusion Prevention events were detected, including the number of times it was triggered.
- **IPS Activity (Prevented)**: Displays the top five reasons Intrusion Prevention events were prevented, including the number of times it was triggered.
- **IPS Computer Activity (Detected)**: Displays the top five computers with detected Intrusion Prevention events.
- **IPS Computer Activity (Prevented)**: Displays the top five computers with prevented Intrusion Prevention events.
- **IPS Event History [2x1]**: Displays recent Intrusion Prevention event history, including if the events were detected or prevented.
- **IPS IP Activity (Detected)**: Displays the top five source IPs that generated detected Intrusion Prevention events.
- **IPS IP Activity (Prevented)**: Displays the top five source IPs that generated prevented Intrusion Prevention events.
- **Latest IPS Activity (Detected)**: Displays the top five reasons Intrusion Prevention events were detected since the latest update.

- **Latest IPS Activity (Prevented)**: Displays the top five reasons Intrusion Prevention events were prevented since the latest update.

Integrity Monitoring:

- **Integrity Monitoring Activity**: Displays 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**: Displays the top five computers where Integrity Monitoring events occurred, including the number of events.
- **Integrity Monitoring Event History [2x1]**: Displays recent Integrity Monitoring event history, including the severity of events.
- **Integrity Monitoring Key Activity**: Displays the top five keys for Integrity Monitoring events. The source of the key varies by Entity Set - for files and directories it's their path, whereas for ports it's their unique protocol, IP, port number, or tuple.

Log Inspection:

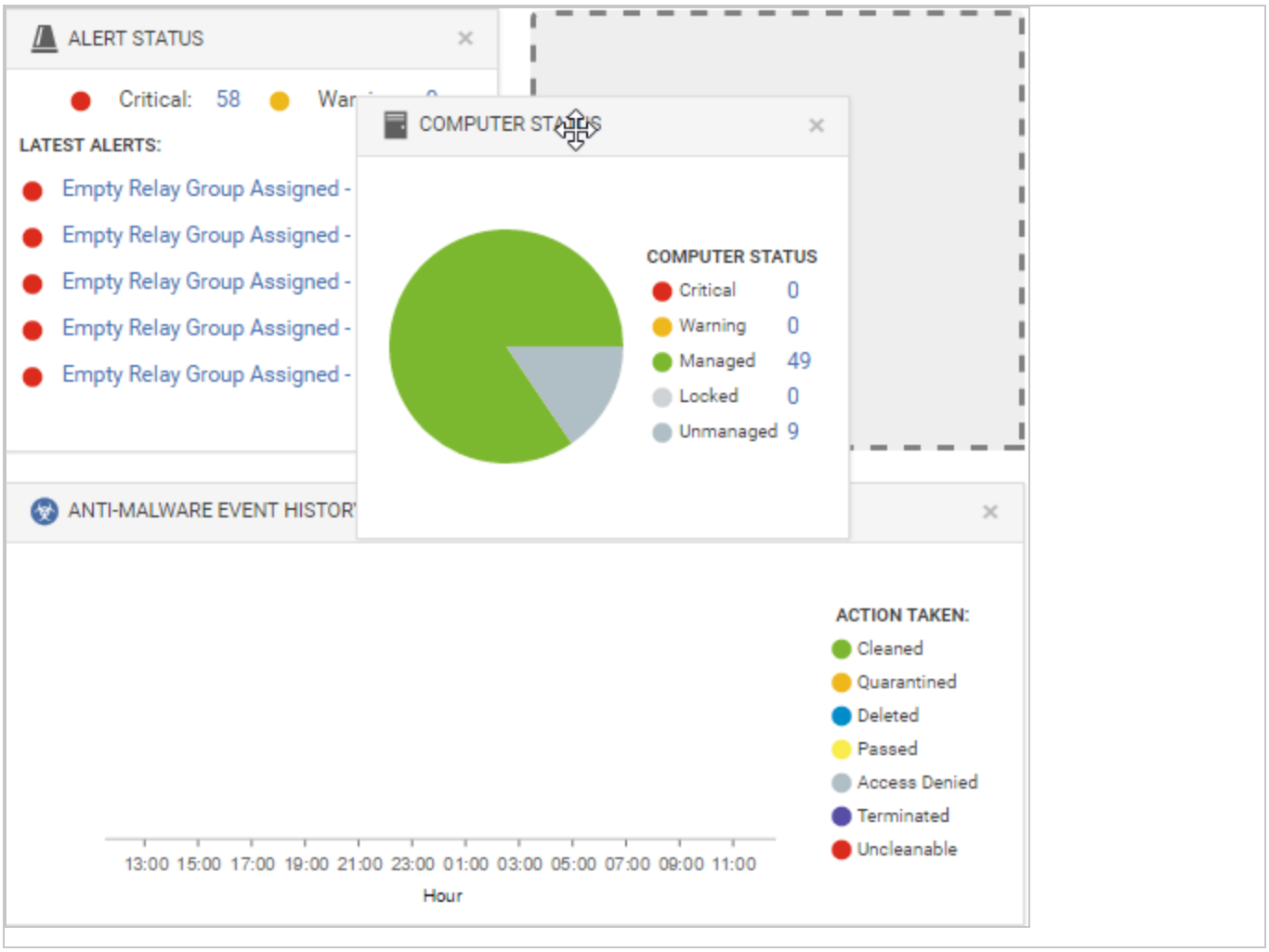
- **Log Inspection Activity**: Displays the top five reasons Integrity Monitoring events occurred, including the number. In this case, the reason refers to the rule that was triggered.
- **Log Inspection Computer Activity**: Displays the top five computers where Log Inspection events occurred, including the number of events.
- **Log Inspection Description Activity**: Displays 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]**: Displays recent Log Inspection event history, including the severity of events.

Application Control:

- **Application Control Maintenance Mode Status [2x1]**: Displays the computers in maintenance mode, including their start and end time.

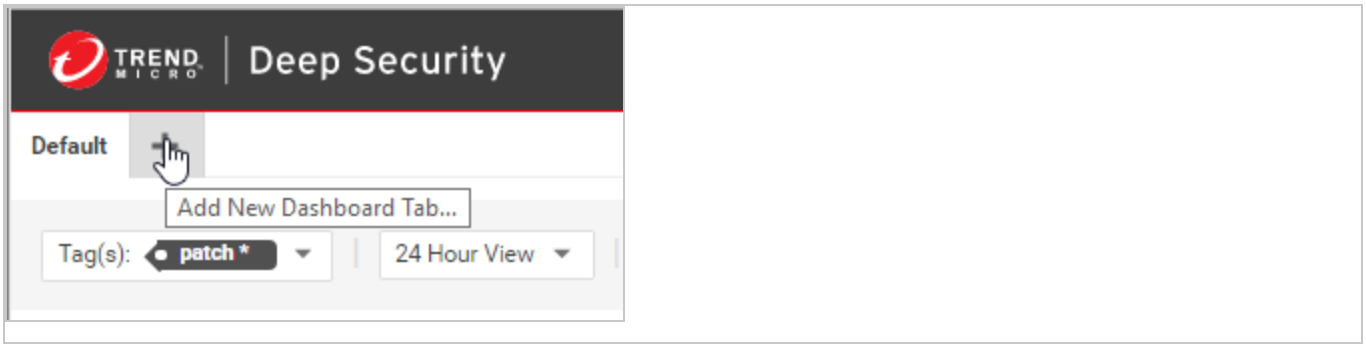
Change the layout

The selected widgets can be moved around the dashboard by dragging them by their title bar. Move the widget over an existing one and 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 will not be 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:



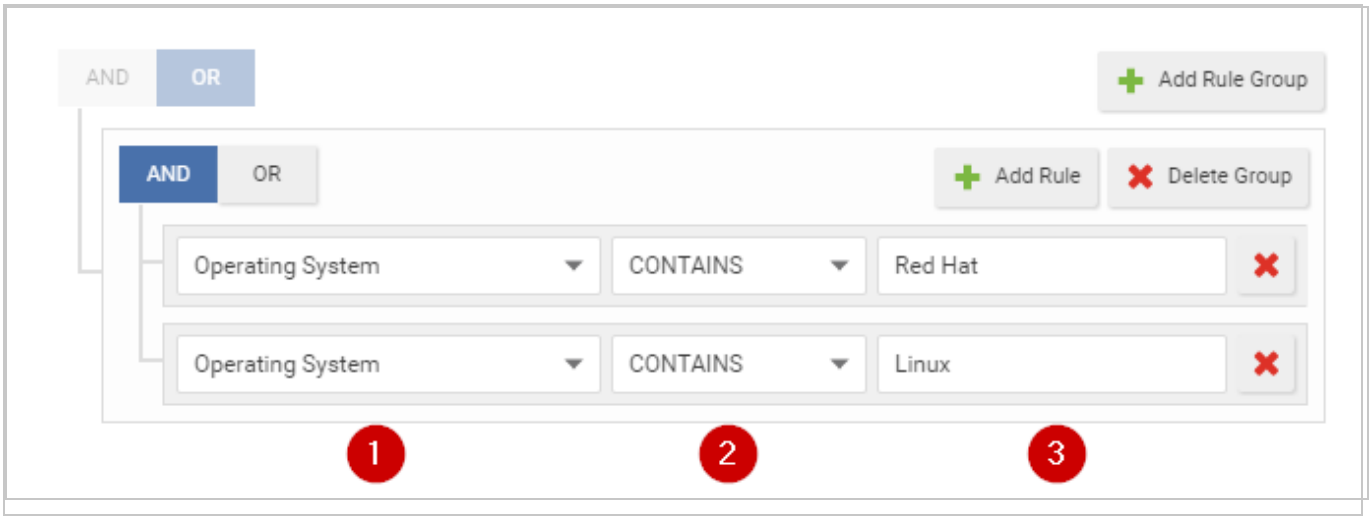
Group computers dynamically with smart folders

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)



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 926.)

   If you selected AWS **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.

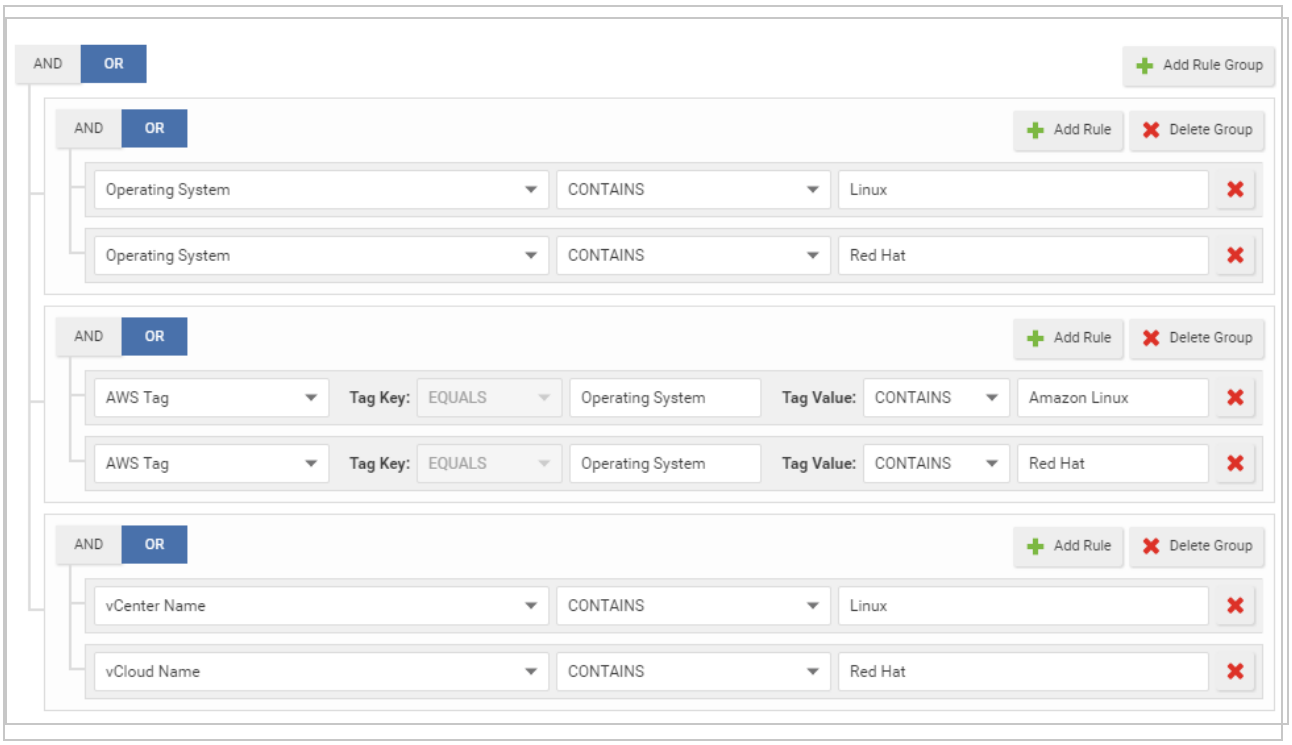
   Tip: If you enter multiple words, it compares the *entire phrase* - not each word separately. No match occurs if the property's value has words in a different order, or only some of the words.
   To match *any* of the words, instead click **Add Rule** and **OR**, and then add another value: one word 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



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 874.

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 and GCP computers only.

Instead of manually creating child folders, you can automatically create sub-folders for each value of an AWS tag or GCP label that's assigned to an Amazon EC2 instance, GCP VM instance, or Amazon Workspace. For information on how to apply AWS tags and GCP labels to

your computers, see Tagging Your Amazon EC2 Resources and Labelling Resources for GCP resources.

Note: AWS tag-based sub-folders or GCP 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 or GCP cloud vendor.
4. Type the name of the AWS 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 an AWS tag or GCP 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
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

Property	Description	Data type	Examples
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.
	
	You can find the IP address in Deep Security Manager. To find the IP of:
	
	• 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:
	  • **Private IP Address**
	  • **Public IP (PIP) Address**
	
	Note: If you added the AWS, GCP, or Azure computer through **Add > Add Computers**, its IP address is located in the same place as a physical computer's.
	
	• a physical computer, go to the computer's details page and on the left, click **Interfaces**
	
	Note: If "DHCP" is displayed
		IPv4 or IPv6 address, or an IPv4 range	172.20.1.5-172.20.1.55
			
			2001:db8:face::5

Property	Description	Data type	Examples
	instead of a static IP address, it won't match the smart folder query. • 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 (option in drop-down list)	Base Policy
Activated	Whether or not the computer has been activated with Deep Security Manager, as seen on **Computers > Details**.	Boolean	Yes
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	Date operator drop-down list, String,	**OLDER THAN**, 7, **DAYS**

Property	Description	Data type	Examples
	Integrity Monitoring or **Log Inspection > Recommendations**.	Date unit drop-down list	
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
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 824.	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	string	Tag Key: env Tag Value: staging

Property	Description	Data type	Examples
	Metadata. Type the tag name, then its value. Case-sensitive.		
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 Account ID, as seen on **Computers** when you right-click **Amazon Account** and select **Properties**. Results include computers in sub-folders.	string	123456789012
Account Name	The computer's associated AWS Account Alias, as seen on **Computers** when you right-click the AWS Cloud Connector and select **Properties**. Results include computers in sub-folders.	string	MyAccount-123
Region ID	The computer's AWS region suffix. Results include computers in sub-folders.	string	us-east-1
Region Name	The computer's associated AWS region name. Results include computers in sub-folders.	string	US East (Ohio)
VPC ID	The computer's Virtual Private Cloud (VPC) ID. If an alias exists, the folder name is the alias,	string	vpc-3005e48a

Property	Description	Data type	Examples
	followed by the VPC ID in parentheses. Otherwise the folder's name is the VPC ID. Results include computers in sub-folders.		
Subnet ID	The computer's associated Virtual Private Cloud (VPC) subnet ID. 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. Results include computers in sub-folders.	string	subnet-b1c2e468
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. The computer's associated Azure subscription account ID, as seen on **Computers** when you right-click **Azure** and select **Properties**.	string	MyAzureAccount

Property	Description	Data type	Examples
	Results include computers in sub-folders.		
Resource Group	The computer's associated resource group.	string	MyResourceGroup

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**. Type the label key, and then its value. Case-sensitive.	string	Label Key: env 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. Results include computers in sub-folders.	string	vCenter - lab13-vc.example.com
Datacenter	The computer's associated vCenter data center. 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 (comma-separated attribute name and value)	env, production

vCloud

Property	Description	Data type	Examples
Name	The computer's associated vCloud. Results include computers in sub-folders.	string	vCloud-lab23
Datacenter	The computer's associated vCloud data center. Results include computers in sub-folders.	string	lab13-datacenter
vApp	The computer's associated vCloud data center folder. Results include computers in sub-folders.	string	db_dev

Folder

Property	Description	Data type	Examples
Name	The hostname of the Microsoft Active Directory or LDAP directory. Results include computers in sub-folders.	string	ad01.example.com

Property	Description	Data type	Examples
Folder	The computer's Microsoft Active Directory or LDAP folder name. 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 with the selected property.	A search query in the Group Name property finds all computers in that group.
IN RANGE	The search query finds all computers between the	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

Operator	Description	Example usage
	specified start and end range.	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. 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. Used with an accompanying DAYS, WEEKS, HOURS, or	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
	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.

