



# 9.6 Deep Security

## Service Pack 1

### Installation Guide (VMware NSX)

Advanced Protection for Physical, Virtual, and Cloud Servers



Cloud & Data Center



Complete End User



Cyber Threats

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 readme files, release notes, and the latest version of the applicable user documentation, which are available from the Trend Micro Web site at:

<http://www.trendmicro.com/download>

Trend Micro, the Trend Micro t-ball logo, Deep Security, Control Server Plug-in, Damage Cleanup Services, eServer Plug-in, InterScan, Network VirusWall, ScanMail, ServerProtect, and TrendLabs are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Document version: 1.3

Document number: APEM97211\_150921

Release date: November 2015

Document last updated: January 19, 2017

# Table of Contents

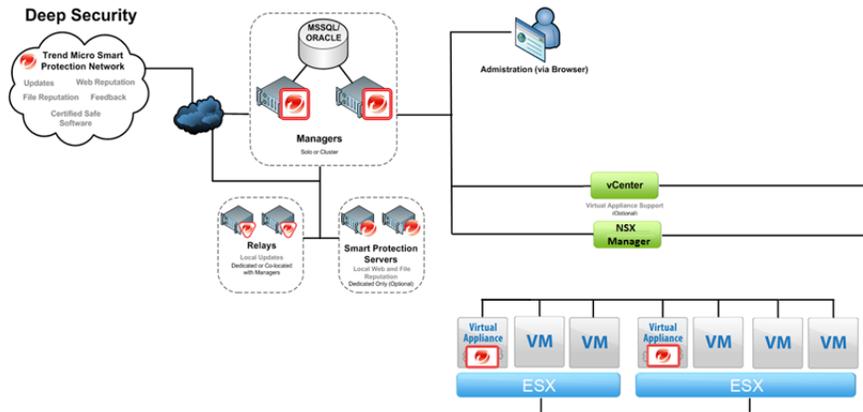
Introduction .....	5
About This Document.....	6
About Deep Security .....	8
What's New .....	11
System Requirements .....	14
Preparation .....	19
What You Will Need (VMware NSX) .....	20
Database Considerations .....	23
Installation .....	25
Installing the Deep Security Manager .....	26
Manually Installing the Deep Security Agent.....	33
Installing and Configuring a Relay-enabled Agent.....	44
Deploying Agentless Protection in an NSX Environment.....	45
Installing the Deep Security Notifier .....	58
Automated Policy Management in NSX Environments .....	60
Upgrading .....	64
Upgrading to Deep Security 9.6 SP1 in an NSX Environment .....	65
Upgrading from a pre-9.6 vShield to a 9.6 SP1 NSX Environment.....	68
Appendices .....	72
Silent Install of Deep Security Manager .....	73
Deep Security Manager Settings Properties File .....	75
Deep Security Manager Memory Usage.....	81
Deep Security Virtual Appliance Memory Usage .....	82
Deep Security Manager Performance Features .....	84
Creating an SSL Authentication Certificate .....	85
Minimum VMware Privileges for DSVa Deployment (NSX) .....	88
Installing a vSphere Distributed Switch .....	89
Preparing ESXi servers .....	90
Installing the Guest Introspection Service .....	91

Creating NSX Security Groups .....	93
Enable Multi-Tenancy .....	95
Multi-Tenancy (Advanced) .....	103
Installing a Database for Deep Security (Multi-Tenancy Requirements) .....	105
Uninstalling Deep Security from your NSX Environment .....	109

# Introduction

# About This Document

## Deep Security Installation Guide (VMware NSX)



This document describes the installation and configuration of the basic Deep Security software components.

1. The Deep Security Manager
2. The Deep Security Virtual Appliance
3. The Deep Security Agent (with Relay functionality)
4. The Deep Security Notifier

This document covers:

1. System Requirements
2. Preparation
3. Database configuration guidelines
4. Installing the Deep Security Manager management console
5. Installing a Relay-enabled Deep Security Agent
6. Integrating Deep Security with a VMware NSX environment
7. Implementing Deep Security protection using Deep Security Protection Policies and Recommendation Scans
8. Guidelines for monitoring and maintaining your Deep Security installation

## Intended Audience

This document is intended for anyone who wants to implement Agentless Deep Security protection in a VMware NSX environment. The information is intended for experienced system administrators who are familiar with virtual machine technology and virtual datacenter operations. This document assumes familiarity with VMware Infrastructure 5.x, including VMware NSX, VMware ESXi, vCenter Server, and the vSphere Web Client.

## Other Deep Security Documentation

You can find other Deep Security documentation, including Installation Guides for other platforms and administrator documentation at <http://docs.trendmicro.com/en-us/enterprise/deep-security.aspx>. In addition, Deep Security Manager includes a help system that is available from within the Deep Security Manager console.

# About Deep Security

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. The following tightly integrated modules easily expand the platform to ensure server, application, and data security across physical, virtual, and cloud servers, as well as virtual desktops.

## Protection Modules

### Anti-Malware

**Integrates with VMware environments for agentless protection, or provides an agent to defend physical servers and virtual desktops.**

Integrates new VMware vShield Endpoint APIs to provide agentless anti-malware protection for VMware virtual machines with zero in-guest footprint. Helps avoid security brown-outs commonly seen in full system scans and pattern updates. Also provides agent-based anti-malware to protect physical servers, Hyper-V and Xen-based virtual servers, public cloud servers as well as virtual desktops. Coordinates protection with both agentless and agent-based form factors to provide adaptive security to defend virtual servers as they move between the data center and public cloud.

### Web Reputation

**Trend Micro Web Reputation Service blocks access to malicious web sites.**

Trend Micro assigns a reputation score based on factors such as a website's age, historical location changes and indications of suspicious activities discovered through malware behavior analysis.

The Web Reputation Service:

- Blocks users from accessing compromised or infected sites
- Blocks users from communicating with Communication & Control servers (C&C) used by criminals
- Blocks access to malicious domains registered by criminals for perpetrating cybercrime

### Firewall

**Decreases the attack surface of your physical and virtual servers.**

Centralizes management of server firewall policy using a bi-directional stateful firewall. Supports virtual machine zoning and prevents Denial of Service attacks. Provides broad coverage for all IP-based protocols and frame types as well as fine-grained filtering for ports and IP and MAC addresses.

### Intrusion Prevention

**Shields known vulnerabilities from unlimited exploits until they can be patched.**

Helps achieve timely protection against known and zero-day attacks. Uses vulnerability rules to shield a known vulnerability -- for example those disclosed monthly by Microsoft -- from an unlimited number of exploits. Offers out-of-the-box vulnerability protection for over 100 applications, including database, web, email and FTP servers. Automatically delivers rules that shield newly discovered vulnerabilities within hours, and can be pushed out to thousands of servers in minutes, without a system reboot.

**Defends against web application vulnerabilities**

Enables compliance with PCI Requirement 6.6 for the protection of web applications and the data that they process. Defends against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities. Shields vulnerabilities until code fixes can be completed.

**Identifies malicious software accessing the network**

Increases visibility into, or control over, applications accessing the network. Identifies malicious software accessing the network and reduces the vulnerability exposure of your servers.

## Integrity Monitoring

**Detects and reports malicious and unexpected changes to files and systems registry in real time.**

Provides administrators with the ability to track both authorized and unauthorized changes made to the instance. The ability to detect unauthorized changes is a critical component in your cloud security strategy as it provides the visibility into changes that could indicate the compromise of an instance.

## Log Inspection

**Provides visibility into important security events buried in log files.**

Optimizes the identification of important security events buried in multiple log entries across the data center. Forwards suspicious events to a SIEM system or centralized logging server for correlation, reporting and archiving. Leverages and enhances open-source software available at [OSSEC](#).

## Deep Security Components

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

- **Deep Security Manager**, the centralized Web-based management console which 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 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.

## Deep Security Manager

Deep Security Manager ("the Manager") is a powerful, centralized web-based management system that allows security administrators to create and manage comprehensive security policies and track threats and preventive actions taken in response to them. Deep Security Manager integrates with different aspects of the datacenter including VMware vCenter and Microsoft Active Directory. To assist in deployment and integration into customer and partner environments, Deep Security has a Web Service API that is exposed to allow for an easy, language-neutral method to externally access data and programming configurations.

## Policies

Policies are templates that specify the settings and security rules to be configured and enforced automatically for one or more computers. These compact, manageable rule sets make it simple to provide comprehensive security without the need to manage thousands of rules. Default Policies provide the necessary rules for a wide range of common computer configurations.