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.

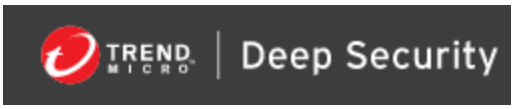
Exported Diagnostics Package Language: Your support provider may ask you generate and send them a Deep Security diagnostics package. This setting specifies the language the package will be in. The diagnostic package is generated on **Administration > System Information**.

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".)

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

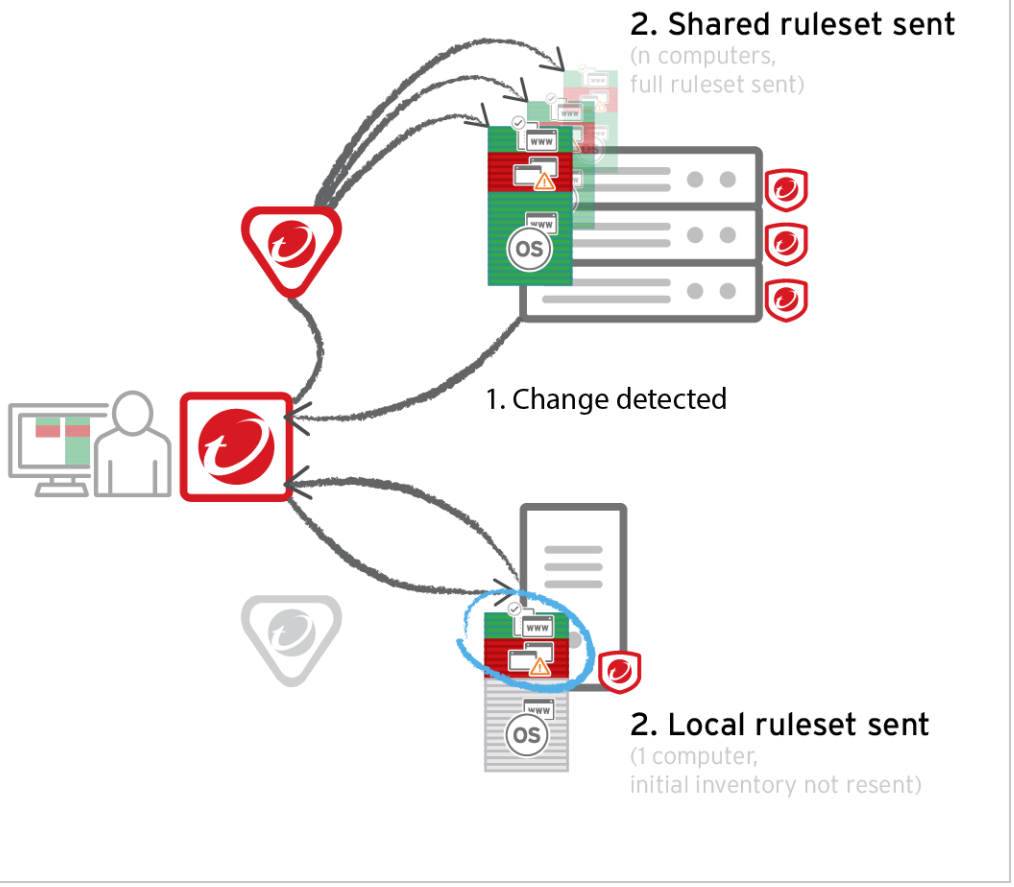
Each time you create an Application Control ruleset or change it, it must be distributed to all computers that use it. Shared rulesets are bigger than local rulesets. Shared rulesets are also often applied to many servers. If they all downloaded the ruleset directly from the manager at the same time, 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 816.)

Steps vary by whether or not you have a multi-tenant deployment.

Single tenant deployments

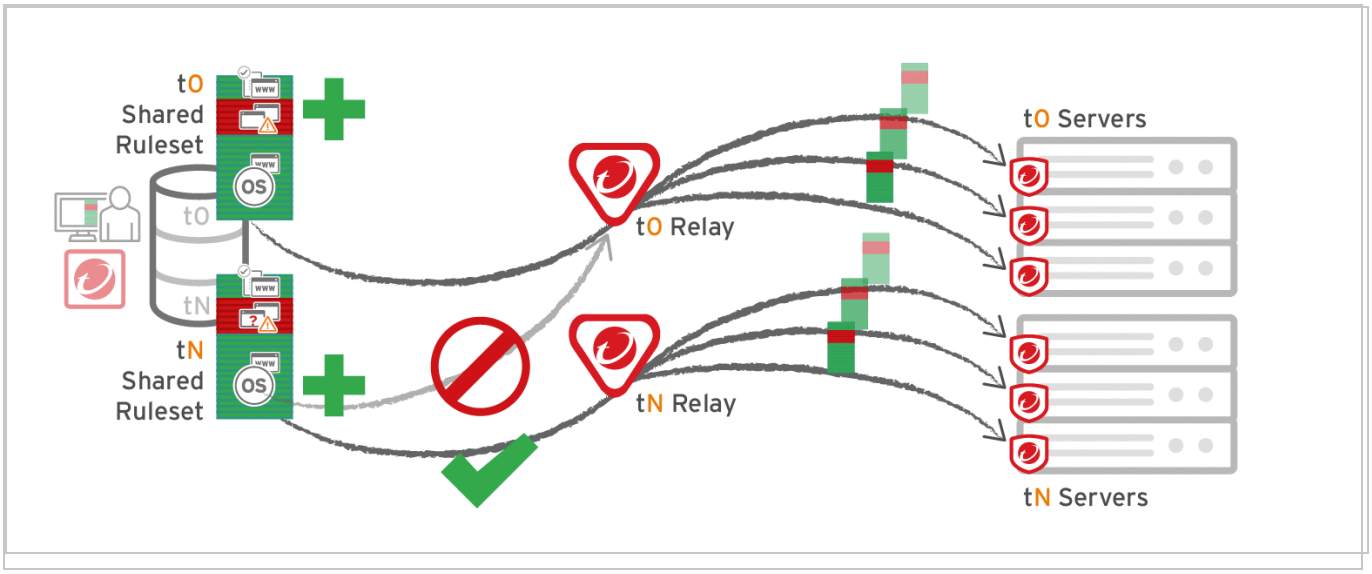
Go to **Administration > System Settings > Advanced** and then select **Serve Application Control rulesets from relays**.



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 **Note:** In Deep Security Agent 10.0 GM	Shared rulesets Global ruleset	Local rulesets	Multi-tenant configurations when non-primary tenants (tN) use the default, primary (t0) relay group: • Agent (tN) > DSR (t0) > DSM (tN) • Agent (tN) > Proxy > DSR (t0) > DSM (tN)

Required for...	Faster performance for...	Slower performance for...	Don't enable for...
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 (including Deep Security as a			

Required for...	Faster performance for...	Slower performance for...	Don't enable for...
Service), then you must either: • update agents' software, then configure the proxy • bypass the proxy • add a relay and then select **Ser**			

Required for...	Faster performance for...	Slower performance for...	Don't enable for...
ve App licat ion Con trol rule sets fro m rela ys			

Harden Deep Security

About Deep Security hardening

Deep Security as a Service and the Deep Security AMI from AWS Marketplace AMIs all run on Amazon Linux. The Deep Security team has hardened those products based on the Center for Internet Security (CIS) standard for Amazon Linux.

Hardening involves making changes to secure the system and make it less vulnerable to attack. For Deep Security, the changes included updating the web installer so that it terminates after the Deep Security Manager is online, removing unnecessary software, and configuring system settings to use the principal of least privilege, wherever it is applicable.

Deep Security AMI from AWS Marketplace is also protected by a Deep Security Agent installed on the same computer as the Deep Security Manager. The Agent has a default " Deep Security Manager" policy applied to it, which provides basic intrusion prevention rules and firewall rules that filter traffic to the manager.

Additionally, you can:

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 874).

  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.

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 894.

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:

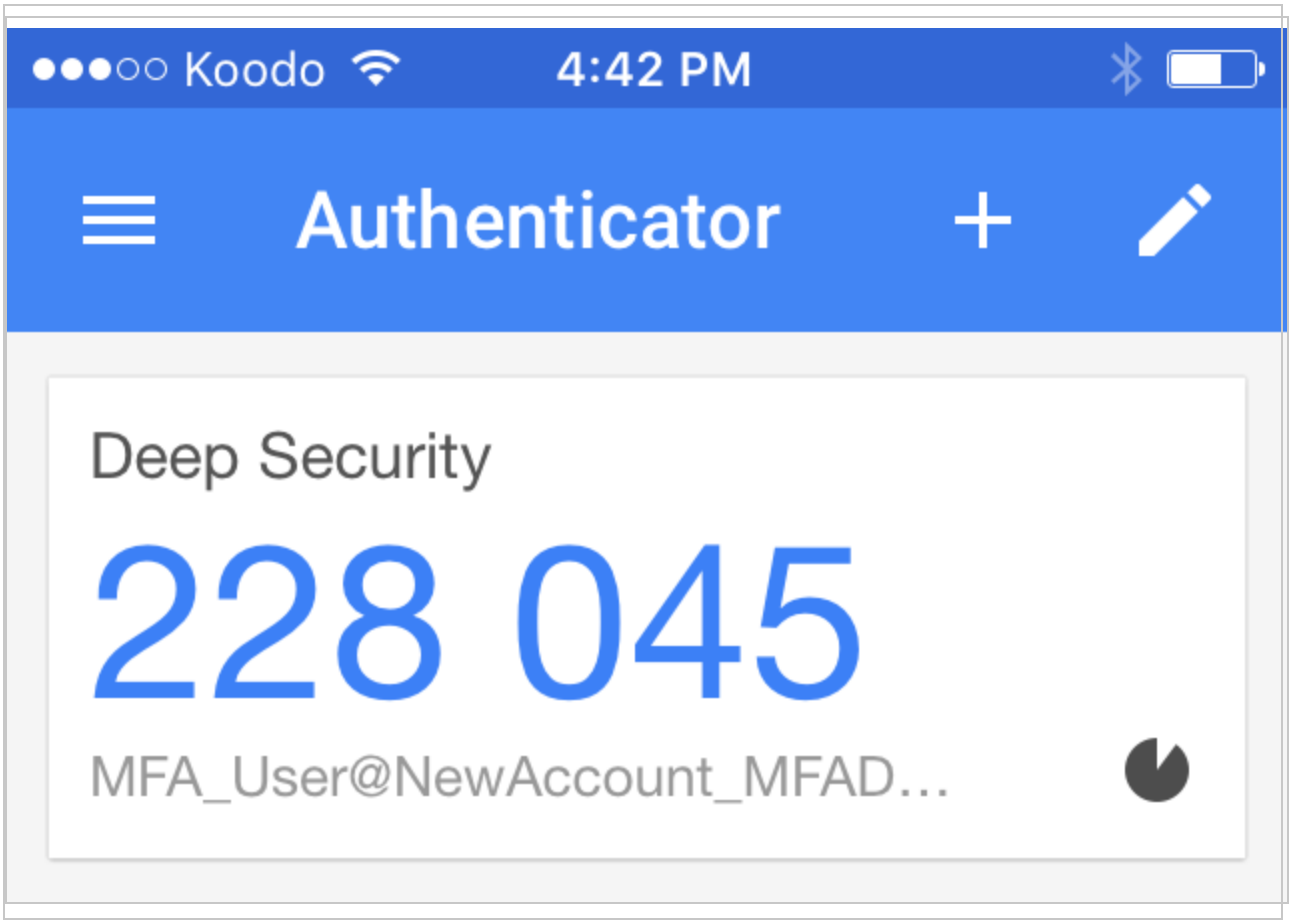
- "Supported multi-factor authentication (MFA) applications" on page 948
- "Troubleshooting MFA" on page 949

Enable multi-factor authentication

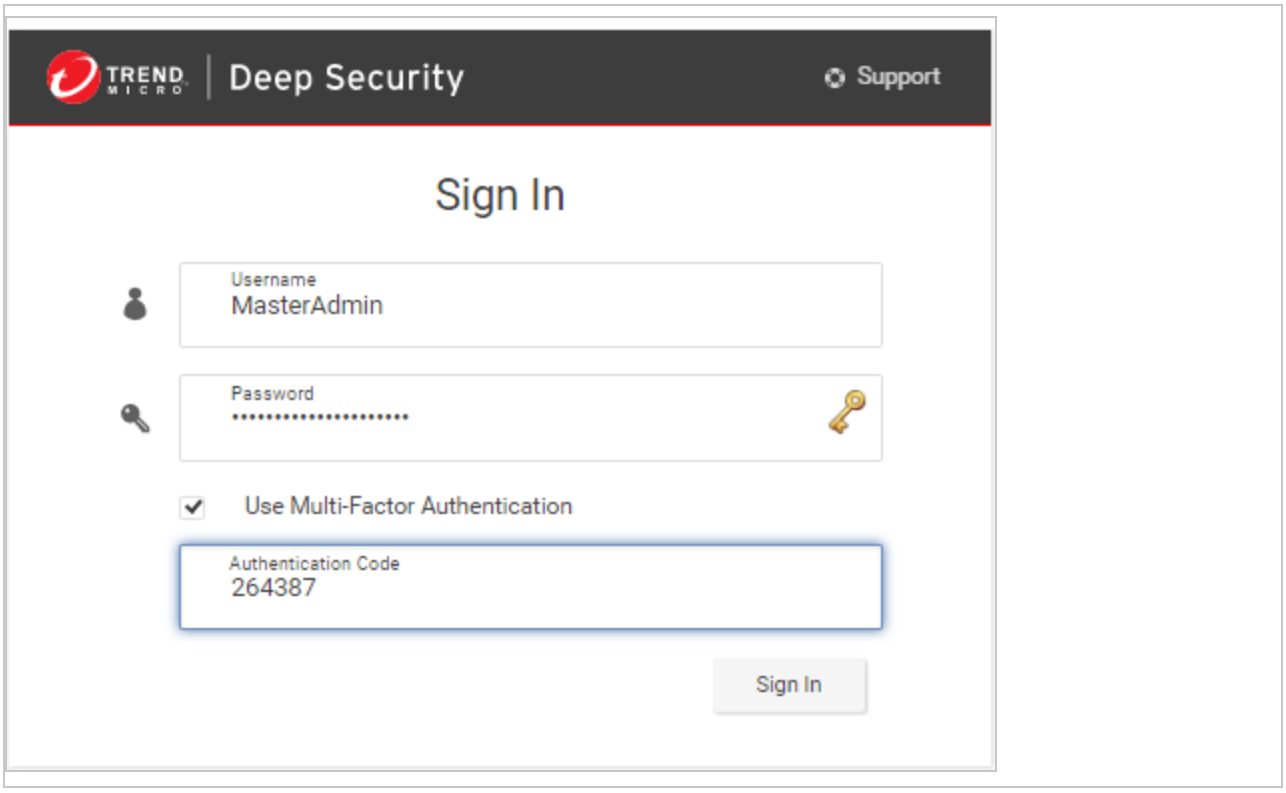
1. In Deep Security Manager, select **User Properties** from the menu under your user name in the upper-right corner.
2. On the **General** tab, click the **Enable MFA** button. This will open the **Enable Multi-Factor Authentication** wizard to guide you through the rest of the process.
3. The first 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 948 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.



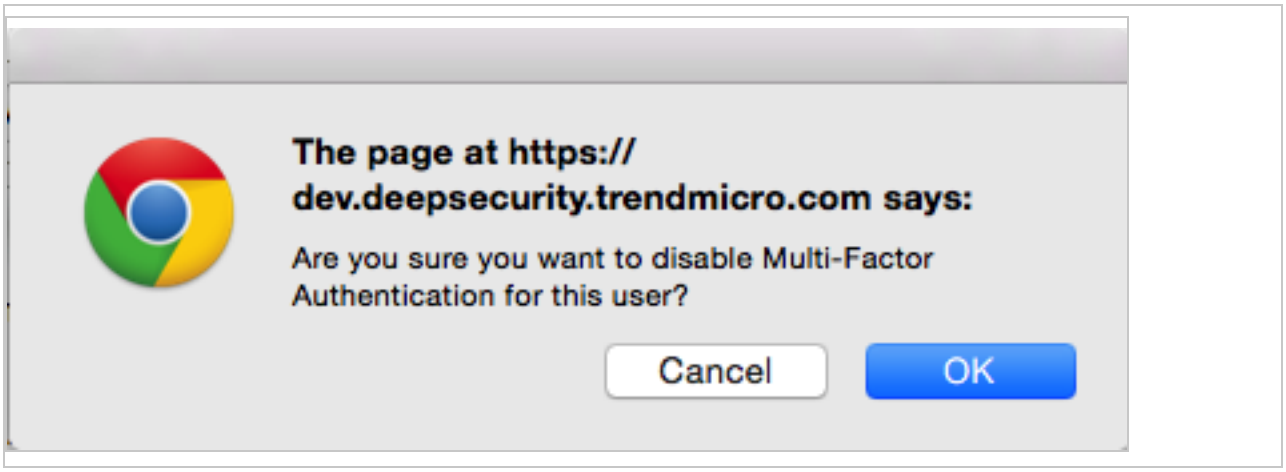
6. If the authorization code is correct, MFA will be enabled for your account and you will be required to enter a new MFA code each time you sign in.