## Dashboard

The customizable, web-based UI makes it easy to quickly navigate and drill down to specific information. It provides:

- Extensive system, event and computer reporting
- Graphs of key metrics with trends
- Detailed event logs
- Ability to save multiple personalized dashboard layouts

## Built-in Security

Role-based access allows multiple administrators (Users), each with different sets of access and editing rights, to edit and monitor different aspects of the system and receive information appropriate to them. Digital signatures are used to authenticate system components and verify the integrity of rules. Session encryption protects the confidentiality of information exchanged between components.

## Deep Security Virtual Appliance

The Deep Security Virtual Appliance runs as a VMware virtual machine and protects the other virtual machines on the same ESXi Server, each with its own individual security policy.

## Deep Security Agent

The Deep Security Agent ("the Agent") is a high performance, small footprint, software component installed on a computer to provide protection.

The Deep Security Agent contains a **Relay module** (off by default). At least one Relay-enabled Agent is required in any Deep Security installation to distribute Security and Software Updates throughout your Deep Security network. You can enable multiple Relay-enabled Agents and organize them into hierarchical groups to more efficiently distribute Updates throughout your network.

## Deep Security Notifier

The Deep Security Notifier is a Windows System Tray application that communicates the state of the Deep Security Agent and Relay-enabled Agent to client machines. The Notifier displays pop-up user notifications when the Deep Security Agent begins a scan, or blocks malware or access to malicious web pages. The Notifier also provides a console utility that allows the user to view events and configure whether pop-ups are displayed.

# What's New

## Deep Security 9.6 SP1

### Increased NSX Policy Integration

- To allow for NSX certification, Deep Security Manager can now be configured to synchronize its policies with NSX. This creates a matching NSX Service Profile (which we call a "Mapped Service Profile" in Deep Security) for each of the Deep Security policies. The Mapped Service Profiles are available as a choice when creating NSX Security Policies.
- vRealize Blueprints can be configured with either an NSX Security Group or an NSX Security Policy that uses a Mapped Service Profile. This will result in VMs being activated and assigned particular Deep Security policies.

### Multi-factor Authentication with Google Authenticator

You can now enable multi-factor authentication when logging in to Deep Security Manager.

### Windows 10 Support

The Deep Security Agent can protect computers that are running Microsoft Windows 10.

---

*Note:* Agentless support requires an update from VMware and is currently unavailable.

---

### Real-Time Anti-Malware Support for Amazon Linux

Real-time Anti-Malware support is now available on Amazon Linux.

### Terms and Conditions

Deep Security Manager can be configured to require users to accept Terms and Conditions before logging in to the Deep Security Manager.

### Report Classifications

The Reports feature has a new option that allows you to classify and mark reports using:

- Top Secret
- Secret
- Confidential
- For Official Use Only
- Law Enforcement Sensitive (LES)
- Limited Distribution
- Unclassified
- Internal Use Only

## Security Module Usage Cumulative Report

A new "Security Module Usage Cumulative" report extends the current Security Module Usage report. The new report provides a cumulative total and the total in blocks of 100, of the protection modules that were active over the course of a specified timeframe.

## Deep Security 9.6

### VMware vSphere 6 Support

- Deep Security 9.6 now supports vSphere 6.
- NSX 6.1.4 Support and Integration:
  - Agentless Anti-Malware, Integrity Monitoring, Firewall, Intrusion Prevention, and Web Reputation are available with NSX.
- vCNS 5.5.4 Support:
  - Agentless Anti-Malware and Integrity Monitoring are available for vCNS.
  - Combined Mode with Agentless Anti-Malware and Integrity Monitoring and Agent-based support for Firewall, Intrusion Prevention, Web Reputation, and Log Inspection.

### SAP Protection For Linux

Deep Security has integrated the SAP adapter into the Deep Security Agent. The SAP adapter works seamlessly with the SAP VSI interface (also referred to as NW-VSI-2.0). The VSI interface is available in applications and platforms such as NetWeaver, HANA and Fiori.

The SAP adapter has been fully incorporated in to Deep Security 9.6 as part of the Red Hat Enterprise Linux and SUSE Enterprise Linux builds and can now be licensed directly through Deep Security Manager.

### IBM QRadar Support

Deep Security can now output syslog messages in Log Event Extended Format (LEEF 2.0) for integration with IBM QRadar.

### Real-Time Anti-Malware for CloudLinux

Real-time Anti-Malware is available on CloudLinux 7.

### Additional Platform Support

Deep Security 9.6 adds support for the following platforms:

- Debian 6 and 7
- Windows 2012 Server Core
- CloudLinux 7
- Oracle Linux 7
- SUSE Enterprise Linux 12

## Deep Security Database Support for Oracle 12c

Deep Security Manager now supports Oracle 12c for its back-end database.

## Active Directory Synchronization on Login

New users created in Active Directory can now log in to Deep Security Manager before the Active Directory Sync task has been run.

## Deep Security Relay Downloads from Trend Micro Download Center

In situations where the Deep Security Relay cannot directly access the Deep Security Manager, the Relay can now download updates from Trend Micro Download Center.

## Minor Report Enhancements

The Security Module usage report now has columns for the Computer Group and the Instance Type (for AWS workloads).

## Automatic Updates of Online Help

The Deep Security online help can now be updated seamlessly in Deep Security Manager through a new Online Help package.

# System Requirements

## Deep Security Manager

- **Minimum Memory:** 8GB, which includes:
  - 4GB heap memory
  - 1.5GB JVM overhead
  - 2GB operating system overhead
- **Minimum Disk Space:** 1.5GB (5GB recommended)
- **Operating System:**
  - Windows Server 2012 (64-bit), Windows Server 2012 R2 (64-bit) with latest service pack or patch
  - Windows Server 2008 (64-bit), Windows Server 2008 R2 (64-bit) with latest service pack or patch
  - Windows 2003 Server R2 SP2 (64-bit) with latest service pack or patch
  - Red Hat Linux 5/6/7 (64-bit)

---

***Note:** If you are installing the AWS Marketplace version of Deep Security Manager, it must be installed on an AWS Linux instance.*

---

- **Database:**
  - Oracle Database 12c
  - Oracle Database 11g, Oracle Database 11g Express
  - Microsoft SQL Server 2014, Microsoft SQL Server 2014 Express
  - Microsoft SQL Server 2012, Microsoft SQL Server 2012 Express
  - Microsoft SQL Server 2008, Microsoft SQL Server 2008 Express
  - Microsoft SQL Server 2008 R2, Microsoft SQL Server 2008 R2 Express
- **Notes:**
  - SQL Server Express is not recommended for production systems, especially in multi-tenant environments.
  - Azure SQL Database is not supported for use with a Deep Security Manager software installation. It is only supported with the Deep Security Manager VM for Azure Marketplace.
- **Web Browser:** Firefox 38+, Internet Explorer 9.x, Internet Explorer 10.x, Internet Explorer 11.x, Chrome 43+, Safari 6+. (Cookies enabled.)
  - **Monitor:** 1024 x 768 resolution at 256 colors or higher

## Deep Security Agent

- **Minimum Memory:**
  - **with Anti-Malware protection:** 512MB
  - **without Anti-Malware protection:** 128MB
- **Minimum Disk Space:**
  - **with Anti-Malware protection:** 1GB
  - **without Anti-Malware protection:** 500MB
  - **with Relay functionality enabled:** 8GB
- **Windows:**
  - Windows Server 2012 (64-bit), Windows Server 2012 R2 (64-bit) - Full Server or Server Core with latest service pack or patch
  - Windows 10 (32-bit and 64-bit)

- Windows 8.1 (32-bit and 64-bit) with latest service pack or patch
  - Windows 8 (32-bit and 64-bit) with latest service pack or patch
  - Windows 7 (32-bit and 64-bit) with latest service pack or patch
  - Windows Server 2008 (32-bit and 64-bit) with latest service pack or patch
  - Windows Server 2008 R2 (64-bit) with latest service pack or patch
  - Windows Vista (32-bit and 64-bit) with latest service pack or patch
  - Windows Server 2003 R2 SP2 (32-bit and 64-bit) with latest service pack or patch
  - Windows XP (32-bit and 64-bit) with latest service pack or patch
  - **With Relay functionality enabled:** All 64-bit Windows versions above
- **Linux:**
    - Red Hat 5 (32-bit and 64-bit)
    - Red Hat 6 (32-bit and 64-bit)
    - Red Hat 7 (64-bit)
    - Oracle Linux 5 (32-bit and 64-bit)
    - Oracle Linux 6 (32-bit and 64-bit)
    - Oracle Linux 7 (64-bit)
    - CentOS 5 (32-bit and 64-bit)
    - CentOS 6 (32-bit and 64-bit)
    - CentOS 7 (64-bit)
    - Debian 6 (64-bit)
    - Debian 7 (64-bit)
    - SUSE 10 SP3 and SP4 (32-bit and 64-bit)
    - SUSE 11 SP1, SP2, and SP3 (32-bit and 64-bit)
    - SUSE 12 (64-bit)
    - CloudLinux 5 (32-bit and 64-bit)
    - CloudLinux 6 (32-bit and 64-bit)
    - CloudLinux 7 (64-bit)
    - Amazon AMI Linux EC2 (32-bit and 64-bit)
    - Ubuntu 10.04 LTS (64-bit)
    - Ubuntu 12.04 LTS (64-bit)
    - Ubuntu 14.04 LTS (64-bit)
    - **With Relay functionality enabled:** All 64-bit Linux versions above