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.



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.

If you're using Deep Security as a Service, you do not have access to the Deep Security Manager command line to check if the time is syncing properly. Please contact Support for assistance.

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 945.

If you are the only administrative user for a Deep Security as a Service account, contact technical support (sign in Deep Security as a Service, and click **Support** in the top right-hand corner) for assistance in temporarily deactivating MFA for your account.

Manage trusted certificates

Trusted certificates are used for code signing and SSL connections to external services such as a Microsoft Active Directory and Deep Security Smart Check.

Import trusted certificates

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.

View trusted certificates

1. In the Deep Security Manager, go to **Administration** > **System Settings** > **Security**.
2. Under **Trusted Certificates**, click **View Certificate List**.

Remove trusted certificates

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**.

SSL implementation and credential provisioning

The 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 are possible. If the agent has been activated (either by an administrator or via the agent-initiated activation feature), the full set of interactions are enabled. The Deep Security Manager acts as an HTTP client in all cases, regardless of whether 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 that it is running on.

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.

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 SecurityAgent 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.)

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, 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 will only inform 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 will tell you that software updates are available. However, if **10.0.xxx** (a major version difference) is released and you don't have any **10.0** agents, the alert will *not* appear (even though **10.0**is newer than **9.6.100**).

Updated software packages are automatically imported into Deep Security as a Service and appear on **Administration > Updates > Software > Local**.

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 in your environment. The relays provided as part of Deep Security as a Service are kept up to date and compatible with the latest available agents. However, if you have deployed your own relays, always upgrade them before upgrading your agents.
- Deep Security as a Service customers can ignore the **Minimum DSM Version** for agents. We host and update the manager as part of the service, and it is always compatible with the latest available agents.

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 136)

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.FileNotSignedValidationException: "corrupted_rules.zip." has not been digitally signed by Trend Micro and cannot be imported.
```

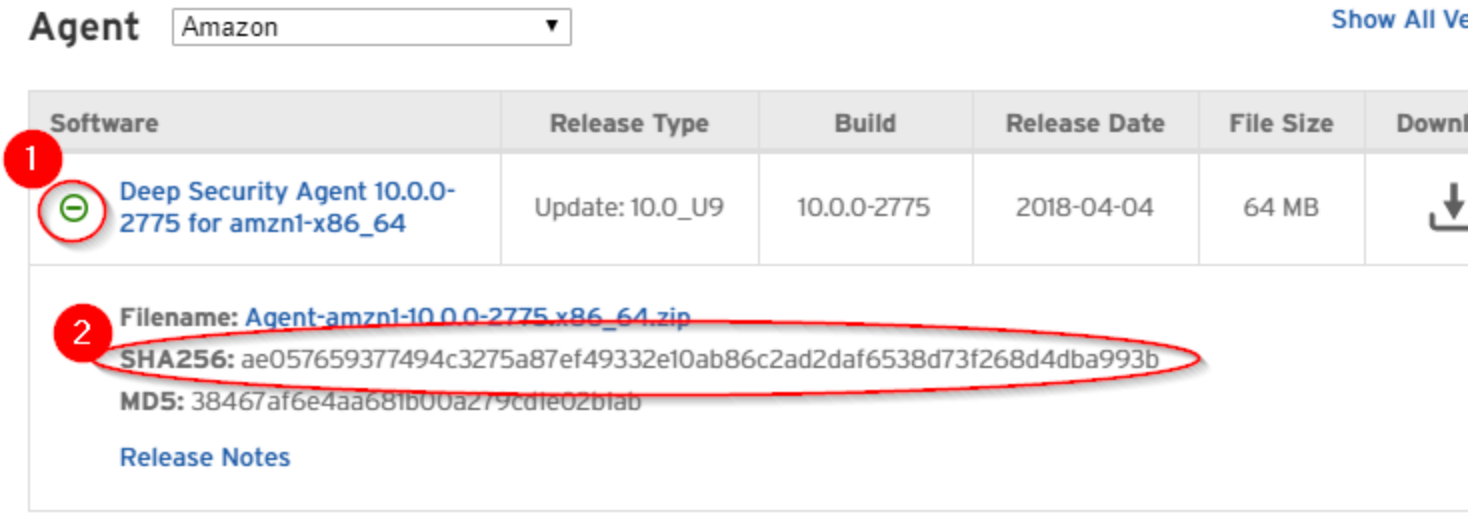
If you manually import a security update package with an invalid digital signature, the manager also displays an error message.

Note: Old security updates that aren't signed will 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.



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 816 and "Configure the update source" on page 819). Then you can:

- "Initiate security updates" below
- "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 956
- "Configure security updates" on page 957

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 991.

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 952.

Configure security updates

You can make the following configurations:

- "Enable automatic patches for rules" below
- "Enable security updates for older agents" below
- "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**[1] **> Settings > General** and in the **Send Policy Changes Immediately** area, select **Automatically apply Rule Updates to Policies**. If it's not selected, you must manually apply downloaded rule updates to policies: go to **Administration > Updates > Security** and click **Apply Rules to Policies**.

Note: By default, changes to policies are automatically applied to computers.

Enable security updates for older agents

For some platforms, Deep Security Manager20 supports older versions. See "Deep Security Agent platforms" on page 80.

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

[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).

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 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 991).
3. Click **Administration > System Settings > Updates**. In the Rules section under Security Updates, make sure **Automatically apply Rule Updates to Policies** is selected.
   For Deep Security as a Service, rule updates are automatically applied by default.
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 954).

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 952 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 966. 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:

- "Upgrade the agent manually" on page 966
- "Upgrade best practices for agents" on page 969

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 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. Upgrade all Deep Security Relays. See "Upgrade Deep Security Relay" on page 961.

   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 1026.

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 "Deep Security Agent Linux kernel support" on page 88

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 1067.
- 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**.

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 836.
2. Continue with "Upgrade the agent from the Computers page" on the next page or "Upgrade the agent manually" on page 966.

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 836.

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 Deep Security as a Service when the agent is activated or reactivated. For details, see "Automatically upgrade agents on activation" on page 853.

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**. In **Agent Self Protection**.
   b. 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 145 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. Export the new agent ZIP from the manager. See "Export the agent installer" on page 145 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. If the computer uses the rpm package manager (Red Hat, CentOS, Amazon Linux, Cloud Linux, SUSE), enter the command:

   ```
   rpm -U <new agent installer rpm>
   ```

   The `-U` argument instructs the installer to perform an upgrade.

---

[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).

4. 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. Export the new agent ZIP from the manager. See "Export the agent installer" on page 145 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 145 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 147.
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 952.

Uninstall Deep Security

Uninstall Deep Security

When you manually uninstall an activated agent from a computer, the computer doesn't notify Deep Security Manager that the software has been uninstalled. On the Computers page in Deep Security Manager, the computer's status will be "Managed (Offline)" or similar, depending on the context. To avoid this, on Deep Security Manager, either:

- Deactivate the agent *before* you uninstall it, or
- Delete the computer from the list *after* you uninstall

Uninstall Deep Security Agent

Uninstall an agent (Windows)

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.

1. Deactivate the agent using the Deep Security Manager by going to the **Computers** page, right-clicking the computer and selecting **Actions** > **Deactivate**.
   If you are unable to deactivate the agent because the Deep Security Manager is unable to communicate with the agent, you will need to do the following before continuing to the next step:
   ```
   C:\Program Files\Trend Micro\Deep Security Agent>dsa_control --selfprotect 0
   ```
2. Go to the Control Panel and select **Uninstall a program**. Look for the Trend Micro Deep Security Agent and then select **Uninstall**.

Alternatively, you can uninstall from the command line:

```
msiexec /x <package name including extension>
```

For a silent uninstall, add `/quiet`.

Uninstall an agent (Linux)

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 instructions below.

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, enter the command:

```
# 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 will be re-enabled when the agent is uninstalled.

---

[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).

If the platform uses Debian package manager (dpkg), such as Debian and Ubuntu, enter the command:

```
$ sudo dpkg -r ds-agent
 Removing ds-agent...
 Stopping ds_agent: .[OK]
```

Uninstall an agent (Solaris 10)

Enter the command:

```
pkgrm ds-agent
```

(Note that uninstall may require a reboot.)

Uninstall an agent (Solaris 11)

Enter the command:

```
pkg uninstall ds-agent
```

Uninstall may require a reboot.

Uninstall an agent (AIX)

Enter the command:

```
installp -u ds_agent
```

Uninstall Deep Security Notifier

From the Windows Control Panel, select **Add/Remove Programs**. Double-click **Trend Micro Deep Security Notifier**, and click **Remove**.

To uninstall from the command line:

```
msiexec /x <package name including extension>
```

For a silent uninstall, add `/quiet`.

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 990.)

The deep-security GitHub repositories contain the following useful scripts:

- CloudFormation templates for deploying Deep Security Manager to AWS.
- Configuration files that contain parsing logic, saved searches, and dashboards for monitoring Deep Security via Splunk.
- 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 also offers many other ways to speed up the protection of your computers and other resources:

- "Schedule Deep Security to perform tasks" on page 991
- "Automatically perform tasks when a computer is added or changed (event-based tasks)" on page 993
- "AWS Auto Scaling and Deep Security" on page 999
- "Use deployment scripts to add and protect computers" on page 1013
- "Automatically assign policies by AWS instance tags" on page 1024
- "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 details, see:

- "Forward Deep Security events to a Syslog or SIEM server" on page 583
- "Set up Amazon SNS" on page 645

Command-line basics

You can use the local command-line interface (CLI) to command both Deep Security Agents and the Deep Security Manager to perform many actions. The CLI can also configure some settings, and to display system resource usage.

Tip: You can also automate many of the CLI commands below using the Deep Security API. To get started with the API, see the First Steps Toward Deep Security Automation guide in the Deep Security Automation Center.

Below are the CLI commands:

- "dsa_control" below
- "dsa_query" on page 988

dsa_control

You can use `dsa_control` to configure some agent settings, and to manually trigger some actions such as activation, anti-malware scans, and baseline rebuilds.

Note: On Windows, when self-protection is enabled, local users cannot uninstall, update, stop, or otherwise control the agent. They must also supply the authentication password when running CLI commands.

Note: `Dsa_control` only supports English strings. Unicode is not supported.

To use `dsa_control`:

In Windows:

1. Open a Command Prompt as Administrator.
2. Change to the agent's installation directory. For example:

   ```
   cd C:\Program Files\Trend Micro\Deep Security Agent\
   ```

3. Run dsa_control:

   ```
   dsa_control <option>
   ```

where `<option>` is replaced with one of the options described in "dsa_control options" below

In Linux:

- `sudo /opt/ds_agent/dsa_control <option>`

  where `<option>` is replaced with one of the options described in "dsa_control options" below

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: `dsm://<host>:<port>/` where: • `<host>` could be either the manager's fully qualified domain name (FQDN), IPv4 address, or IPv6 address • `<port>` is the manager's listening port number 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 978. 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 around the key:value pair are required if it includes spaces or special characters.
`-b, --bundle`	Create an update bundle.

Parameter	Description
`-c <str>, --cert=<str>`	Identify the certificate file.
`-d, --diag`	Generate an agent package. For more detailed instructions, see "Create an agent diagnostic package via CLI on a protected computer" on page 1076.
`-g <str>, --agent=<str>`	Agent URL. Defaults to: `https://localhost:<port>/` where `<port>` is the manager's listening port number.
`-m, --heartbeat`	Force the agent to contact the manager now.
`-p <str>` or `--passwd=<str>`	Authentication password that you might have configured in Deep Security Manager previously. See "Configure self-protection through Deep Security Manager" on page 858 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`. Example: `dsa_control -m -p MyPa$$w0rd` 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. Example: `dsa_control -m -p *`
`-r, --reset`	Reset the agent's configuration. This will remove the activation information from the agent and deactivate it.
`-R <str>, --restore=<str>`	Restore a quarantined file. On Windows, you can also restore cleaned and deleted files.
`-s <num>, --`	Enable agent self-protection (1: enable, 0: disable). Self-

Parameter	Description
`selfprotect=<num>`	protection prevents local end-users from uninstalling, stopping, or otherwise controlling the agent. For details, see "Enable or disable agent self-protection" on page 858. This is a Windows-only feature. **Note:** Although dsa_control lets you enable self-protection, it does not let you configure an associated authentication password. You'll need Deep Security Manager for that. See "Configure self-protection through Deep Security Manager" on page 858 for details. Once configured, the password will need to be entered at the command line using the `-p` or `--passwd=` option. **Note:** 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 user name and password, if the proxy requires authentication. Separate the user name and password by a colon (:). To remove the user name and password, type an empty string (`""`). Basic authentication only. Digest and NTLM are not supported. Note: 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 user name and password, if the proxy requires authentication. Separate the user name and password by a colon (:). To remove the user name and password, type an empty string (`""`). Note: Using `dsa_control -w` only applies to the agent's local

Parameter	Description
	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 (""). See also the -u option. For more information, see "Connect to Deep Security Manager via proxy" on page 809. Note: Using `dsa_control -x` only applies to the agent's local configuration. No security policy is changed on the 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 (""). See also the -w option. For more information, see "Connect to Deep Security Relays via proxy" on page 810. Note: 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.

Parameter	Description
`--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.

Note: 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 852.

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 (443).

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. Cancels an on-demand ("manual") scan that is currently occurring on the computer.	`"AntiMalwareCancelManualScan:true"`	no	yes
`AntiMalwareManualScan`	Boolean. Initiates an on-demand ("manual") anti-malware scan on the computer.	`"AntiMalwareManualScan:true"`	no	yes
`description`	String. Sets the computer's description. Maximum length 2000 characters.	`"description:Extra information about the host"`	yes	yes
`displayname`	String. Sets the display name shown in parentheses next to the hostname on **Computers**. Maximum length 2000	`"displayname:the_name"`	yes	yes

Parameter	Description	Example	Use during Activation	Use during Heartbeat
	characters.			
`externalid`	Integer. 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
`group`	String. Sets which group the computer belongs to on **Computers**. Maximum length 254 characters per group name per hierarchy level. The forward slash ("/") indicates a	`"group:Zone A web servers"`	yes	yes

Parameter	Description	Example	Use during Activation	Use during Heartbeat
	group hierarchy. The `group` parameter can read or create a hierarchy of groups. This parameter can only be used to add computers to standard groups under the main "Computers" 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. Maximum	`"hostname:www1"`	yes	no

Parameter	Description	Example	Use during Activation	Use during Heartbeat
	length 254 characters. The hostname can specify an IP address, hostname or FQDN that the manager can use to connect to the agent.			
`IntegrityScan`	Boolean. Initiates an integrity scan on the computer.	`"IntegrityScan:true"`	no	yes
`policy`	String. Maximum length 254 characters. The policy name is a case-insensitive match to the policy list. If the policy is not found, no policy will be assigned. A policy	`"policy:Policy Name"`	yes	yes

Parameter	Description	Example	Use during Activation	Use during Heartbeat
	assigned by an event-based task will override a policy assigned during agent-initiated activation.			
`policyid`	Integer.	`"policyid:12"`	yes	yes
`relaygroup`	String. Links the computer to a specific relay group. Maximum length 254 characters. 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 will be used.	`"relaygroup:Custom Relay Group"`	yes	yes

Parameter	Description	Example	Use during Activation	Use during Heartbeat
	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.
	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.
		`"tenantID:12651ADC-D4D5"`
		`and`
		`"token:8601626D-56EE"`
			yes	yes

`RecommendationScan`	Boolean. Initiate a recommendation scan on the	`"RecommendationScan:true"`	no	yes

Parameter	Description	Example	Use during Activation	Use during Heartbeat
	computer.			
`UpdateComponent`	Boolean. Instructs Deep Security Manager to perform a security update. When using the `UpdateComponent` parameter on Deep Security Agent 12.0 or later, make sure the Deep Security Relay is also at version 12.0 or later. Learn more.	`"UpdateComponent:true"`	no	yes
`RebuildBaseline`	Boolean. Rebuilds the Integrity Monitoring baseline on the computer.	`"RebuildBaseline:true"`	no	yes
`UpdateConfiguration`	Boolean. Instructs Deep Security Manager to	`"UpdateConfiguration:true"`	no	yes

Parameter	Description	Example	Use during Activation	Use during Heartbeat
	perform a "Send Policy" operation.			

Activate an 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

```
/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

```
/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

```
/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 1076.

Note: 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 will remove the activation information from the target agent and deactivate 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

```
/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 <string>`	Authentication password used with the optional agent self-protection feature. Required if you specified a password when enabling self-protection. **Note:** For some query-commands, authentication can be bypassed directly, in such case, password is not required.
`-c,--cmd <string>`	Execute query-command against the agent. The following commands are supported: • `"GetHostInfo"`: to query which identity is returned to the manager during a heartbeat • `"GetAgentStatus"`: to query which protection modules are enabled, the status of Anti-Malware or Integrity Monitoring scans in progress, and other miscellaneous information • `"GetComponentInfo"`: to query version information of anti-malware patterns and engines • `"GetPluginVersion"`: to query version information of the agent and protection modules
`-r,--raw <string>`	Returns the same query-command information as `"-c"` but in raw data format for third party software interpretation.

Parameter	Description
`pattern`	Wild card pattern to filter result. Optional. **Example:** `dsa_query -c "GetComponentInfo" -r "au" "AM*"`

Check CPU usage and RAM usage

Windows

Use the Task Manager or procmon.

Linux

```
top
```

Check that ds_agent processes or services are running

Windows

Use the Task Manager or procmon.

Linux

```
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.

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.

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.

Deep Security as a Service performs some tasks (for example, backup and checking for software updates) automatically.

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.

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 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.

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).)

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

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 998, 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, seehttps://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 or GCP labels that have been added to your AWS or GCP instances.

  Note: This match condition is only available for AWS instances and GCP VMs added to the manager through **Computers > Add >** [**Add AWS 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 only match on AWS and GCP vendors.

  Note: Cloud Vendor only works if you added your cloud instances to the manager through **Computers > Add >** [**Add AWS 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+ **or** FIN-.*
RD-ABCD	RD-\w+ **or** RD-.*
AB **or** ABC **or** ABCCCCCCCCC	ABC*
Microsoft Windows 2003 **or** Windows XP	.*Windows.*
Red Hat 7 **or** 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

If multiple event-based tasks are triggered by the same condition, the tasks are executed in alphabetical order by task name.

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 852

- 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.

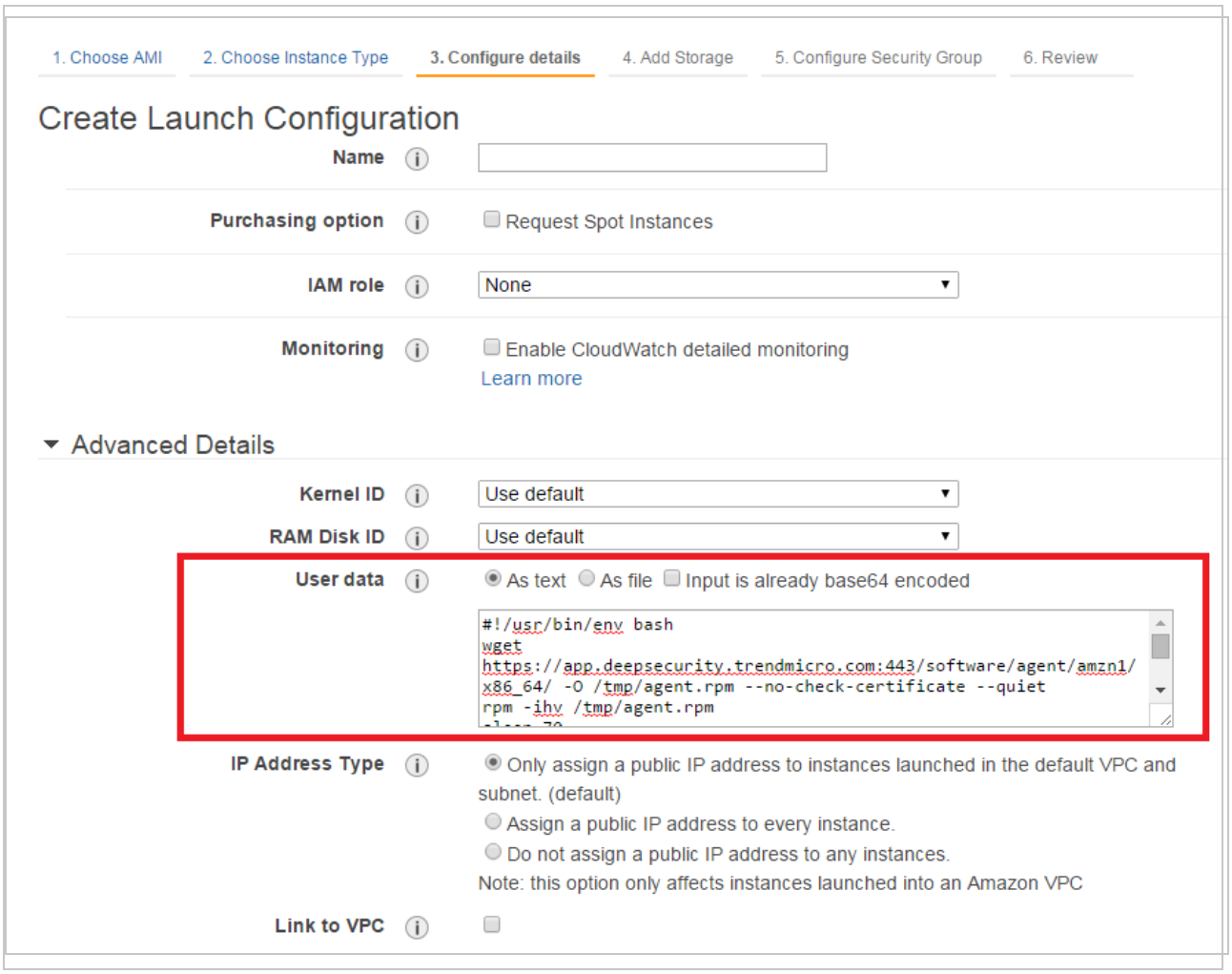
Tip: You can generate deployment scripts to automate the agent installation using the Deep Security API. For more information, see Generate an agent deployment script.

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 852.

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**.



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 171 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" on the next page
- "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 187.

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 1013. 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" below 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 852.

- 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.

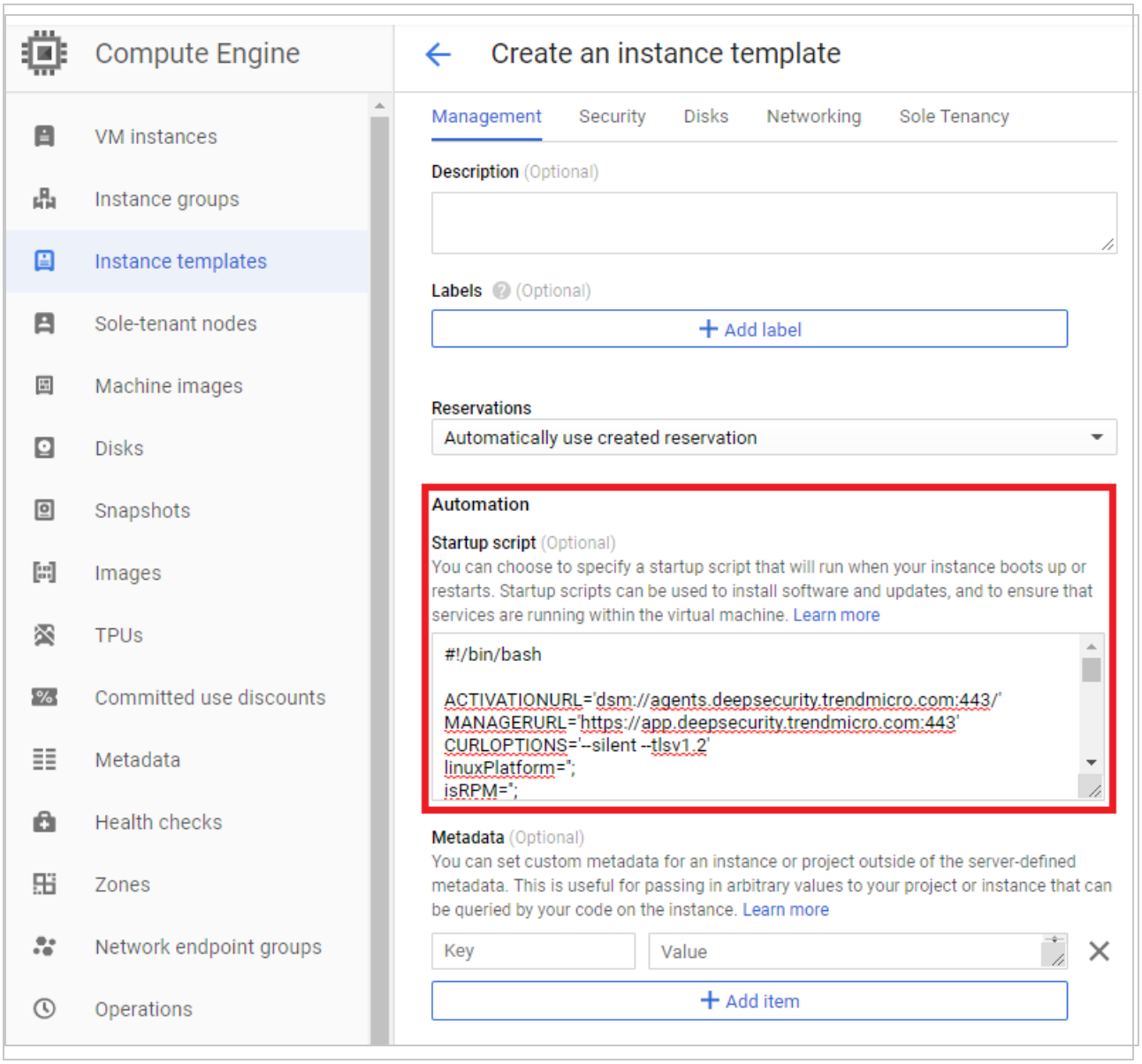
In order for the deployment script to work:

- 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 852.

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**.



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 199 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 your agent version control settings are configured as desired. See "Configure agent version control" on page 836 for details.
   b. 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 852 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**.

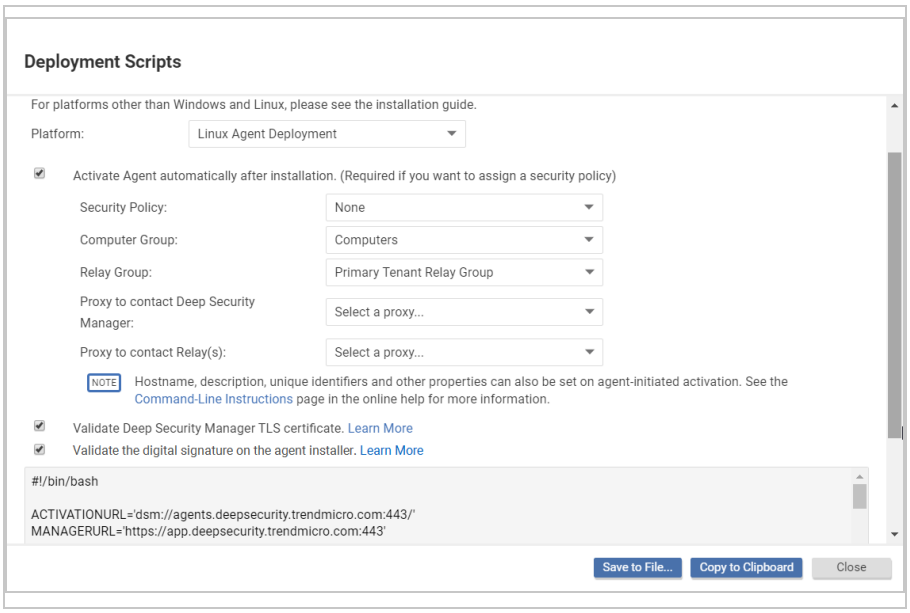
   Agents must be activated before you apply a policy to protect the computer. Activation registers the agent with the manager during an initial communication.

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.

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 140 and "Check the signature on a DEB file" on page 142.
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**.



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, remove the `--tls1.2` tag (Linux) or `[Net.ServicePointManager]::SecurityProtocol =`

`[Net.SecurityProtocolType]::Tls12;` line (Windows) 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 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.
- 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 836 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" below.
- 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" below.

URL format for download of the agent

The Deep Security Agent software package can be downloaded from Deep Security as a Service, 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 Deep Security as a Service 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 Deep Security as a Service, which is `app.deepsecurity.trendmicro.com`. Deep Security as a Service can be used for testing any of the examples provided in this topic.

<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 Red Hat Enterprise Linux, CentOS, Oracle, CloudLinux, Amazon Linux, SUSE	`agent.rpm`
Linux Debian, Ubuntu	`agent.deb`
Windows	`agent.msi`

Platform	<filename>
AIX	`agent.bff.gz`
Solaris 11+	`agent.p5p.gz`
Solaris 10 or earlier	`agent.pkg.gz`

Note: Deep Security as a Service 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 Deep Security as a Service 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 LTS agent released by Trend Micro 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.

  the latest LTS agent 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 1023.

<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

Platform	Distribution	<platform>	<arch>	<filename>	Example
	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
	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

Platform	Distribution	<platform>	<arch>	<filename>	Example
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 Updates 7-11	Solaris_5.10_U7	x86_64	agent.pkg.gz	/software/agent/Solaris_5.10_U7/x86_64/agent.pkg.gz
		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

Platform	Distribution	<platform>	<arch>	<filename>	Example
	AIX 6.1 (Deep Security Agent 9.0)	AIX_6.1	power pc	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	power pc	agent.bff.gz	/software/agent/AIX_7.1/powerpc/agent.bff.gz
	AIX 6.1, 7.1, 7.2 (Deep Security Agent 12 and up)	AIX	power pc	agent.bff.gz	/software/agent/AIX/powerpc/agent.bff.gz

Examples

Without `<agent version>`:

- `https://app.deepsecurity.trendmicro.com/software/agent/RedHat_EL7/x86_64/agent.rpm`
- `https://app.deepsecurity.trendmicro.com/software/agent/Windows/x86_64/agent.msi`

With `<agent version>`:

- `https://app.deepsecurity.trendmicro.com/software/agent/RedHat_EL7/x86_64/12.0.0.481/agent.rpm`
- `https://app.deepsecurity.trendmicro.com/software/agent/Windows/x86_64/12.0.0.481/agent.msi`

Exceptions for backwards compatibility

If no `<filename>` is provided after `[...]/<platform>/<arch>/`, Deep Security as a Service 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), Deep Security as a Service will return the agent download for that platform as described in the table above.

Examples:

- `https://app.deepsecurity.trendmicro.com/software/agent/RedHat_EL7/x86_64/`
- `https://app.deepsecurity.trendmicro.com/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

Examples

For examples, refer to the sample deployment script generated from Deep Security as a Service. 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 by AWS instance tags

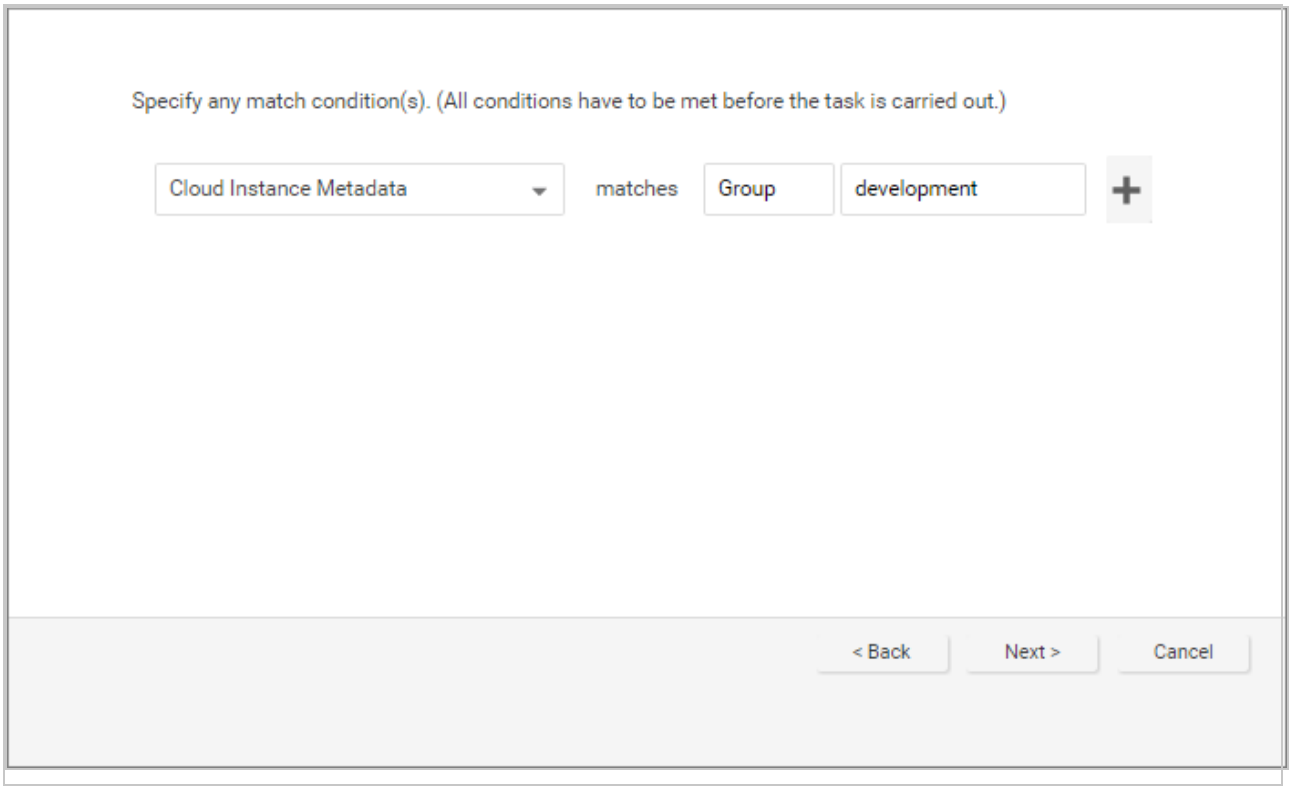
AWS tags allows you to categorize your resources by assigning metadata to AWS EC2 instances in the form of keys and values. You can also tag Amazon WorkSpaces with the similar key and value pair. Deep Security can use this metadata to trigger the automatic assigning of a policy to a Deep Security Agent 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** and **development** into the key and value fields, and click **Next**.



5. 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 page 1034
- "GDPR" on page 1034
- Set up AWS Config Rules
- "Bypass vulnerability management scan traffic in Deep Security" on page 1035
- "Use TLS 1.2 with Deep Security" on page 1037

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.	If you do **not** have a Deep Security Relay in your environment: 1. "Create a diagnostic package and logs" on page 1075 and send it to the Trend Micro support team. If you **have** a Deep Security Relay in your

ID	Event	Reason	Solution
			environment: 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" below and "Upgrade Deep Security Relay" on page 961 accordingly. Confirm signature files sync to your update source. 2. Confirm your signature files have synced to your update source. 3. Attempt to upgrade your agent or send your updated policy again. 4. If the issue isn't resolved, "Create a diagnostic package and logs" on page 1075 and send it to the Trend Micro support team.
5300	Agent/Plugin package signature validation failed.	The agent package might have been tampered with or something is wrong on the package.	"Create a diagnostic package and logs" on page 1075 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

	Deep Security 20	Deep Security Feature Release	Deep Security 12
Supported Deep Security Relay	Deep Security Agent 20	**Windows** - Deep Security Agent FR 2020-04-16 (12.5.0.834)	Deep Security Agent 12.0 update 8 (12.0.0.967)

	Deep Security 20	Deep Security Feature Release	Deep Security 12
version		**Linux** - Deep Security Agent FR 2020-05-19 (12.5.0.936)	

Deep Security Trust Center

As a global leader in security, Trend Micro develops innovative security solutions that make the world safe for businesses and consumers to exchange digital information. With more than 30 years of security expertise, we're recognized as the market leader in server security, cloud security, and small business content security.

Trend Micro Deep Security as a Service provides world-class security to cloud workloads. This offering is hosted through Amazon Web Services (AWS) and offers workload protection through the installation of Deep Security Agents.

Deep Security as a Service is committed to earning and preserving the trust of our customers. The following resources demonstrate our commitment to security, privacy, transparency, and compliance to industry-recognized standards.

 Compliance	 Privacy	 Security
"PCI DSS " below "ISO 27001 " on the next page	"GDPR" on the next page Deep Security as a Service Data Collection Notice Privacy Policy	"FAQ" on the next page

PCI DSS

Deep Security as a Service is certified as a PCI DSS level 1 service provider.

Coalfire, a Qualified PCI Auditor, has certified Deep Security as a Service according to version 3.2 of the PCI Data Security Standard. The Attestation of Compliance is available on request. AWS is also PCI certified.

For more information, see "Meet PCI DSS requirements with Deep Security" on page 1034.

ISO 27001

ISO 27001 is an internationally recognized security standard that outlines the requirements for information security management systems. Deep Security as a Service has been added to the Trend Micro ISO 27001 certification, as of December 2018. You can view the ISO 27001 certificate on the Trend Micro product certifications site.

GDPR

Trend Micro and Deep Security as a Service were ready for, and have met, all of our obligations under GDPR for May 25th 2018. One key item to note for Deep Security as a Service is that, as a data processor under GDPR, our processing of 'personal data' is limited.

- Where appropriate, we implement Technical and Organization Measures (“TOMs”) to support our processing of data under GDPR.
- Details on the data processed by Deep Security as a Service, and the controls available to you over that data, are documented in the Deep Security as a Service Data Collection Notice.

For more information, see the Trend Micro GDPR Compliance site and see "Privacy and personal data collection disclosure" on page 1040 for information about personal data collection in Deep Security as a Service.

FAQ