---

**Note:** *The CentOS Agent software is included in the Red Hat Agent software package. To install a Deep Security Agent on CentOS, use the Red Hat Agent installer.*

---

**Note:** *For a list of supported Deep Security features by software platform, see the document titled **Deep Security 9.6 SP1 Supported Features and Platforms**. For a list of specific Linux kernels supported for each platform, see the document titled **Deep Security 9.6 SP1 Supported Linux Kernels**.*

---

## Upgrading a Deep Security Agent system to Windows 10

If you currently have Deep Security Agent 9.6 installed on a Microsoft Windows 7, 8, or 8.1 system and want to upgrade that host system to Microsoft Windows 10 keep these points in mind:

- Upgrade the Deep Security Agent to version 9.6 SP1 before upgrading the operating system. Earlier versions of the Deep Security Agent are incompatible with Windows 10.
- If a Deep Security Agent system has been upgraded to Windows 10 before upgrading to Deep Security Agent 9.6 SP1, you will need to uninstall the Deep Security Agent, reboot the system, and then install Deep Security Agent 9.6 SP1 on the system.
- The upgrade to Deep Security 9.6 SP1 may require a system reboot on Windows 8 and 8.1 systems. If you are prompted to reboot the system, perform the reboot before upgrade the operating system.
- Windows 10 is not supported with Agentless systems and combined mode.
- If you decide to uninstall the Deep Security 9.6 SP1 Agent from a Windows 10 host, it will require a system reboot.

## Deep Security Virtual Appliance

- **Minimum Memory:** 4GB (Memory requirements can vary depending on the number of VMs being protected).
- **Minimum Disk Space:** 20GB
- **VMware Environment:**
  - **NSX Environment:**
    - VMware vCenter 5.5, with ESXi 5.5
    - VMware vCenter 6.0, with ESXi 5.5 or 6.0
  - **vShield Environment:** VMware vCenter 5.5 or 6.0 with ESXi 5.5 or 6.0
- **Additional VMware Utilities:**
  - NSX Environment:** VMware Tools, VMware vCenter Server Appliance 5.5, VMware NSX Manager 6.1.5 or 6.2
- **Supported guest platforms for which the Virtual Appliance can provide protection:**

---

**Note:** *Not all Deep Security features are supported on all platforms. For a list of supported Deep Security features by software platform, see the document titled **Deep Security 9.6 SP1 Supported Features and Platforms**.*

---

- **Windows:**
  - Windows Vista (32-bit) with latest service pack or patch
  - Windows 7 (32-bit and 64-bit) with latest service pack or patch
  - Windows XP SP3 or higher (32-bit) with latest service pack or patch
  - Windows 2003 SP2 or higher (32-bit and 64-bit) with latest service pack or patch
  - Windows 2008 (32-bit and 64-bit) with latest service pack or patch
  - Windows 2008 R2 (64-bit) with latest service pack or patch
  - Windows 8 (32-bit and 64-bit) (vSphere 5.5 only) with latest service pack or patch
  - Windows 8.1 (32-bit and 64-bit) (vSphere 5.5 - ESXi build 1892794 or higher) with latest service pack or patch
  - Windows 2012 (64-bit) (vSphere 5.5 only) with latest service pack or patch
  - Windows 2012 R2 (64-bit) (vSphere 5.5 - ESXi build 1892794 or higher) with latest service pack or patch
- **Linux:**
  - Red Hat Enterprise 5 (32-bit and 64-bit)
  - Red Hat Enterprise 6 (32-bit and 64-bit)
  - Red Hat Enterprise 7 (64-bit)
  - CentOS 5 (32-bit and 64-bit)
  - CentOS 6 (32-bit and 64-bit)
  - CentOS 7 (64-bit)
  - Oracle Linux 5 (32-bit and 64-bit) - RedHat kernel

- Oracle Linux 6 (32-bit and 64-bit) - RedHat kernel
- Oracle Linux 5 (64-bit) - Unbreakable Kernel
- Oracle Linux 6 (64-bit) - Unbreakable Kernel
- Oracle Linux 7 (64-bit)
- SUSE 10 SP3, SP4 (32-bit and 64-bit)
- SUSE 11 SP1, SP2, SP3 (32-bit and 64-bit)
- SUSE 12 (64-bit)
- Ubuntu 10.04 LTS (64-bit)
- Ubuntu 12.04 LTS (64-bit)
- Ubuntu 14.04 LTS (64-bit)
- CloudLinux 5 (32-bit and 64-bit)
- CloudLinux 6 (32-bit and 64-bit)

---

**Note:** Your VMware vCenter must be either an NSX Environment or a vShield Environment, not a mixture of the two. If you want to use both NSX and vShield, they must be in separate vCenters. You can add more than one vCenter to Deep Security Manager.

---

**Note:** The Deep Security Virtual Appliance uses 64-bit CentOS/Red Hat (included in the Virtual Appliance software package). Because the Deep Security Virtual Appliance uses the same Protection Module plug-ins as Deep Security Agents, importing an update to the 64-bit Red Hat Agent software can lead to a notification that new software is available for the Virtual Appliance as for Red Hat Agents.

---

**Note:** If using **MTU 9000** (jumbo frames), you must use ESXi build 5.5.0.1797756 or later.

---

## ESXi Requirements for the Deep Security Virtual Appliance

In addition to the ESXi standard system requirements, the following specifications must be met:

- **CPU:** 64-bit, Intel-VT or AMD-V present and enabled in BIOS
- **Supported vSwitches:**
  - **NSX:** vSphere Distributed Switch (vDS)
  - **vShield:** vSphere Standard Switch (vSS) or third party vSwitch (Cisco Nexus 1000v)

---

**Note:** VMware does not support running nested ESXi servers in production environments. For more information, see this [VMware Knowledge Base article](#).

---

## Deep Security Notifier System Requirements

- **Windows:**
  - Windows Server 2012 R2 (64-bit) with latest service pack or patch
  - Windows Server 2012 (64-bit) with latest service pack or patch
  - Windows 8.1 (32-bit and 64-bit) with latest service pack or patch
  - Windows 8 (32-bit and 64-bit) with latest service pack or patch
  - Windows 7 (32-bit and 64-bit) with latest service pack or patch
  - Windows Server 2008 R2 (64-bit) with latest service pack or patch
  - Windows Server 2008 (32-bit and 64-bit) with latest service pack or patch

- Windows Vista (32-bit and 64-bit) with latest service pack or patch
- Windows Server 2003 SP2 (32-bit and 64-bit) with latest service pack or patch
- Windows Server 2003 R2 (32-bit and 64-bit) with latest service pack or patch
- Windows XP (32-bit and 64-bit) with latest service pack or patch

---

**Note:** *On VMs protected by a Virtual Appliance, the Anti-Malware module must be licensed and enabled on the VM for the Deep Security Notifier to display information.*

---

# Preparation

# What You Will Need (VMware NSX)

## Deep Security Software Packages

Download the following software install packages from the Trend Micro Download Center:

- **Deep Security Manager**
- **Deep Security Virtual Appliance**
- **Deep Security Agent**

---

**Note:** Any Deep Security installation, regardless of whether it is providing Agentless or Agent-based protection, requires at least one Relay-enabled Agent to be installed to download and distribute Security and Software Updates. Any 64-bit Windows or Linux Agent can provide Relay functionality.

---

- **Deep Security Notifier**

The download center is located at:

<http://downloadcenter.trendmicro.com/>

---

**Note:** To manually confirm that you possess a legitimate version of each install package, use a hash calculator to calculate the hash value of the downloaded software and compare it to the value published on the Trend Micro Download Center Web site.

---

Once the Deep Security Manager is installed, you will need to manually import the Virtual Appliance from a local directory into the Manager. (To deploy the Deep Security service to your vCenter, the Appliance must be imported to Deep Security Manager.)

### To import the Deep Security Virtual Appliance software:

1. Download the Deep Security Virtual Appliance software package from the Trend Micro Download Center (<http://downloadcenter.trendmicro.com>) to the Deep Security Manager host machine.
2. In the Deep Security Manager, go to the **Administration > Updates > Software > Local** page and click **Import...** in the toolbar and import the software package to Deep Security. (The Deep Security manager will then automatically download the latest 64-bit Red Hat agent software package which will later be used to upgrade the Virtual Appliance's Protection Modules.)

To import the Deep Security Agent software, see [Installing the Deep Security Agent \(page 33\)](#) and [Installing and Configuring a Relay-enabled Agent \(page 44\)](#).

The Deep Security Notifier is an optional component that you can install on your protected Windows VMs. It displays local notifications of system Events in the notification area.

## License (Activation Codes)

You will require Deep Security Activation Codes for the protection modules and a separate Activation Code for Multi-Tenancy if you intend to implement it.

(VMware Licenses will also be required for VMware components.)

## Administrator/Root Privileges

You need to have Administrator/Root privileges on the computers on which you will install Deep Security software components.

## SMTP Server

You will need an SMTP server to send alert emails. The DSM uses Port 25 by default for connection to the SMTP Server.

## Available Ports

### On the Deep Security Manager

You must make sure the following ports on the machine hosting Deep Security Manager are open and not reserved for other purposes:

- **Port 4120:** The port for "heartbeat", used by Deep Security Agents and Appliances to communicate with Deep Security Manager (configurable).
- **Port 4119:** Used for the Deep Security Manager console. Also used for communication from ESXi. Ensure that port 4119 is open from the NXS Manager to the Deep Security Manager.
- **Port 1521:** Bi-directional Oracle Database server port.
- **Ports 1433 and 1434:** Bi-directional Microsoft SQL Server Database ports.
- **Ports 389, 636, and 3268:** Used for connection with an LDAP Server and Active Directory (configurable).
- **Port 25:** Communication to a SMTP Server to send email alerts (configurable).
- **Port 53:** For DNS Lookup.
- **Port 514:** Communication with a Syslog server (configurable).
- **Port 443:** Communication with VMware vCloud, vCenter, vShield/NSX Manager, Amazon AWS, Microsoft Azure, and other cloud accounts.

---

**Note:** For more details about how each of these ports are used by Deep Security, see **Ports Used by Deep Security** in the Reference section of the online help or the Administrator's Guide.

---

### On the Relay-enabled Agents, Agents, and Appliances

You must make sure the following ports on the machine hosting a Relay-enabled Agent are open and not reserved for other purposes:

- **Port 4122:** Relay to Agent/Appliance communication.
- **Port 4118:** Manager-to-Agent communication.
- **Port 4123:** Used for internal communication. Should not be open to the outside.
- **Port 80, 443:** connection to Trend Micro Update Server and Smart Protection Server.
- **Port 514:** bi-directional communication with a Syslog server (configurable).

The Deep Security Manager automatically implements specific Firewall Rules to open the required communication ports on machines hosting Relay-enabled Agents, Agents and Appliances.

## Network Communication

Communication between Deep Security Manager and Relay-enabled Agents, Agents/Appliances and hypervisors uses DNS hostnames by default. In order for Deep Security Agent/Appliance deployments to be successful, you must ensure that each computer can resolve the hostname of the Deep Security Manager and a Relay-enabled Agent. This may require that the Deep Security Manager and Relay-enabled Agent computers have a DNS entry or an entry in the Agent/Appliance computer's hosts file.

---

**Note:** You will be asked for this hostname as part of the Deep Security Manager installation procedure. If you do not have DNS, enter an IP address during the installation.

---

## Reliable Time Stamps

All computers on which Deep Security Software is running should be synchronized with a reliable time source. For example, regularly communicating with a Network Time Protocol (NTP) server.

## Performance Recommendations

See [Deep Security Manager Performance Features \(page 84\)](#).

## Deep Security Manager and Database Hardware

Many Deep Security Manager operations (such as Updates and Recommendation Scans) require high CPU and Memory resources. Trend Micro recommends that each Manager node have four cores and sufficient RAM in high scale environments.

The Database should be installed on hardware that is equal to or better than the specifications of the best Deep Security Manager node. For the best performance the database should have 8-16GB of RAM and fast access to the local or network attached storage. Whenever possible a database administrator should be consulted on the best configuration of the database server and a maintenance plan should be put in effect.

For more information, see [Database Considerations \(page 23\)](#).

## Dedicated Servers

The Deep Security Manager and the database can be installed on the same computer if your final deployment is not expected to exceed 1000 computers (real or virtual). If you think you may exceed 1000 computers, the Deep Security Manager and the database should be installed on dedicated servers. It is also important that the database and the Deep Security Manager be co-located on the same network with a 1GB LAN connection to ensure unhindered communication between the two. The same applies to additional Deep Security Manager Nodes. A two millisecond latency or better is recommended for the connection from the Manager to the Database.

## High Availability Environments

If you use VMware's High Availability (HA) features, make sure that the HA environment is established before you begin installing Deep Security. Deep Security must be deployed on all ESXi hypervisors (including the ones used for recovery operations). Deploying Deep Security on all hypervisors will ensure that protection remains in effect after a HA recovery operation.

---

**Note:** *When a Virtual Appliance is deployed in a VMware environment that makes use of the VMware Distributed Resource Scheduler (DRS), it is important that the Appliance does not get vMotioned along with the virtual machines as part of the DRS process. Virtual Appliances must be "pinned" to their particular ESXi server. You must actively change the DRS settings for all the Virtual Appliances to "Manual" or "Disabled" (recommended) so that they will not be vMotioned by the DRS. If a Virtual Appliance (or any virtual machines) is set to "Disabled", vCenter Server does not migrate that virtual machine or provide migration recommendations for it. This is known as "pinning" the virtual machine to its registered host. This is the recommended course of action for Virtual Appliances in a DRS environment. An alternative is to deploy the Virtual Appliance onto local storage as opposed to shared storage. When the Virtual Appliance is deployed onto local storage it cannot be vMotioned by DRS. For further information on DRS and pinning virtual machines to a specific ESXi server, please consult your VMware documentation.*

---

**Note:** *If a virtual machine is vMotioned by DRS from an ESXi protected by a DSVA to an ESXi that is not protected by a DSVA, the virtual machine will become unprotected. If the virtual machine is subsequently vMotioned back to the original ESXi, it will not automatically be protected again unless you have created an Event-based Task to activate and protect computers that have been vMotioned to an ESXi with an available DSVA.*

---

# Database Considerations

Refer to your database provider's documentation for instructions on database installation and deployment but keep the following considerations in mind for integration with Deep Security.

## Install before Deep Security

You must install the database software, create a database instance for Deep Security (if you are not using the default instance), and create a user account for Deep Security *before* you install Deep Security Manager.

## Location

The database must be located on the same network as the Deep Security Manager with a connection speed of 1Gb/s over LAN. (WAN connections are not recommended.)

## Dedicated Server

The database should be installed on a separate dedicated machine.

## Microsoft SQL Server

- Enable "Remote TCP Connections". (See [http://msdn.microsoft.com/en-us/library/bb909712\(v=vs.90\).aspx](http://msdn.microsoft.com/en-us/library/bb909712(v=vs.90).aspx))
- The database account used by the Deep Security Manager must have **db\_owner** rights.
- If using Multi-Tenancy, the database account used by the Deep Security Manager must have **dbcreator** rights.
- Select the "simple" recovery model property for your database. (See <http://technet.microsoft.com/en-us/library/ms189272.aspx>)

## Oracle Database

- Start the "Oracle Listener" service and make sure it accepts TCP connections.
- The database account used by the Deep Security Manager must be granted the **CONNECT** and **RESOURCE** roles and **UNLIMITED TABLESPACE, CREATE SEQUENCE, CREATE TABLE** and **CREATE TRIGGER** system privileges.
- If using Multi-Tenancy, the database account used by the Deep Security Manager must be granted the **CREATE USER, DROP USER, ALTER USER, GRANT ANY PRIVILEGE** and **GRANT ANY ROLE** system privileges.

## Transport Protocol

The recommended transport protocol is **TCP**.

If using **Named Pipes** to connect to a SQL Server, a properly authenticated Microsoft Windows communication channel must be available between Deep Security Manager host and the SQL Server host. This may already exist if:

- The SQL Server is on the same host as Deep Security Manager.
- Both hosts are members of the same domain.
- A trust relationship exists between the two hosts.

If no such communication channel is available, Deep Security Manager will not be able to communicate to the SQL Server over named pipes.

## Connection Settings Used During Deep Security Manager Installation.

During the Deep Security Manager installation, you will be asked for Database connection details. Enter the Database hostname under "Hostname" and the pre-created database for Deep Security under "Database Name".

The installation supports both SQL and Windows Authentication. When using Windows Authentication, click on the "Advanced" button to display additional options.