How are security logs monitored?

> Deep Security protection modules generate security events for the Deep Security as a Service production workloads. Security events collected from Deep Security as a Service are forwarded to a central SIEM. Security events are generated for all relevant protection modules: Anti-Malware, Firewall, Intrusion Prevention, Integrity Monitoring,

Log Inspection. Additional AWS logs (CloudTrail, CloudWatch), system, and database logs are forwarded to the SIEM. Access to Deep Security event management console and SIEM is restricted based on roles.

Deep Security as a Service enables automated alerts and employs 24/7 on-call staff. Security logs are reviewed for all systems on a daily basis. If a security incident is suspected, it is immediately reported to the Trend Micro Security Operations Center (SOC). This potential incident is prioritized based on the severity of the suspected incident, and a team from the SOC, as well as technical experts, is assigned to investigate.

How are Trend Micro employees trained?

All Trend Micro employees undergo a security awareness training course upon being hired and on a yearly basis. All employees must adhere to Trend Micro's Internet, Computer, Remote Access and Mobile device acceptable use policies. Failure to comply with these policies may result in disciplinary actions which could include termination.

All new employees and contractors are required to complete a criminal background check.

What are Trend Micro's password policies and standards?

Trend Micro adheres to the following password polices and standards:

- All passwords must be changed at least on a quarterly basis.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Passwords must not be shared or revealed to anyone.
- Passwords must be changed immediately if compromise is suspected.
- Passwords must be encrypted during transmission and stored hashed with a salt.
- Passwords must be at least eight alphanumeric characters long.
- Passwords must contain both upper and lower case characters (for example, a-z, A-Z).

- Password reuse prevention is enforced.
- Passwords must not be based on personal information, names of family, and so on.

How is access to Trend Micro's infrastructure controlled?

Remote access to Trend Micro’s infrastructure is strictly controlled and monitored. All authentication methods use industry best practices and standards, and include such things as certificate based authentication and multi-factor authentication. Where appropriate, single sign-on (SSO) that leverages Trend Micro's Active Directory is used.

How does Trend Micro handle sensitive information?

In relation to the Deep Security as a Service environment, Trend Micro primarily handles data that is collected through the protection policy and security events. Each tenant's information is separated using a dedicated database schema. Access and storage of this information is strictly controlled and is used for diagnostic and support purposes only. Client contact details, such as their email address, are retained encrypted at rest for client management purposes.

What change control practices does Deep Security as a Service follow?

Application upgrades within the Deep Security as a Service environment are completed after meeting our quality objectives. Trend Micro uses best practices for changes, including full backups and approval processes. Deep Security as a Service has multiple dedicated development and testing environments.

Any changes requested are first reviewed by technical stakeholders to determine the urgency and potential impact of the changes. All changes require a documented back-out plan. These changes are tracked and recorded in a change control system.

How is communication secured?

All communication between customers, software, and infrastructure is encrypted using

---

industry-accepted ciphers and algorithms. These ciphers and algorithms are reviewed continuously to determine whether adjustments should be made, such as the deprecation of old or insecure ciphers and cipher suites. To take advantage to these improvements, customers must ensure that their agents are updated regularly.

Encryption keys are stored in AWS KMS. Only a limited number of Deep Security as a Service team member have access to the KMS.

How does Trend Micro handle physical security?

All access to Trend Micro offices and networks is strictly controlled to authorized or accompanied individuals only. Access is given through a key card system and approval is required before entry is granted into sensitive areas. The Deep Security as a Service infrastructure is hosted in AWS.

What is the Trend Micro incident response plan?

Trend Micro has a dedicated Information Security (InfoSec) team that is responsible for ensuring compliance with Trend Micro security policies. Deep Security as a Service engineers immediately contact the InfoSec team when a security incident is discovered. In addition, InfoSec independently monitors Deep Security as a Service environment logs.

If a security incident is discovered, the incident is prioritized based on severity. A dedicated team of technical experts is assigned to investigate, advise on containment procedures, perform forensics, and manage communication.

Following an incident, the team examines the root cause, and revises the response plan accordingly.

In the event of a breach involving customer data, Trend Micro will follow its obligations under GDPR. For more information, see https://www.trendmicro.com/en_ca/business/capabilities/solutions-for/gdpr-compliance/our-journey.html.

Does Deep Security as a Service conduct vulnerability and penetration testing?

Vulnerability scans of the Deep Security as a Service production environment are

---

performed weekly by a PCI authorized scanning vendor (ASV), Tenable.io. A PCI ASV attestation is obtained quarterly. The same vendor is used for automated weekly internal scans of the Deep Security as a Service Virtual Private Cloud (VPC).

Deep Security software and the Deep Security as a Service production environment undergo yearly penetration tests conducted by third-party security experts to detect and rectify common security issues. The scope of the third-party penetration tests includes application security tests, internal and external network scans, and network segmentation tests.

Trend Micro InfoSec conducts web application assessments of the Deep Security Manager application for any major release and at least annually using leading dynamic analysis security tools.

The Deep Security code base is scanned weekly using a leading static analysis security tool. The development team receives automated alerts if new issues are identified, and a clean scan is a requirement for each product release.

Third-party components included with Deep Security are monitored continuously using a leading software composition analysis tool. Scans are executed as part of nightly builds to automatically detect newly introduced third-party software.

Does the development team follow secure coding practices?

Deep Security software developers are trained in secure coding practices using an industry-standard curriculum based on SANS 25/OWASP Top 10/PCI 6.5. Education campaigns are conducted on an annual basis and when an employee joins the company.

The Deep Security development team employs specialized staff to handle product security.

Security testing, secure code review, and threat modeling are part of the development lifecycle.

How are vulnerabilities and patches handled?

Vulnerabilities are continuously monitored and tracked. Each vulnerability is assigned a

---

CVSS score. Patching requirements that specify time frames for addressing a vulnerability according to CVSS-based severity are included in the Secure Development Compliance Policy. The Deep Security software in the Deep Security as a Service environment is updated weekly to use the latest available code base, including vulnerability fixes.

The Deep Security as a Service team is responsible for patching the Deep Security software and supporting AWS services. The client is responsible for updating the Deep Security Agents deployed on client workloads.

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. Coalfire (a PCI auditor) has written a commissioned white paper that examines how Trend Micro Deep Security can be used to help secure Payment Card Industry (PCI) data in accordance with the PCI Data Security Standard (PCI DSS).

For more information, see the white paper Using Trend Micro's Hybrid Cloud Security Solution to Meet PCI DSS 3.2 Compliance.

Tip: For information on how to:
- accelerate PCI DSS compliance in AWS, see Accelerating PCI Compliance in AWS using Deep Security.
- enable TLS 1.2 for PCI compliance, see "Use TLS 1.2 with Deep Security" on page 1037.

Trend Micro Deep Security as a Service is now a PCI DSS Level 1 Service Provider. This means you can further streamline your PCI DSS certification process and take more items off of your to do list. For more information, see Trend Micro Deep Security as a Service Achieves PCI DSS Level 1 Certification.

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 as a Service, see "Privacy and personal data collection disclosure" on page 1040.

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 1037

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.

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

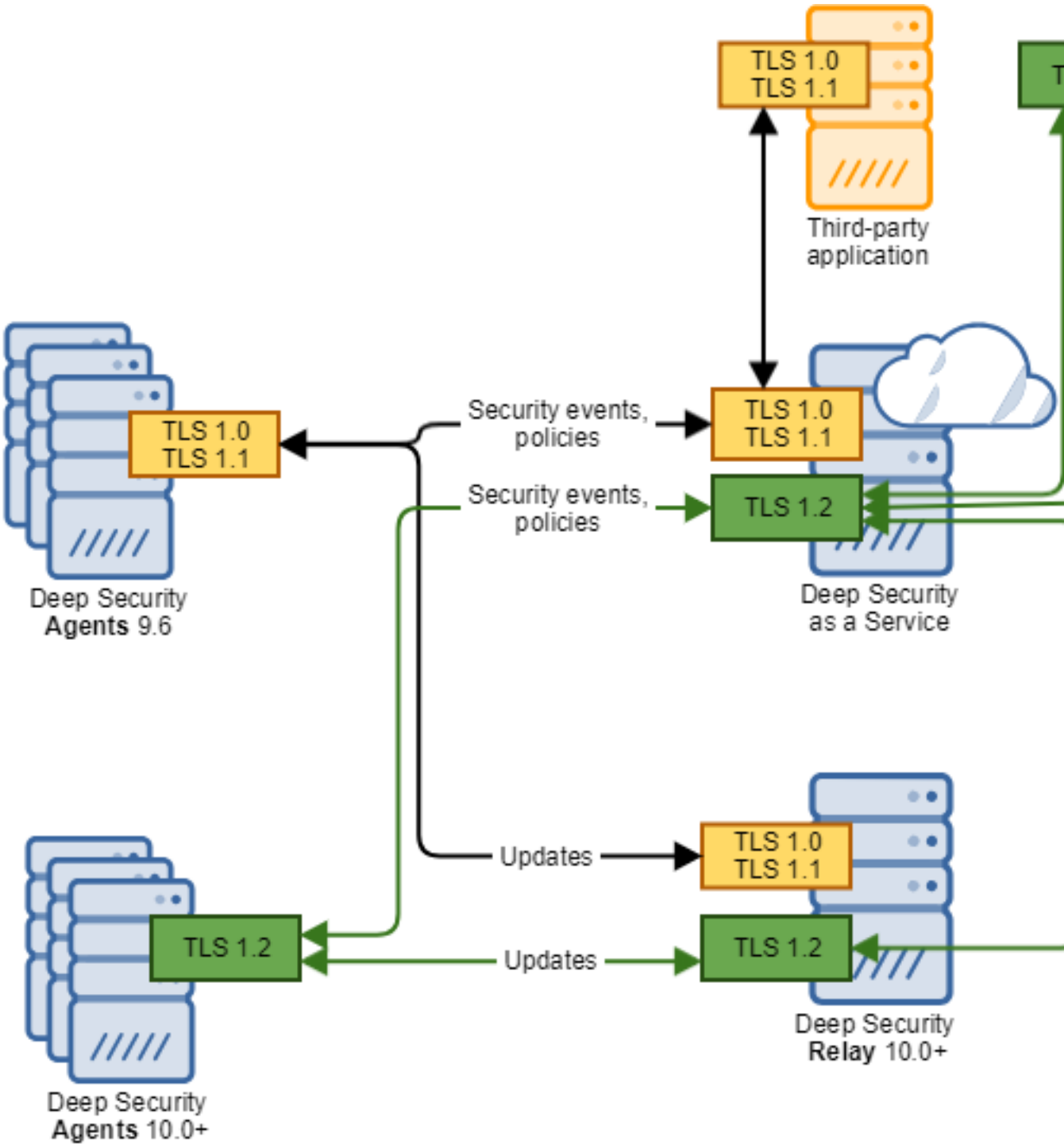
In Deep Security Manager 11.1 and higher, TLS 1.2 is enforced by default for new installations.

Topics on this page:

TLS architecture

Figure 1 shows the TLS communication in a Deep Security as a Service environment. You can see that 10.0 or higher agents communicate with Deep Security as a Service over TLS 1.2, while 9.6 versions communicate over early TLS. Similarly, newer third-party applications use TLS 1.2, while older ones use early TLS.

Figure 1: TLS communication in a Deep Security as a Service environment


TLS 1.0
TLS 1.1
Third-party
application
TLS 1.0
TLS 1.1
Deep Security
Agents 9.6
Security events,
policies
TLS 1.0
TLS 1.1
Security events,
policies
TLS 1.2
Deep Security
as a Service
Updates
TLS 1.0
TLS 1.1
TLS 1.2
Updates
TLS 1.2
Deep Security
Relay 10.0+
Deep Security
Agents 10.0+

Enable the TLS 1.2 architecture

To enable TLS 1.2 in your Deep Security as a Service environment, you may need to upgrade your agents and relays. Follow these guidelines:

- If you have 9.6 agents in your environment, you must upgrade them to 10.0 or later. Only 10.0 or later agents support TLS 1.2.
- If you have 9.6 relays in your environment, you must upgrade them to 10.0 or later. Only 10.0 or later relays support TLS 1.2.

First, upgrade your agents:

- See "Upgrade Deep Security Agent" on page 962.

Next, upgrade your relays:

- See "Upgrade Deep Security Relay" on page 961.

Next steps (deploy new agents and relays)

After setting up your TLS 1.2 environment, if you decide to "Use deployment scripts to add and protect computers" on page 1013 (among other methods) to deploy new agents and relays, adhere to the guidelines below.

Guidelines for using deployment scripts

1. If you are deploying an agent or relay onto Windows computers, use PowerShell 4.0 or higher, which uses TLS 1.2 to communicate with the manager or relay to obtain agent software and install it.
2. If you are deploying an agent or relay onto Linux, use curl 7.34.0 or higher. This version uses TLS 1.2 to communicate with the manager or relay to obtain agent software and install it.
3. If you are deploying onto Red Hat Enterprise Linux 6 which uses curl 7.19 by default, upgrade to curl 7.34.0 or later. If you can't upgrade curl, see the next step for a workaround.
4. If you are deploying onto Windows XP, 2003, or 2008, where PowerShell 4.0 is not supported, remove these lines:

```
#requires -version 4.0
```

```
[Net.ServicePointManager]::SecurityProtocol =
[Net.SecurityProtocolType]::Tls12;
```

OR

If you are deploying onto Red Hat Enterprise Linux 6, which uses curl 7.19 by default, remove this tag:

```
--tls1.2
```

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 as a Service 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

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. 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 891.
2. 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.
3. In the lifecycle template, enter your API Key generated in step 1. . Leave the FQDN of your console as the default entry.
4. 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.

5. Once all your accounts have been imported, "Install the agent" on page 146 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 180.

Integrate with AWS PrivateLink

AWS PrivateLink allows you to configure your AWS deployment to use AWS private connectivity, rather than the public internet, for data connections between any instances or applications running in AWS and Deep Security as a Service.

Connecting to Deep Security as a Service without AWS PrivateLink

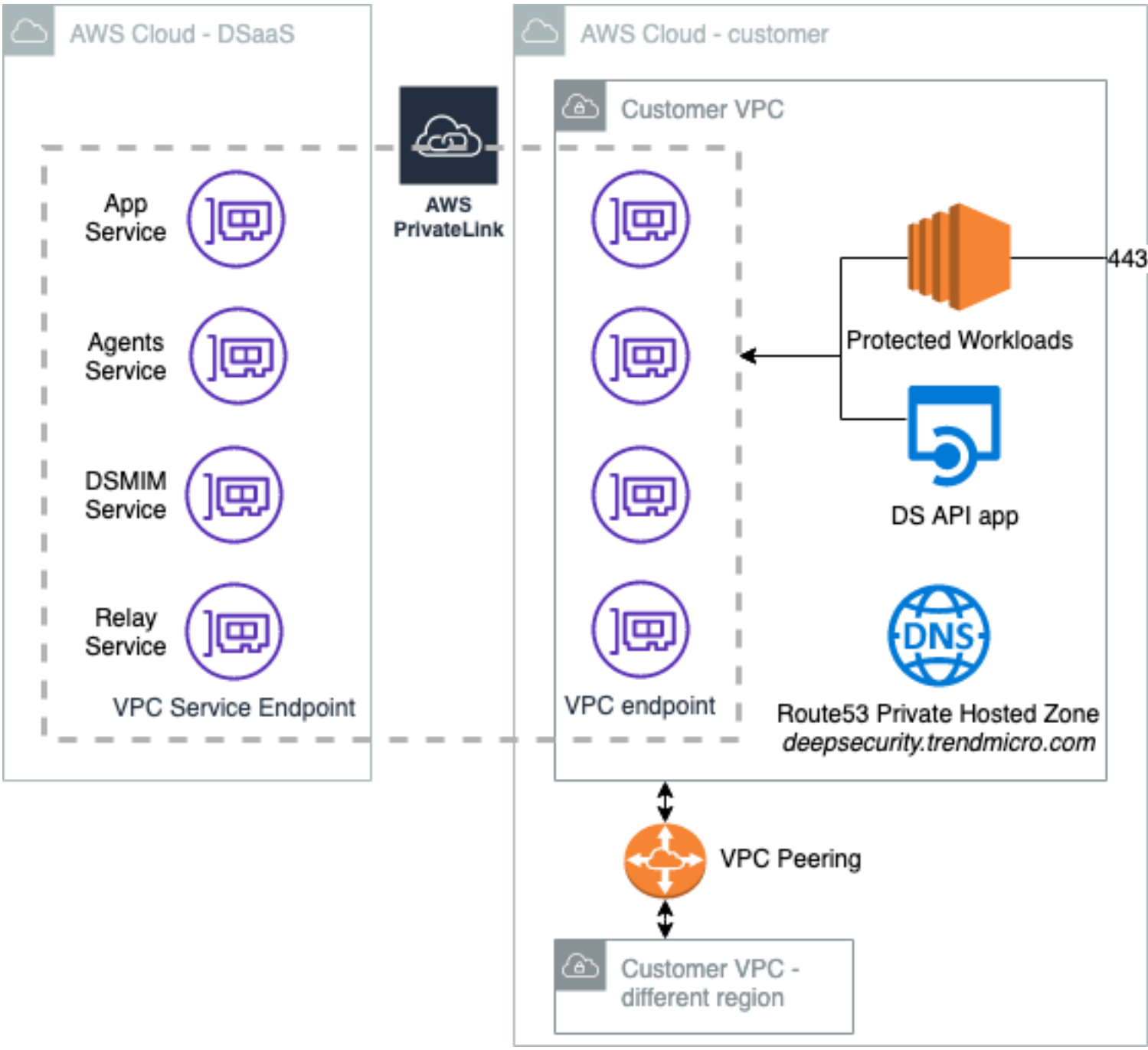
The standard deployment model for Deep Security as a Service requires that the data connections from Deep Security Agents, any API-based applications, and browser-based administrative access for the four services listed below are accessed from the public internet.

Service address (internet-facing)	Description
relay.deepsecurity.trendmicro.com	Deep Security Agent retrieval of security updates and packages
agents.deepsecurity.trendmicro.com	Deep Security Agent Traffic

Service address (internet-facing)	Description
dsmim.deepsecurity.trendmicro.com	Deep Security Agent Traffic
app.deepsecurity.trendmicro.com	API and browser-based administrative access

For a full list of Deep Security as a Service network requirements, see "Port numbers, URLs, and IP addresses" on page 106.

How does AWS PrivateLink work with Deep Security as a Service?



When using AWS PrivateLink with Deep Security as a Service, the four services listed in the table above are accessed as VPC Service Endpoints.

Using AWS Route53 and VPC services, a private DNS hosted zone transparently routes traffic going to those four services to the private VPC Service Endpoint addresses directly, rather than to the public internet.

For example, when using PrivateLink for Deep Security as a Service, agents.deepsecurity.trendmicro.com resolves to the private IP of the VPC Services Endpoint instead of mapping to a public IP address. As a result, connections from the Deep Security Agent terminate on the VPC service endpoint and are routed using AWS PrivateLink rather than the public internet.

VPC Service Endpoints for use with AWS PrivateLink

Service address	Description	VPC Service Endpoint for use with AWS PrivateLink
relay.deepsecurity.trendmicro.com	Deep Security Agent retrieval of security updates and packages	com.amazonaws.vpce.us-east-1.vpce-svc-0ca160f19663f348e
agents.deepsecurity.trendmicro.com	Deep Security Agent Traffic	com.amazonaws.vpce.us-east-1.vpce-svc-0ecb2dc36c34b3aef
dsmim.deepsecurity.trendmicro.com	Deep Security Agent Traffic	com.amazonaws.vpce.us-east-1.vpce-svc-01a733ad6b4b0afc1
app.deepsecurity.trendmicro.com	API and browser-based administrative access	com.amazonaws.vpce.us-east-1.vpce-svc-04912367f0b0c73d9

Note: Even when using AWS PrivateLink, Deep Security Agent traffic not listed in the table above (for example, traffic destined for the Trend Micro Smart Protection network) must still be routed from your VPCs directly to the internet. For a complete list of Deep Security as a Service network requirements, see "Port numbers, URLs, and IP addresses" on page 106.

Deep Security as a Service VPC Service Endpoint region support

Deep Security as a Service provides VPC Service Endpoints in all availability zones for the **us-east-1 (North Virginia)** region:

- us-east-1a (use1-az1)
- us-east-1b (use1-az2)
- us-east-1c (use1-az4)
- us-east-1d (use1-az6)
- us-east-1e (use1-az3)
- us-east-1f (use1-az5)

Configure PrivateLink for use with Deep Security as a Service

1. Create a VPC Endpoint in **us-east-1** for each of the services provided by Deep Security as a Service. See the table above for the four services.
2. Ensure DNS hostnames and DNS resolution are enabled on your VPC.
3. Configure a private hosted zone for the **deepsecurity.trendmicro.com** domain. Add an A alias entry for each service that Deep Security as a Service exposes (relay, agents, dsmim, app) that maps to the VPC endpoints you created in step 1.
4. Use a tool like nslookup to verify that service DNS addresses are now pointing to private IPs (rather than to the public internet addresses).

What if my traffic originates from a region without a VPC service endpoint?

If you have traffic originating from regions outside of us-east-1 (which means there is no corresponding Deep Security as a Service VPC service endpoint available in that region), you can use VPC peering to connect VPCs from other regions or AWS accounts to a VPC that you host in us-east-1. That VPC then forwards traffic to the Deep Security as a Service PrivateLink service endpoints that are exposed by Trend Micro. AWS provides an example of this type of configuration.

You must still enable DNS hostnames and DNS resolution on all VPCs that will use AWS PrivateLink, as well as configure Route53 records for DNS resolution (steps 2 and 3 in "Configure PrivateLink for use with Deep Security as a Service" on the previous page).

For more information on using VPC peering, see What is VPC Peering? in the AWS documentation.

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 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 > Instances & Nodes > 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 Apex Central

You can integrate Deep Security as a Service and Trend Micro Apex Central (formerly "Control Manager"). Once integrated:

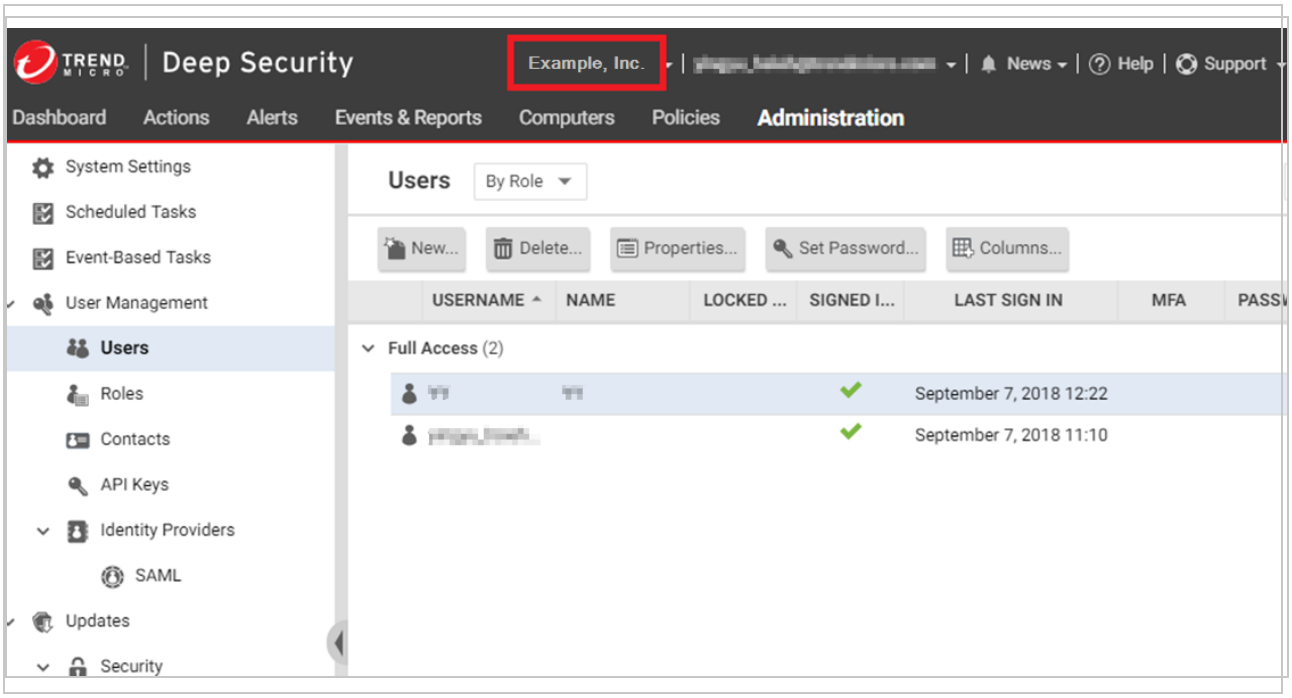
- the Deep Security widgets appear in Apex Central.
- the Deep Security logs appear in Apex Central and can be queried.

Note: Deep Security as a Service does not support the Connected Threat Defense feature when integrated with Apex Central.

To integrate these products:

1. Add Deep Security as a Service to Apex Central by following these instructions.
2. When following the instructions, adhere to these guidelines:
   - From the **Server Type** drop-down list, select **Deep Security**.
   - In the **Server** field, enter the Deep Security as a Service URL, which is https://app.deepsecurity.trendmicro.com.
   - In the **Display name** field, enter a friendly name for your Deep Security as a Service account.
   - In the **User name** field, enter the user name of a Deep Security as a Service user with at least auditor privileges.

- In the **Password** field, enter the Deep Security as a Service user's password.
- In the **Tenant Name** field, enter your Deep Security as a Service account name, which is typically your organization's name. This name is displayed at the top of the Deep Security as a Service application (see the image below).



Integrate with Smart Protection Server

If you have Deep Security Agents in AWS, and you want them to be able to access Trend Micro's Smart Protection Network, then you must allow them to connect to the Internet on port 80 (HTTP) or 443 (HTTPS). (See "Port numbers, URLs, and IP addresses" on page 106.) If this is not possible, you can deploy your own Smart Protection Server (SPS) within your Virtual Private Network (VPC) in AWS, or another VPC. The Smart Protection Server connects outbound to the Smart Protection Network to retrieve the latest anti-malware, file reputation, and web reputation information and then passes this information along to your agents.

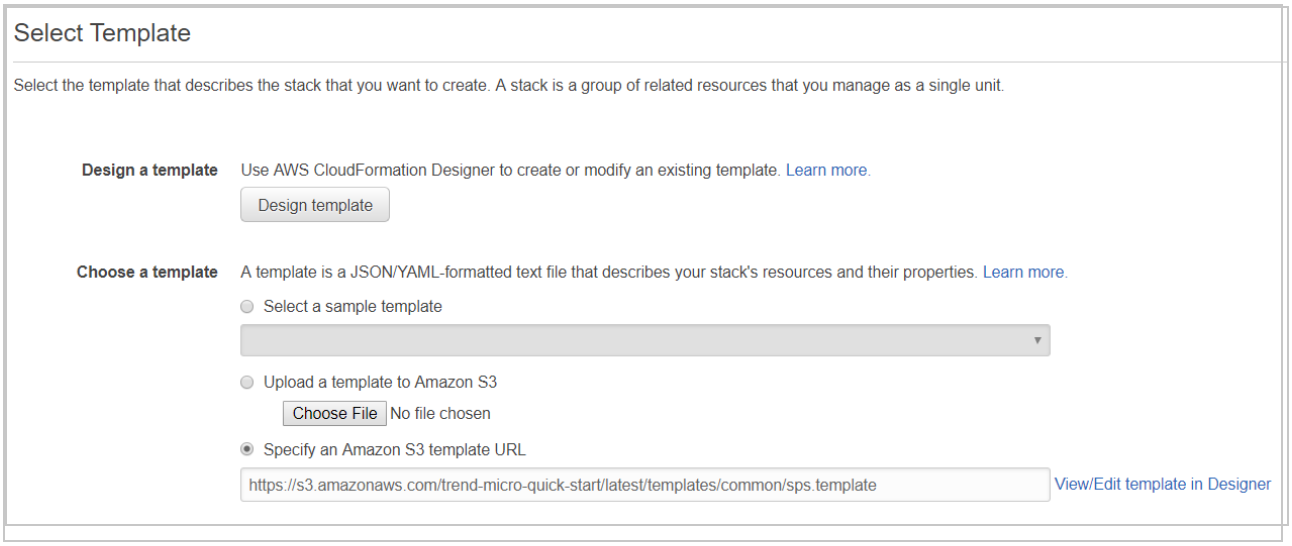
To deploy a Smart Protection Server in AWS, you can either:

- use an AWS CloudFormation template created by Trend Micro . This is the easiest way to deploy the server because the configuration is automated.
- install it manually. See the Smart Protection Server documentation for details.

The instructions below describe how to deploy the Smart Protection Server using the CloudFormation template.

1. In AWS, at the top, click **Services** and search for the **CloudFormation** service.
2. On the **CloudFormation** service page, click **Create Stack**.

   The **Select Template** page appears.



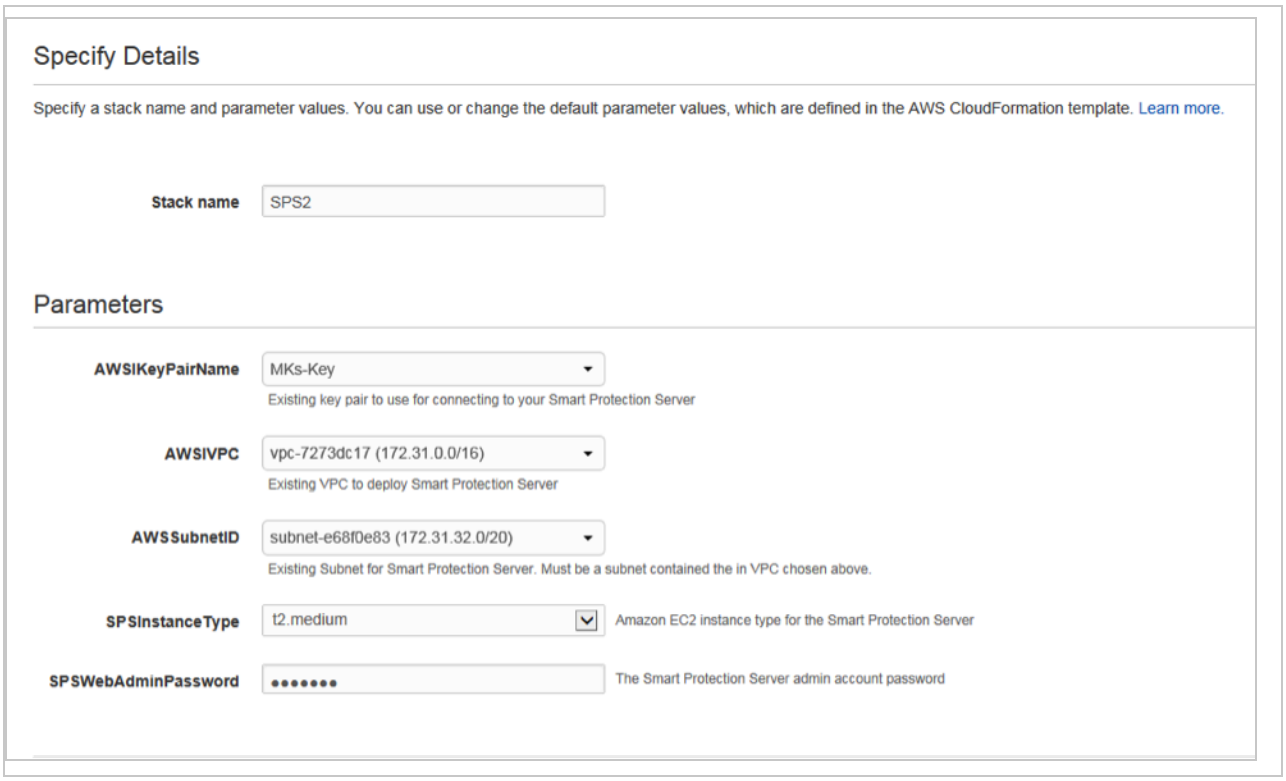
3. Select **Specify an Amazon S3 template URL** and enter this URL into the underlying field:

   ```
   https://s3.amazonaws.com/trend-micro-quick-start/latest/templates/common/sps.template
   ```

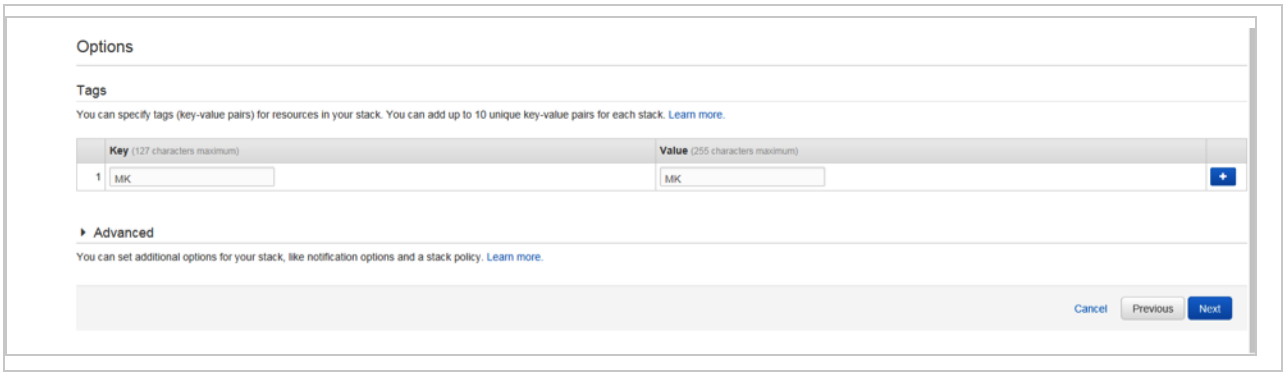
4. Click **Next**.

   Finish entering settings in the template. Choose the AWS key pairs you would like to use to authenticate to the server, the VPC and subnet where the Smart Protection Server will reside, and an administrator password. The password cannot contain special characters such as: !@#$%^&*()

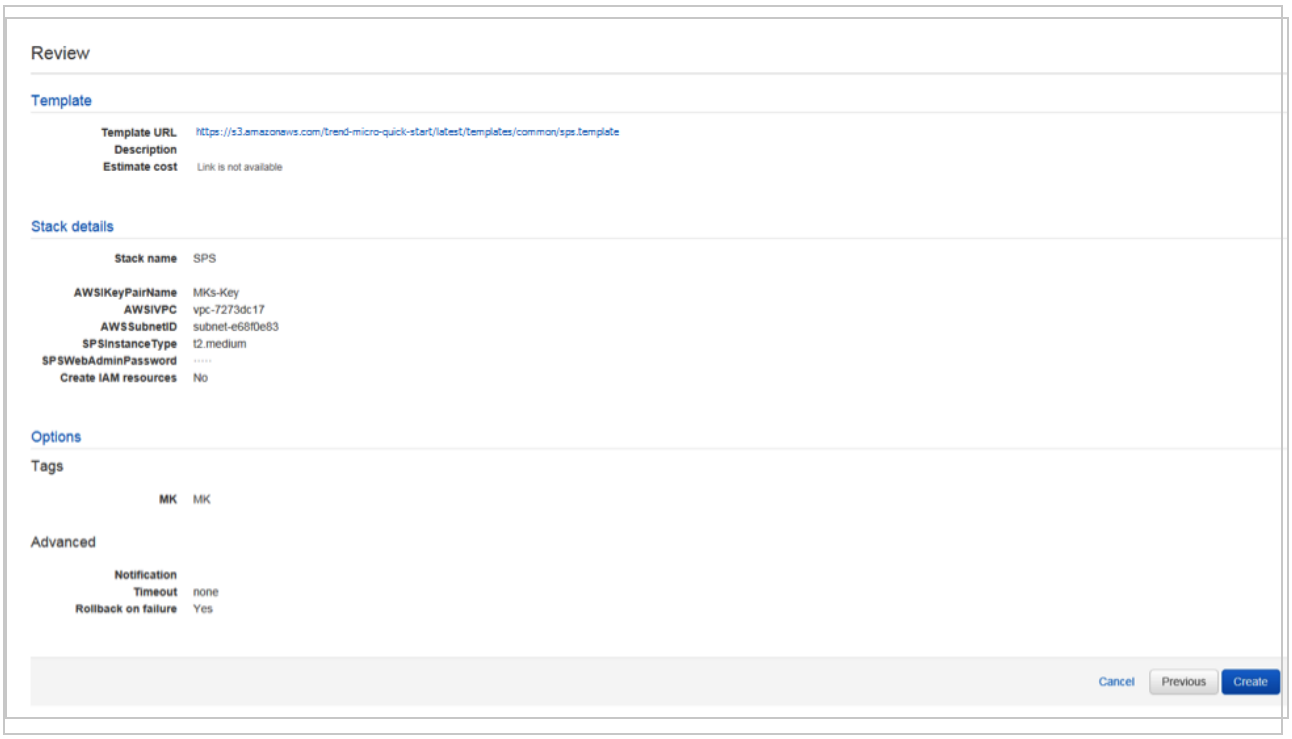
   Warning: Do not enter a password that contains dictionary words. It should be at least 8 characters in length. Failure to do this will result in a weak password that is vulnerable to guessing and brute force attacks, and could compromise the security of your network.



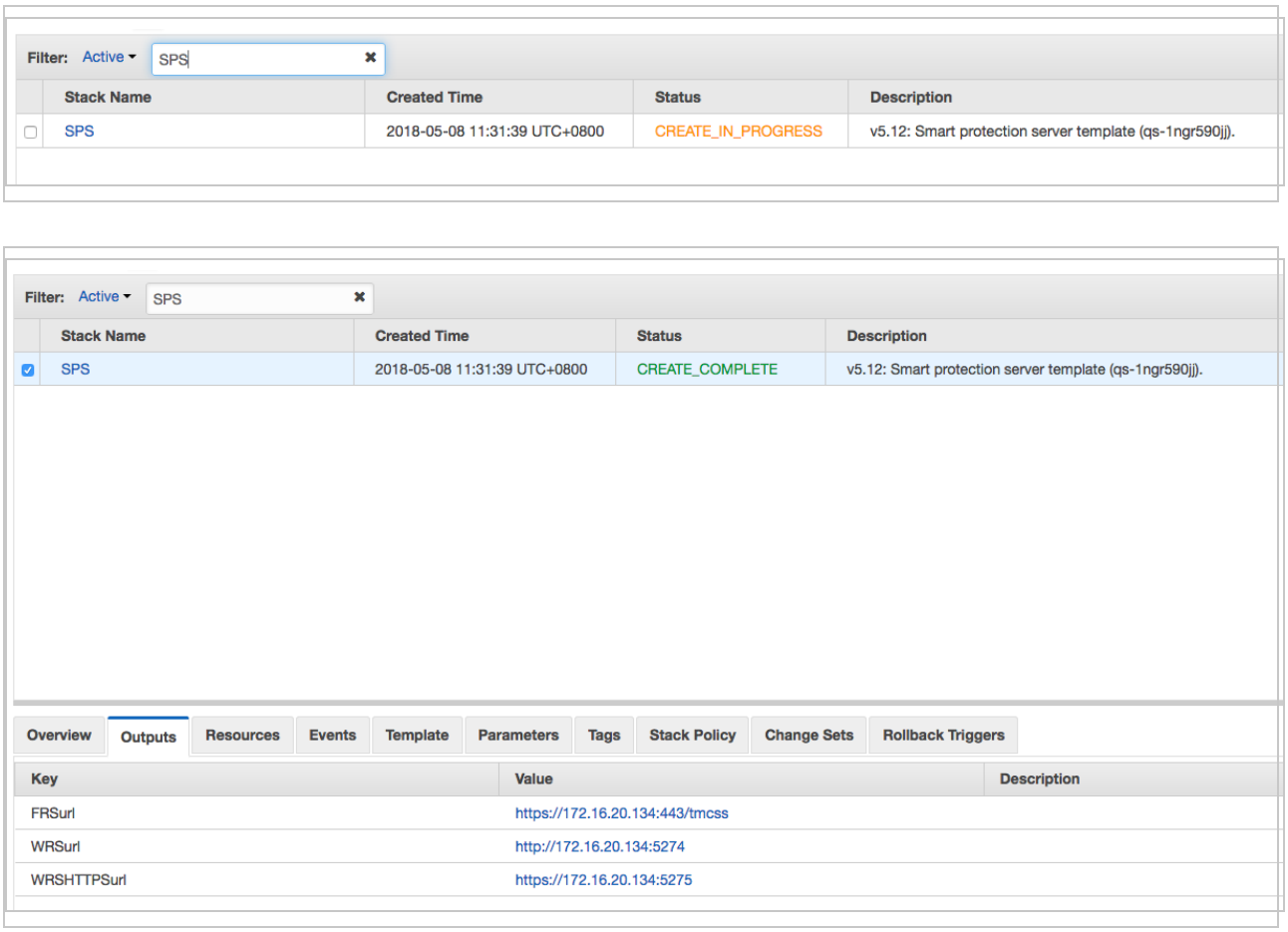
5. Click **Next**.
6. Optionally, create any tags that you would like to associate with this server, then click **Next**.



7. Review your settings, and then click **Create**.



While your server is being installed, the screen will indicate progress. To verify that the process has completed, you may need to click **Refresh** at the top of the screen.



8. After it is done creating, click the **Outputs** tab at the bottom of the screen. You see three URLS. In the Deep Security Manager's GUI, you must configure your computers to use the Smart Protection Server.
9. Log in to Deep Security Manager.
10. At either the policy level (recommended method) or at the computer level, go to the anti-malware section.
11. Click the Smart Protection tab at the top. Toward the bottom of the screen, deselect **Inherited** under **Smart Protection Server for File Reputation Service**.
12. Select **Use locally installed Smart Protection Server**.
13. Enter in the URL from the **Outputs** screen in your AWS console labeled "FRSurl" and click **Add**.
14. Click **Save**.
15. Open the web reputation section of the policy or computer and click the **Smart Protection** tab at the top.