## Avoid special Characters for the database user name (Oracle)

---

**Note:** Although Oracle allows special characters in database object names if they are surrounded by quotes, Deep Security does not support special characters in database object names. This page on Oracle's web site describes the allowed characters in non-quoted names: [http://docs.oracle.com/cd/B28359\\_01/server.111/b28286/sql\\_elements008.htm#SQLRF00223](http://docs.oracle.com/cd/B28359_01/server.111/b28286/sql_elements008.htm#SQLRF00223)

---

## Keep the database Name Short (SQL Server)

If using Multi-Tenancy, keeping the main database name short will make it easier to read the database names of your Tenants. (ie. If the main database is "MAINDB", the first Tenant's database name will be "MAINDB\_1", the second Tenant's database name will be "MAINDB\_2", and so on.)

---

**Note:** If you are using a Pay-Per-Use license with the AWS Marketplace version of Deep Security Manager, Multi-Tenancy is not supported.

---

## Oracle RAC (Real Application Clusters) Support

Deep Security supports:

- SUSE Linux Enterprise Server 11 SP3 with Oracle RAC 12c Release 1 (v12.1.0.2.0)
- Red Hat Linux Enterprise Server 6.6 with Oracle RAC 12c Release 1 (v12.1.0.2.0)

---

**Note:** The default Linux Server Deep Security Policy is compatible with the Oracle RAC environment, with the exception of Firewall settings. You can disable Firewall or customize the Firewall settings according to the instructions in the "Firewall Settings with Oracle RAC" section of the Deep Security Manager Help or Administrator's Guide.

---

## High Availability

The Deep Security database is compatible with database failover protection so long as no alterations are made to the database schema. For example, some database replication technologies add columns to the database tables during replication which can result in critical failures.

For this reason, database mirroring is recommended over database replication.

# Installation

# Installing the Deep Security Manager

## Before You Begin

### Database

Before you install Deep Security Manager, you must install database software, create a database and user account for Deep Security Manager to use. For information on installing a database, see [Database Considerations \(page 23\)](#).

### Co-Located Relay-enabled Agent

A Deep Security deployment requires at least one Relay (a Deep Security Agent with Relay functionality enabled). Relays distribute Software and Security Updates to Agents/Appliances which keep your protection up to date. Trend Micro recommends installing a Relay-enabled Agent on the same computer as the Deep Security Manager to protect the host computer and to function as a local Relay.

During the installation of the Deep Security Manager, the installer will look in its local directory for an Agent install package (the full zip package, not just the core Agent installer). If it doesn't find an install package locally, it will attempt to connect to the Trend Micro Download Center over the Internet and locate an Agent install package there. If it locates an install package in either of those locations, it will give you the option to install a co-located Relay-enabled Agent during the installation of the Deep Security Manager. (If Agent install packages are found in both locations, the latest of the two versions will be selected.) The Agent can be used to protect the Deep Security manager host machine, however it will initially be installed with only the Relay module enabled. To enable protection you will have to apply an appropriate Security Policy.

If no Agent install package is available, the installation of the Deep Security Manager will proceed without it (but you will have to install a Relay-enabled Agent at a later time).

---

**Note:** Depending on your environment, additional Relay-enabled Agents can be installed at a later time. (For instructions on installing a Relay-enabled Agent, see [Installing the Deep Security Agent \(page 33\)](#) and [Configuring a Relay \(page 44\)](#).)

---

### Proxy Server Information

If the Deep Security will need to use a proxy server to connect to Trend Micro Update Servers over the Internet, have your proxy server address, port, and log in credentials ready.

### Multi-Node Manager

Deep Security Manager can be run as multiple nodes operating in parallel using a single database. Running the Manager as multiple nodes provides increased reliability, redundant availability, virtually unlimited scalability, and better performance.

Each node is capable of all tasks and no node is more important than any of the others. Users can sign in to any node to carry out their tasks. The failure of any node cannot lead to any tasks not being carried out. The failure of any node cannot lead to the loss of any data.

Each node must be running the same build number of the Manager software. When performing an upgrade of the Manager software, the first Manager to be upgraded will take over all Deep Security Manager duties and shut down all the other Deep Security Manager nodes. They will appear as "offline" in the **Network Map with Activity Graph** in the **System Activity** section of the **System Information** page with an indication that an upgrade is required. As the upgrades are carried out on the other nodes, they will automatically be brought back online and begin sharing in the DSM tasks.

**To add a Deep Security Manager node to your installation**, run the Manager install package on a new computer. When prompted, type the location of and login credentials for the database being used. Once the installer connects to the database, you can proceed with adding the node to the system.

---

**Note:** You must be using either MS SQL Server or Oracle Database to run multiple nodes.

---

**Note:** At no point should more than one instance of the installer be running at the same time. Doing so can lead to unpredictable results including corruption of the database.

---

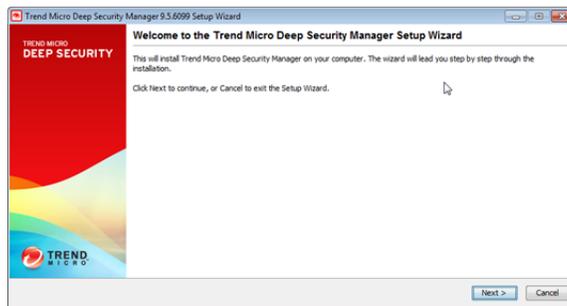
## Download the the Installer Package

Download the latest version of the Deep Security Manager (and optionally the Deep Security Agent) software from the Trend Micro Download Center at:

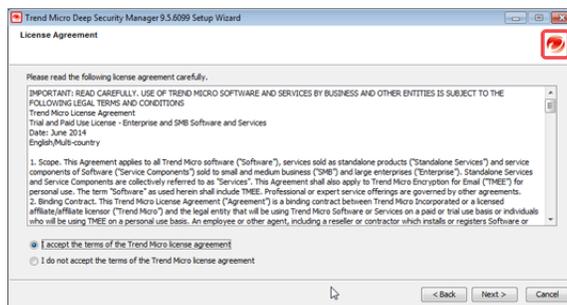
<http://downloadcenter.trendmicro.com/>

## Install the Deep Security Manager for Windows

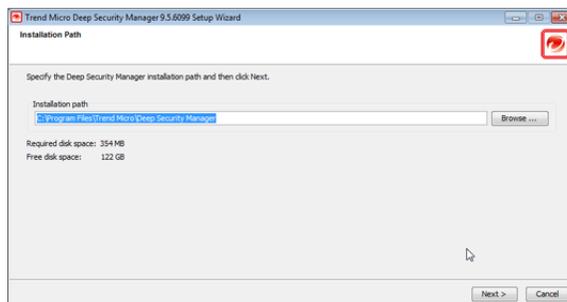
1. Copy the Deep Security Manager installer package to the target machine. Start the Deep Security Manager installer by double-clicking the install package.



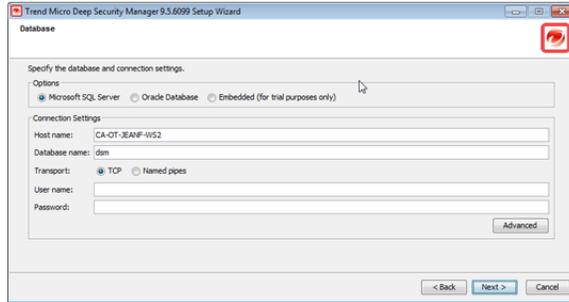
2. **License Agreement:** If you agree to the terms of the license agreement, select **I accept the terms of the Trend Micro license agreement**.



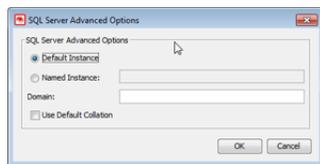
3. **Installation Path:** Select the folder where Deep Security Manager will be installed and click **Next**.



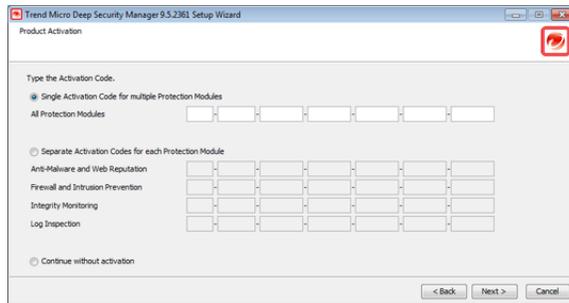
4. **Database:** Select the database you installed previously.



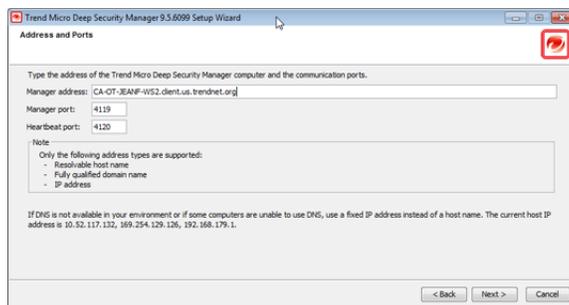
If your database is SQL Server, click **Advanced** to specify a **Named Instance**, a **Domain**, or the use of **Default Collation**. Collation determines how strings are sorted and compared. The default is "unselected", which means that Deep Security will use Latin1\_General\_CS\_AS for collation on text-type columns. If you select **Use Default Collation**, Deep Security will use the collation method specified by your SQL Server database. For additional information on collation, refer to your SQL Server documentation.



5. **Product Activation:** Enter your Activation Code(s). Enter the code for All Protection Modules or the codes for the individual modules for which you have purchased a license. You can proceed without entering any codes, but none of the Protection Modules will be available for use. (You can enter your first or additional codes after installation of the Deep Security Manager by going to **Administration > Licenses**.)



6. **Address and Ports:** Enter the hostname, URL, or IP address of this computer. The Manager Address must be either a resolvable hostname, a fully qualified domain name, or an IP address. If DNS is not available in your environment, or if some computers are unable to use DNS, a fixed IP address should be used instead of a hostname. Optionally, change the default communication ports: The "Manager Port" is the port on which the Manager's browser-based UI is accessible through HTTPS. The "Heartbeat Port" is the port on which the Manager listens for communication from the Agents/Appliances.



7. **Administrator Account:** Enter a username and password for the Master Administrator account. Selecting the Enforce strong passwords (recommended) requires this and future administrator passwords to include upper and lower-case letters, non-alphanumeric characters, and numbers, and to require a minimum number of characters.

---

**Note:** *The username and password are very important. You will need them to log in to Deep Security Manager.*

---

**Note:** *If you have admin rights on the Manager host machine, you can reset an account password using the `dsm_c -action unlockout -username USERNAME -newpassword NEWPASSWORD [-disablemfa]` command.*

---

8. **Configure Security Updates:** Selecting the **Create Scheduled Task to regularly check for Security Updates** option will create a Scheduled Task to automatically retrieve the latest Security Updates from Trend Micro and distribute them to your Agents and Appliances. (You can configure Updates later using the Deep Security Manager.) If the Deep Security Manager will need to use a proxy to connect to the Trend Micro Update servers over the Internet, select **Use Proxy Server when connecting to Trend Micro to check for Security Updates** and enter your proxy information.

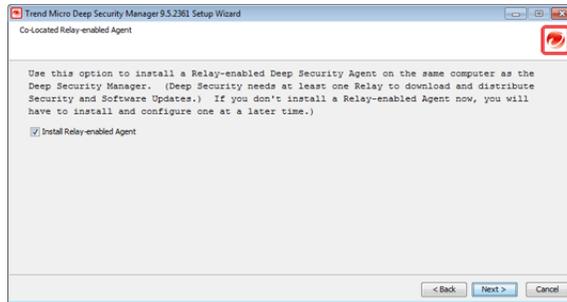
9. **Configure Software Updates:** The options for software updates are the same as those for security updates in the previous step.

10. **Co-Located Relay-enabled Agent:** If an Agent install package is available either in the local folder or from the Trend Micro Download Center, you will be given the option to install a co-located Relay-enabled Agent. Any Deep Security installation requires at least one Relay to download and distribute Security and Software Updates. If you don't install a Relay-enabled Agent now, you will need to do so at a later time.

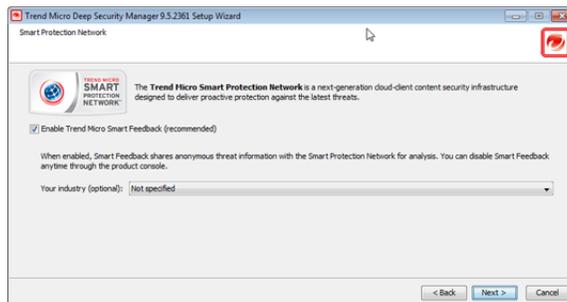
---

**Note:** *Installing a co-located Relay-enabled Agent is strongly recommended.*

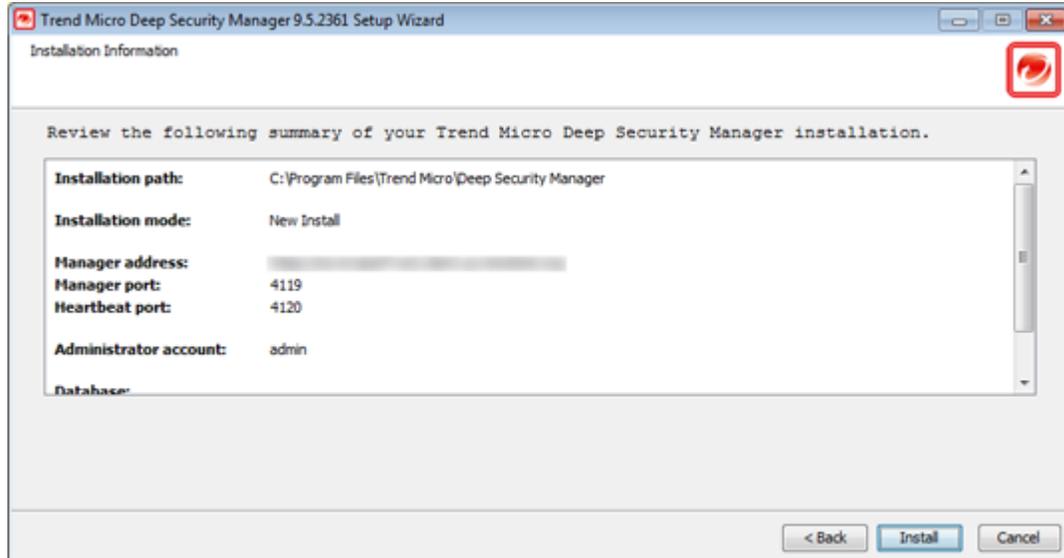
---



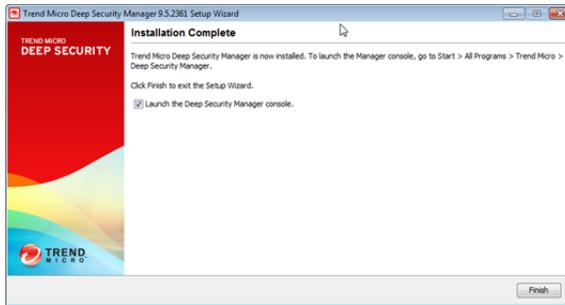
11. **Smart Protection Network:** Select whether you want to enable Trend Micro Smart Feedback (recommended). (You can enable or configure Smart Feedback later using the Deep Security Manager). Optionally enter your industry by selecting from the drop-down list.



12. **Installation Information:** Verify the information you entered and click **Install** to continue.



13. Select **Launch the Deep Security Manager console** to open web a browser to the Deep Security Manager URL when setup is complete. Click **Finish** to close the Setup wizard.



The Deep Security Manager service will start when setup is complete. The installer places a shortcut to Deep Security Manager in the program menu. You should take note of this URL if you want to access the Manager from a remote location.

## Installing the Deep Security Manager for Linux

The sequence of steps for installing Deep Security Manager on a Linux OS with X Window System are the same as those described for Windows (above). For information on performing a silent Linux installation, see [Silent Install of Deep Security Manager \(page 73\)](#).

---

**Note:** *If you are installing Deep Security Manager on Linux with iptables enabled, you will need to configure the iptables to allow traffic on TCP ports 4119 and 4120.*

---

## Starting Deep Security Manager

The Deep Security Manager service starts automatically after installation. The service can be started, restarted and stopped from the Microsoft Services Management Console. The service name is "Trend Micro Deep Security Manager".

To run the Web-based management console, go to the **Trend Micro** program group in the Start menu (MS Windows) or K-Menu (X Windows) and click **Deep Security Manager**.

To run the Web-based management console from a remote computer you will have to make note of the URL:

**https://[hostname]:[port]/**

where **[hostname]** is the hostname of the server on which you have installed Deep Security Manager and **[port]** is the "Manager Port" you specified in step 8 of the installation (4119 by default).

Users accessing the Web-based management console will be required to sign in with their User Account credentials. (The credentials created during the installation can be used to log in and create other User accounts.)

---

**Note:** *The Deep Security Manager creates a 10-year self-signed certificate for the connections with Agents/Appliances, Relays, and Users' web browsers. However, for added security, this certificate can be replaced with a certificate from a trusted certificate authority (CA). (Such certificates are maintained after a Deep Security Manager upgrade.) For information on using a certificate from a CA, see [Creating an SSL Authentication Certificate \(page 85\)](#).*

---

## Manually Importing Additional Deep Security Software

Deep Security Agents and their supporting software packages can be imported from within the Deep Security Manager on the **Administration > Updates > Software > Download Center** page. Other software packages must be imported manually from the Trend Micro Download Center web site (<http://downloadcenter.trendmicro.com/>).