16. Deselect **Inherited** under **Smart Protection Server for Web Reputation Service**.
17. Select **Use locally installed Smart Protection Server**.

18. Add the URL from the **Outputs** screen in your AWS console labeled "WRSurl" or "WRSHTTPSurl" and click **Add**. You can use the HTTP or HTTPS URL, but HTTPS is only supported with 11.0 Deep Security Agents and up.
19. Click **Save**.
20. If you don't have your system set up to automatically send policies, you will need to manually send the policy from your Deep Security Manager.

FAQs

Am I protected during an outage? What is the SLA?

If you'd like to know when scheduled maintenance is planned, see "Scheduled maintenance" on page 79.

One week before scheduled Deep Security as a Service maintenance windows, we notify customers on the Deep Security as a Service login page. Then, during the maintenance window, the login page will explain that the service is temporarily unavailable while back end maintenance occurs.

While Deep Security as a Service is down, connectivity is interrupted, so Deep Security agents will not be able to auto-register. Agents will not be able to forward event logs to Deep Security as a Service during that time, and (if you had pending changes) agents won't receive any policy changes either.

Security policies on the agents, however, will still be active. Events will be queued as long as the computer has enough disk space, and the agent will transmit events to Deep Security as a Service the next time that they connect. If configured, the agents also will continue to forward logs to third-party, external syslog or SIEM devices. When Deep Security as a Service becomes available again, the agents will connect again with it during the next heartbeat.

You can view the Service Level Agreement (SLA).

How are features released in Deep Security as a Service?

Previews

Features that are in preview are sometimes enabled for selected customers to allow early engagement testing with the product team. Features that are in preview have not yet reached General Availability (GA).

When a feature is in preview, there may be changes to the user experience, performance, and functionality as customer feedback influences and evolves the feature prior to General Availability. Features and capabilities that are in preview are not committed for delivery.

Support for features in preview is provided through direct engagement with the product team. Support for all other aspects of Deep Security as a Service is provided using the standard support process.

The Help Center documentation for preview features is visible to all customers and is identified by this banner at the top of each page:

This feature is part of a controlled release and is in preview. Content on this page is subject to change.

If you have any questions or concerns about features in preview, please discuss with your point of contact in the product team.

General Availability

Deep Security as a Service is updated multiple times per week without a service impact to customers. Check the "Deep Security as a Service release notes" on page 79 for information on new content and changes.

The typical process for General Availability of features is to make the feature available to all customers at the same time. However, in some cases, we may perform a staggered rollout of features to customers. This is typically done to minimize the overall risk associated with the introduction of a larger feature and sometimes involves direct interaction with specific customers.

Features that are Generally Available but in the process of being released using a staggered rollout process are identified by this banner at the top of their corresponding Help Center page:

This feature is now GA and being rolled out to Deep Security as a Service customers. If it's not available in your account yet, it will be soon.

When the rollout is complete and the feature is enabled for all customers, the banner is removed.

Features that are part of a staggered rollout process are Generally Available and are supported using the normal support process.

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 news feed has been discontinued. Instead, you can find the latest news on product changes in the What's new in Workload Security 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 on either a Solaris global zone or kernel 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 147 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

Traffic Flow	Protected by agent
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 and to any kernel zones that have an agent installed. 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 AWS GovCloud (US) instances?

There are two ways that Deep Security provides AWS GovCloud (US) support:

- You can use the Trend Micro Deep Security AMI (Per Protected Instance Hour or BYOL license type) that is available from the AWS Marketplace for AWS GovCloud (US). The deployment instructions for the AWS GovCloud (US) region are the same as any other region. See Getting started with Deep Security AMI from AWS Marketplace.
- You can install the enterprise version of the Deep Security software on an AWS instance running in the AWS GovCloud (US) region.

Note: Deep Security as a Service does not support AWS GovCloud. Computers on the AWS GovCloud must comply with user and data transmission restrictions as specified by United States of America International Traffic in Arms Regulations (ITAR). Because the Deep Security as a Service operating model requires the transmission of data outside of the AWS GovCloud, using it to manage computers in the AWS GovCloud would break this compliance.

Protecting AWS GovCloud (US) instances using a manager in a commercial AWS instance

Warning: Be aware that if your Deep Security Manager is outside of the AWS GovCloud, using it to manage computers in the AWS GovCloud would break ITAR compliance.

If your Deep Security Manager is in a commercial AWS instance and you want to use it to protect AWS GovCloud instances, you cannot use the cloud connector provided in the Deep Security Manager console to add the instances. If Deep Security Manager is running in a special region (like AWS GovCloud), it can connect to that region and also connect to instances in commercial AWS regions. But if Deep Security Manager is in a commercial region, it can connect to all commercial AWS regions but not special regions like AWS GovCloud.

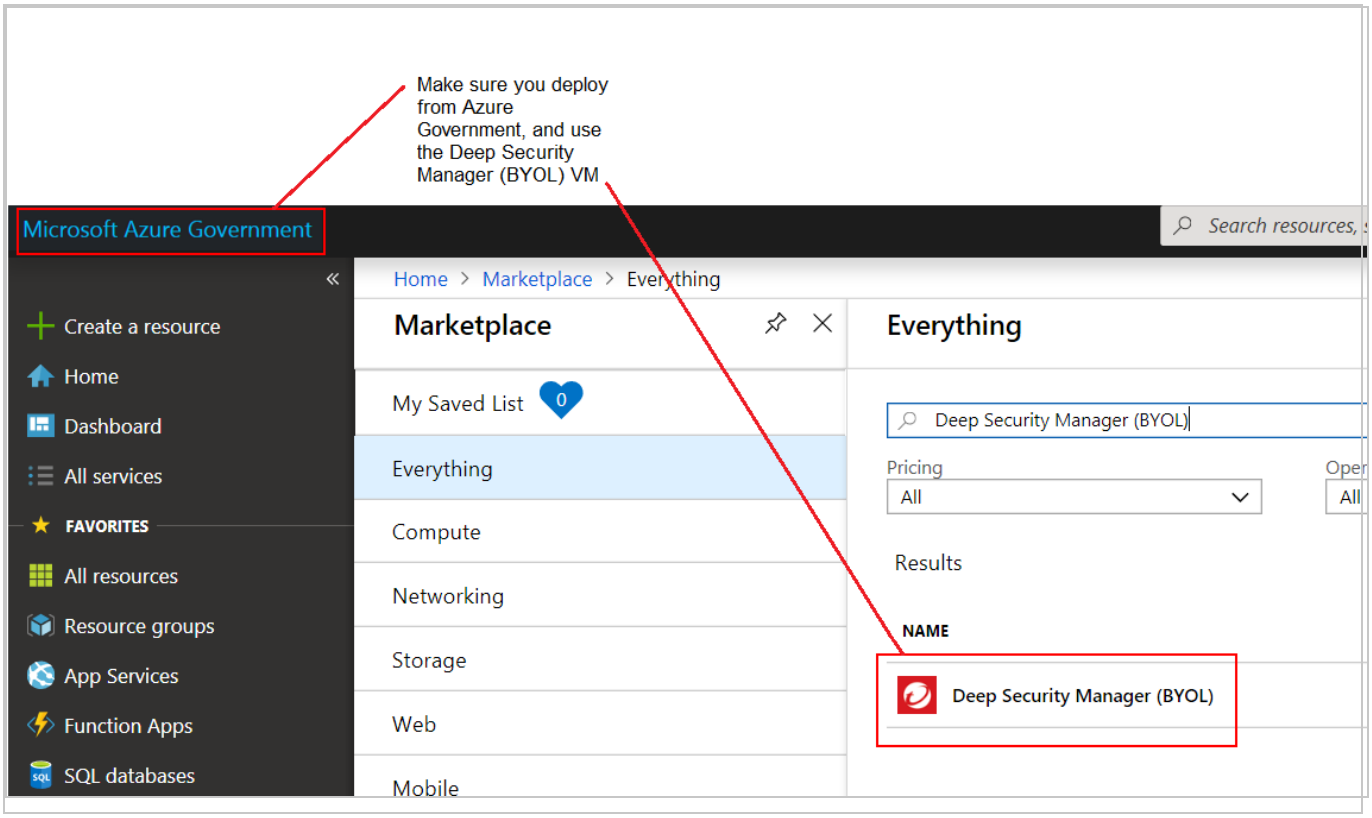
If you want to add a special region connector (like AWS GovCloud) into a Deep Security Manager running in commercial AWS, you will need to use the Deep Security legacy REST API to do so and supply the `seedRegion` argument to tell the Deep Security Manager that it's connecting outside of commercial AWS. For information about the API, see "Use the Deep Security API to automate tasks" on page 990.

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.
- You can install the Deep Security Manager on-premises software onto an Azure VM running inside Azure Government.

Note: Deep Security as a Service does not support Azure Government. Computers in Azure Government must comply with user and data transmission restrictions as specified by United States of America International Traffic in Arms Regulations (ITAR). Because the Deep Security as a Service operating model requires the transmission of data outside of Azure Government, using it to manage computers in the Azure Government would break this compliance.



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.

If your Deep Security Manager is located outside the Azure Government cloud, and you want to use it to protect instances in the Azure Government cloud, you will need to use the Deep Security legacy REST API, and supply the `azureADLoginEndPoint` and `azureEntryPoint` arguments. For details on using the API, see .

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 and the right instance size is used for metered billing.

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.	If you determine that the creation of duplicate computers has occurred, you can use inactive agent cleanup to automatically remove these computers.
Incorrect billing of instance hours at the default rate of $0.06 per hour rather than the rate associated with the workload size.	If the Deep Security Agent does not have access to Instance Metadata Service Version 1 (IMDSv1) or 2 (IMDSv2), Deep Security cannot properly determine the instance size for metered billing. As a result, the computer does not appear under a cloud account and is charged at the data center rate.	For more details, see Configuring the Instance Metadata Service.	If you believe overbilling has occurred please ensure that: 1. The Deep Security Agent

Issue	Root cause	Resolution	Additional notes
			has access to IMDS v1 or IMDS v2. 2. You have added the AWS cloud account to Deep Security. Please contact technical support for additional assistance.
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.		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 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.

[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).

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 190.

> **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.

Troubleshooting

"Offline" agent

A computer status of "Offline" or "Managed (Offline)" means that the Deep Security Manager hasn't communicated with the Deep Security Agent's instance for some time and has exceeded the missed heartbeat threshold. The status change can also appear in alerts and events.

Causes

Heartbeat connections can fail because:

- 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 "Activation Failed - Blocked port" on page 789 for troubleshooting tips.
- Bi-directional communication is enabled, but only one direction is allowed or reliable
- 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
- The agent'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

Tip: If you are using manager-initiated or bi-directional communication, and are having communication issues, we strongly recommend that you change to agent-initiated activation (see "Activate and protect agents using agent-initiated activation and communication" on page 852).

To troubleshoot the error, verify that the agent is running, and then that it 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. Method varies by 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 can't 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 will fail, 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 239).

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 agents.deepsecurity.trendmicro.com:443
```