**To manually import additional Deep Security software to the Deep Security Manager:**

1. Download the software from the Trend Micro Download Center web site to a local directory.

2. In the Deep Security Manager, go to **Administration > Updates > Software > Local** and click **Import...** in the toolbar to display the **Import Software** wizard.
3. Use the **Browse...** option to navigate to and select your downloaded software.
4. Click **Next** and then **Finish** to exit the wizard.

The software is now imported into the Deep Security Manager.

# Manually Installing the Deep Security Agent

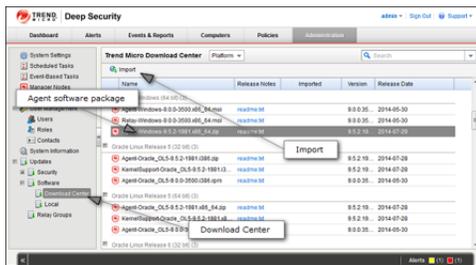
This section describes how to install and activate Deep Security Agents and how to enable Relay functionality (if required).

## Importing Agent Software

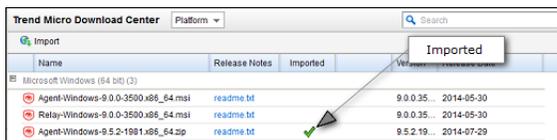
A Deep Security Agent is initially installed with core functionality only. It is only when a Protection Module is enabled on an Agent that the plug-ins required for that module are downloaded and installed. *For this reason, Agent software packages must be imported into Deep Security Manager before you install the Agent on a computer.* (A second reason for importing the Agent to Deep Security Manager is for the convenience of being able to easily extract the Agent installer from it using the Deep Security Manager's UI.)

### To import Agent software packages to Deep Security:

1. In Deep Security Manager, go to **Administration > Updates > Software > Download Center**. The **Download Center** page displays the latest versions all Agent software available from Trend Micro.
2. Select your Agent software package from the list and click **Import** in the menu bar. Deep Security will begin to download the software from the Trend Micro Download Center to the Deep Security Manager.



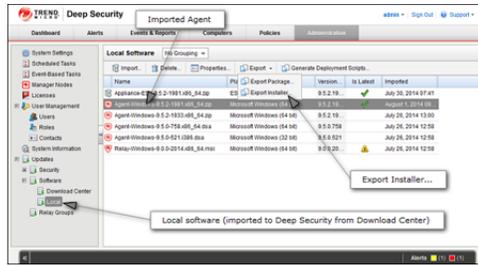
3. When the software has finished downloading, a green check mark will appear in the **Imported** column for that Agent.



### To export the Agent installer:

1. In Deep Security Manager, go to **Administration > Updates > Software > Local**.
2. Select your Agent from the list and select **Export > Export Installer...** from the menu bar.

**Note:** *If you have older versions of the Agent for the same platform, the latest version of the software will have a green check mark in the **Is Latest** column.*



3. Save the Agent installer to a local folder.

**Note:** Only use the exported Agent **installer** (the .msi or the .rpm file) on its own to install the Deep Security Agent. If you extract the full Agent zip package and then run the Agent installer from the same folder that holds the other zipped Agent components, all the Security Modules will be installed (but not turned on). If you use the Agent installer, individual Modules will be downloaded from Deep Security Manager and installed on an as-needed basis, minimizing the impact on the local computer.

The Deep Security Agent "zip" files are made available on the Trend Micro Download Center for users who need to manually import the Agents into their Deep Security environment because their Deep Security Manager is air-gapped and cannot connect directly to the Download Center web site. Users whose Deep Security Manager is able to connect to the Download Center are strongly encouraged to import their Agent software packages using the Deep Security Manager console. Attempting to install an Agent when the corresponding software package has not been imported to Deep Security Manager can lead to serious issues.

## Installing the Windows Agent

1. Copy the Agent installer file to the target machine and double-click the installation file to run the installer package. At the Welcome screen, click **Next** to begin the installation.

**Note:** On Windows Server 2012 R2 Server Core, you must launch the installer using this command: `msiexec /i Agent-Core-Windows-9.6.x-xxxx.x86_64.msi`

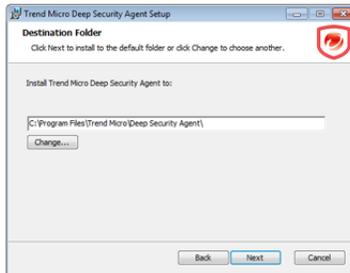
**Note:** When installing the Agent on Windows 2012 Server Core, the Notifier will not be included.



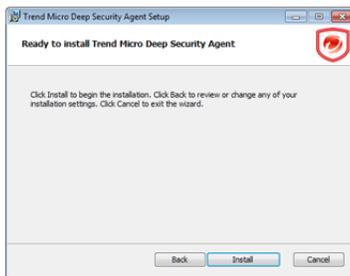
2. **End-User License Agreement:** If you agree to the terms of the license agreement, select **I accept the terms of the license agreement** and click **Next**.



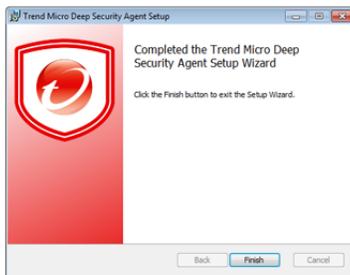
3. **Destination Folder:** Select the location where you would like Deep Security Agent to be installed and click **Next**.



4. **Ready to install Trend Micro Deep Security Agent:** Click **Install** to proceed with the installation.



5. **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:** *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.*

---

## Installing the Red Hat, SUSE, Oracle Linux, or Cloud Linux Agent

---

**Note:** You must be logged on as "root" to install the Agent. Alternatively, you can use "sudo".

---

1. Copy the installation file to the target machine.
2. Use "rpm -i" to install the ds\_agent package:

```
# rpm -i <package name>
Preparing... ##### [100%]
1:ds_agent ##### [100%]
Loading ds_filter_im module version ELx.x [ OK ]
Starting ds_agent: [ OK ]
```

(Use "rpm -U" to upgrade from a previous install. This approach will preserve your profile settings)

3. The Deep Security Agent will start automatically upon installation.

## Installing the Ubuntu or Debian Agent

Follow the instructions under "Importing Agent Software" (above) to import the appropriate Ubuntu or Debian Agent software package from the Download Center to Deep Security Manager and then export the installer (.deb file).

To install on Ubuntu or Debian, copy the installer file (.deb) to the target machine and use the following command:

```
sudo dpkg -i <installer file>
```

## Starting, stopping and resetting the Agent on Linux:

Command-line options:

To start the Agent:

```
/etc/init.d/ds_agent start
```

To stop the Agent:

```
/etc/init.d/ds_agent stop
```

To reset the Agent:

```
/etc/init.d/ds_agent reset
```

To restart the Agent:

```
/etc/init.d/ds_agent restart
```

## Installing the Solaris Agent

### Requirements:

For Solaris Sparc/9:

- libiconv 1.11 or better

- pfil\_Solaris\_x.pkg
- Agent-Solaris\_5.9-9.0.0-xxxx.sparc.pkg.gz

For Solaris X86/10:

- Agent-Solaris\_5.10\_U7-9.0.0-xxxx.x86\_64.pkg.gz
- Agent-Solaris\_5.10\_U5-9.0.0-xxxx.x86\_64.pkg.gz

For Solaris X86/11:

- Agent-Solaris\_5.11-9.0.0-xxxx.i386.p5p.gz

For Solaris SPARC/11:

- Agent-Solaris\_5.11-9.0.0-xxxx.sparc.p5p.gz

## To install the Solaris 11 Agent:

1. Copy the installation file to the target machine
2. Install the agent:

```
gunzip Agent-Solaris_5.x_sparc-9.x.x-xxxx.sparc.p5p.gz
pkg install -g Agent*p5p ds-agent
svcadm enable ds_agent
```

## To install the Solaris 10 Agent:

1. Copy the installation file to the target machine
2. Install the Agent:

```
gunzip Agent-Solaris_5.10_U7-9.x.x-xxxx.x86_64.pkg.gz
pkgadd -d Agent-Solaris_5.10_U7-9.x.x-xxxx.x86_64.pkg all
```

## To install the Solaris Sparc 9 Agent:

1. Acquire all of the required packages (see above)
2. Copy the installation file to the target machine
3. Install libiconv-1.8-solx-sparc.gz:

```
gunzip libiconv-1.8-solx-sparc.gz
pkgadd -d libiconv-1.8-solx-sparc all
```

4. Install libgcc-3.4.6-solx-sparc.gz:

```
gunzip libgcc-3.4.6-solx-sparc.gz
pkgadd -d libgcc-3.4.6-solx-sparc all
```

5. Install pfil:

```
pkgadd -d pfil_Solaris_x.pkg all
```

6. Push the pfil stream module into the network interface:

```
ifconfig <interface> modinsert pfil@2
```

---

**Note:** *pfil should go right after ip in the network interface stream. To determine where ip is, perform: ifconfig <interface> modlist and ensure that the number used on the modinsert is one higher than the number of ip in the modlist.*