If telnet fails, trace the route to discover which point on the network is interrupting connectivity.

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 Amazon's documentation on Amazon EC2 Security Groups for Linux Instances or Amazon EC2 Security Groups for Windows Instances. For an Azure VM instance, see Microsoft's Azure documentation on modifying a Network Security Group.

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 239).

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 up 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 970.
2. Install the Deep Security Agent 11.0. See "Install the agent manually" on page 147.
3. Re-activate the agent on the manager. See "Activate the agent" on page 164.

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 "Performance tips for anti-malware" on page 336 and "Performance tips for intrusion prevention" on page 406.
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

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" on the next page
- "An incompatible Anti-Malware component from a third-party product" on the next page
- "Other/unknown Error" on the next page

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 the Deep Security Agent.
3. Add Deep Security to the third-party software's exception list. Contact Trend Micro support if you need assistance.

Other/unknown Error

To solve this error:

1. Uninstall and reinstall the Deep Security Agent.
2. If the error is not resolved, call Trend Micro support for assistance.

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).

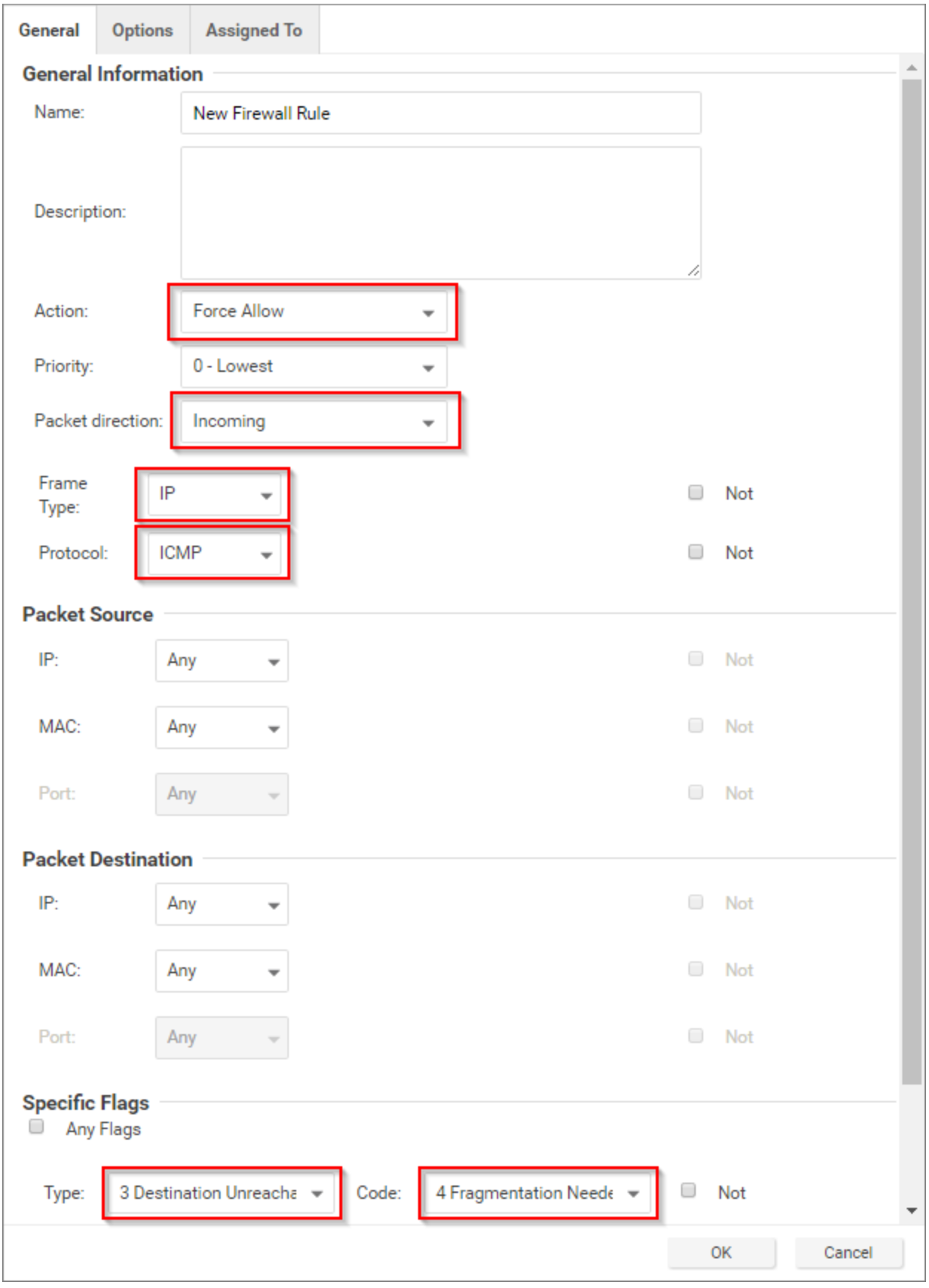
   If you are using Deep Security as a Service, you might not be using your own relays; instead, you will be using the relays that are built into the service: relay.deepsecurity.trendmicro.com.

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.

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
Options
Assigned To
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
OK
Cancel

Issues adding your AWS account to Deep Security

When adding your AWS account to Deep Security, you may encounter the following issues.

In this topic:

AWS is taking longer than expected

If AWS is taking longer than expected, it might be because:

1. The template is still running

While the Cloud Formation Template is running, Deep Security has no information on how far it has progressed or when it will finish. Deep Security is notified when the template has completed successfully. Because of this, Deep Security has a timeout that is triggered if the template has not completed within the expected time. If the timeout was triggered it doesn't mean the template has failed, AWS could just be taking longer than usual.

To check the status of the template, go to the Cloud Formation section of the AWS console. From there, look for the Status of the Stack Named **DeepSecuritySetup**. If the status field shows CREATE_IN_PROGRESS then the template is still running and more time is required.

2. The template has failed to complete

If the status field in the Cloud Formation section of the AWS console shows ROLLBACK_IN_PROGRESS, ROLLBACK_COMPLETE, or CREATE_FAILED then the template creation has failed within AWS. If this happens, go to the **Events** tab in the Cloud Formation interface to find more information about why the template failed.

Contact Deep Security technical support for help. Sign in to Deep Security as a Service, and click **Support** in the upper-right corner.

Resource is not supported in this region

The Cloud Formation Template creates a Lambda function to create the cross-account role. AWS Lambda is not currently supported in all regions, so if the Cloud Formation Template is run in a region that does not support Lambda then it will fail to create the cross-account role. By default, the link provided by the wizard will run the Cloud Formation Template in the US East (N. Virginia) region. The other regions that currently support Lambda are:

- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- EU (Frankfurt)
- EU (Ireland)
- US East (N. Virginia)
- US West (Oregon)

Template validation issue

The user running the Cloud Formation Template doesn't have the required permissions to run the template.

In the IAM console, scroll down and find the user that is currently logged in and running the template. Open the user properties by double-clicking on the user. Scroll down to the **Managed Policies** and **Inline Policies** section and click the **Show Policy** link on any policies visible. All of the permissions listed below must be contained in at least one of the polices attached to the user.

- cloudformation:CreateStack
- cloudformation:DescribeStackEvents
- cloudformation:DescribeStacks
- cloudformation:EstimateTemplateCost
- cloudformation:GetTemplate
- cloudformation:GetTemplateSummary
- cloudformation:ListStackResources
- cloudformation:ListStacks

- ec2:CreateTags
- ec2:DescribeAvailabilityZones
- ec2:DescribeImages
- ec2:DescribeInstances
- ec2:DescribeRegions
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeTags
- ec2:DescribeVpcs
- iam:AddRoleToInstanceProfile
- iam:AttachRolePolicy
- iam:CreateInstanceProfile
- iam:CreatePolicy
- iam:CreateRole
- iam:DeleteInstanceProfile
- iam:DeleteRole
- iam:DeleteRolePolicy
- iam:GetRole
- iam:GetRolePolicy
- iam:PassRole
- iam:PutRolePolicy
- iam:RemoveRoleFromInstanceProfile
- lambda:InvokeFunction
- lambda:CreateFunction
- lambda:GetFunctionConfiguration
- sts:AssumeRole
- sts:DecodeAuthorizationMessage
- workspaces:DescribeWorkspaces
- workspaces:DescribeWorkspaceDirectories
- workspaces:DescribeWorkspaceBundles
- workspaces:DescribeTags

Deep Security was unable to add your AWS account

The information that Deep Security received from AWS was incomplete.

If this happens, close the wizard and try running it again from the beginning as there might be a temporary system problem.

If the error happens a second time, contact technical support (sign in Deep Security as a Service, and click **Support** in the upper-right corner).

Create a diagnostic package and logs

To diagnose an issue, your support provider may ask you to send a diagnostic package containing debug information for Deep Security Agent.

Deep Security Agent diagnostics

For an agent, you can create a diagnostic package either:

- 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 360.

Your support provider may also ask you collect:

- 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

Note: Deep Security Manager must be able to connect to an agent remotely to create a diagnostic package for it. If the 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.

1. Go to **Computers**.
2. Double-click the name of the computer you want to generate the diagnostic package for.
3. Select the **Actions** tab.
4. Under **Support**, click **Create Diagnostics Package**.
5. Click **Next**.

   The package will take several minutes to create. After the package has been generated, a summary will be displayed and your browser will download a ZIP file containing the diagnostic package.

Note: When the **System Information** check box is selected, it might create a huge diagnostic package that could have a negative impact on performance. The check box is greyed out if you are not a primary tenant or do not have the proper viewing rights.

Create an agent diagnostic package via CLI on a protected computer

Linux, AIX, and Solaris

1. Connect to the server that you want to generate the diagnostic package for.
2. Enter the command:

   ```
   sudo /opt/ds_agent/dsa_control -d
   ```

   The output shows the name and location of the diagnostic package: `/var/opt/ds_agent/diag`

Windows

1. Connect to the computer that you want to generate the diagnostic package for.
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 will increase, which will make 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 this 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.

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 SELinux alerts

To check if SELinux is enabled, enter the following command: `sestatus`.

When the SELinux policy is set to enable and block ds_agent, the following alert sample might appear in the system log or SELinux log (/var/log/audit/audit.log or /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:

1. Connect to the Deep Security Agent 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.
4. 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 are still occurring, run the commands from step 2 again. This will update the existing policy and re-apply it.

To remove the SELinux policy, use the following command: `semodule -r ds_agent`.

PDFs

Deep Security Administration Guide

The Deep Security Administration Guide is a PDF version of the Deep Security Help Center:

Open the Deep Security as a Service Administration Guide

Deep Security Best Practice Guide

The Deep Security as a Service 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 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 as a Service for optimum performance.

The Deep Security as a Service Best Practice Guide is currently available in PDF format and includes the following:

- Deployment considerations and recommendations
- Upgrade guidelines and scenarios
- Best practice tips for VDI, private, and public cloud environments