---



---

**Note:** *pfil must be added to the network stack for each of the interfaces the Agent will be protecting touch /etc/ipf.conf/etc/init.d/pfil start (For more information, see "Notes on Installing PFIL on a Solaris (8 and 9 Sparc) Host ", below.)*

---

7. Install the Agent:

```
gunzip Agent-Solaris_5.x_sparc-9.x.x-xxxx.sparc.pkg.gz
pkgadd -d Agent-Solaris_5.x_sparc-9.x.x-xxxx.sparc.pkg all
```

## To start, stop and reset the Agent on Solaris 10 and 11

- `svcadm enable ds_agent` - starts the Agent
- `svcadm disable ds_agent` - stops the Agent
- `/opt/ds_agent/dsa_control -r` - resets the Agent
- `svcadm restart ds_agent` - restarts the Agent
- `svcs -a | grep ds_agent` - displays Agent status

## To start, stop and reset the Agent on Solaris 9:

- `/etc/init.d/ds_agent start` - starts the Agent
- `/etc/init.d/ds_agent stop` - stops the Agent
- `/opt/ds_agent/dsa_control -r` - resets the Agent
- `/etc/init.d/ds_agent restart` - restarts the Agent

---

**Note:** *Note that the filtering activity log files are in /var/log/ds\_agent*

---

## Notes on Installing PFIL on a Solaris (8 and 9 Sparc) Host

The Solaris Agent uses the PFIL IP filter component developed by Darren Reed. Deep Security currently supports version 2.1.11. We have built this source code and provided a package on the Trend Micro Download Center, <http://downloadcenter.trendmicro.com>.

Further information can be found at: <http://coombs.anu.edu.au/~avalon>. (For a copy of the PFIL source code, contact your support provider.)

## Notes on pfil

(The following assumes your interface is hme)

If you do "ifconfig modlist", you will see a list of STREAMS modules pushed onto the interface like this (for hme0):

```
0 arp
1 ip
2 hme
```

You need to insert pfil between ip and hme:

```
ifconfig hme0 modinsert pfil@2
```

Checking the list, you should see:

```
0 arp
1 ip
2 pfil
3 hme
```

To configure the pfil Streams module to be automatically pushed when the device is opened:

```
autopush -f /etc/opt/pfil/iu.ap
```

At this point,

```
strconf < /dev/hme
```

should return:

```
pfil
hme
```

Also, `modinfo` should show:

```
# modinfo | grep pfil
110 102d392c 6383 24 1 pfil (pfil Streams module 2.1.11)
110 102d392c 6383 216 1 pfil (pfil Streams driver 2.1.11)
```

## Installing the HP-UX Agent

1. Log in as Root
2. Copy the installation file to the target machine
3. Copy the package to a temporary folder ("/tmp")
4. Unzip the package using `gunzip`:

```
/tmp> gunzip Agent-HPUX_xx.xx-x.x.x-xxxx.ia64.depot.gz
```

5. Install the Agent: (Note that the package is referenced using the full path. Relative paths will not be accepted.)

```
/tmp> swinstall -s /tmp/Agent-HPUX_xx.xx-x.x.x-xxxx.ia64.depot ds_agent
```

To start and stop the Agent on HP-UX, enter one of the following:

- `/sbin/init.d/ds_agent start`
- `/sbin/init.d/ds_agent stop`

## Installing the AIX Agent

1. Log in as Root

2. Copy the installation file to the target machine
3. Copy the package to a temporary folder ("/tmp")
4. Unzip the package using gunzip:

```
/tmp> gunzip Agent-AIX_x.x-x.x.x-xxxx.powerpc.bff.gz
```

5. Install the Agent:

```
/tmp> installp -a -d /tmp/Agent-AIX_x.x-x.x.x-xxxx.powerpc.bff ds_agent
```

To start the Agent on AIX:

```
# startsrc -s ds_agent
```

To stop the Agent on AIX:

```
# stopsrc -s ds_agent
```

To load the driver on AIX:

```
# /opt/ds_agent/ds_fctrl load
```

To unload the driver on AIX:

```
# /opt/ds_agent/ds_fctrl unload
```

## Using Deployment Scripts to Install Agents

Adding a computer to your list of protected resources in Deep Security and implementing protection is a multi-step process. Most of these steps can be performed locally from the command line on the computer and can therefore be scripted. The Deep Security Manager's Deployment Script generator can be accessed from the Manager's Support menu.

---

**Note:** When installing the Agent on Windows 2012 Server Core, the Notifier will not be included.

---

### To generate a deployment script:

1. Start the Deployment Script generator by clicking **Deployment Scripts...** from the Deep Security Manager's Support menu (at the top right of the Deep Security Manager window).
2. Select the platform to which you are deploying the software.

---

**Note:** Platforms listed in the drop-down menu will correspond to the software that you have imported into the Deep Security Manager.

---

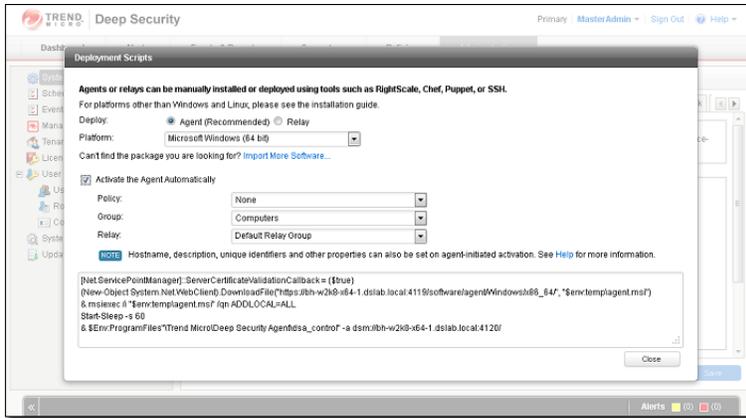
3. Select **Activate Agent automatically after installation**. (Optional, but Agents must be activated by the Deep Security Manager before a protection Policy can be implemented.)
4. Select the Policy you wish to implement on the computer (optional)
5. Select the computer Group (optional)
6. Select the Relay Group

As you make the above selections, the Deployment Script Generator will generate a script which you can import into your deployment tool of choice.

---

**Note:** The Deployment Script Generator can also be started from the menu bar on the **Administration > Updates > Software > Local** page.

---



**Note:** The deployment scripts generated by Deep Security Manager for Windows Agents must be run in Windows PowerShell version 2.0 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:** On windows machines, 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.

## Iptables on Linux

Deep Security 9.5 or later does not disable Linux iptables during installation. If the Firewall or Intrusion Prevention modules are enabled, iptables is disabled. If the Agent is disabled, iptables is enabled and the settings are reverted. For instructions on how to prevent the Deep Security Agent from changing iptables, see the *Deep Security Best Practice Guide*.

## Activating the Agent

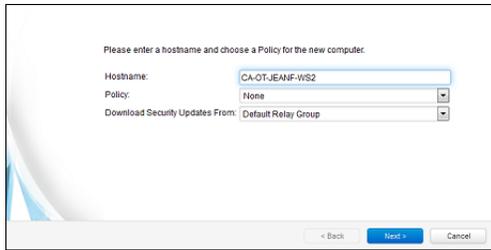
The Agent must be activated from the Deep Security Manager before it can be configured to act as a Relay or to protect the host computer.

**To activate the newly installed Agent:**

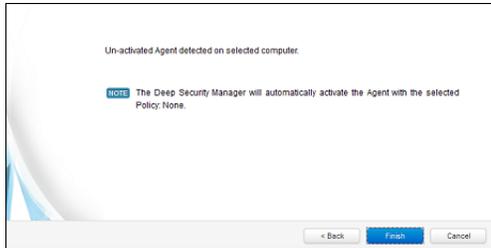
1. In the Deep Security Manager, go to the Computers page and click **New > New Computer...** to display the **New Computer Wizard**.



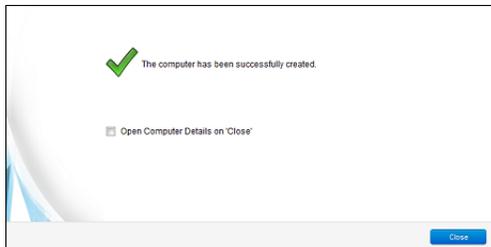
2. Enter the hostname or IP address of the computer. If you want to use the Agent to provide protection for the host computer as well as function as a Relay, select a Deep Security Policy from the **Policy** menu. Otherwise leave **Policy** set to "None".



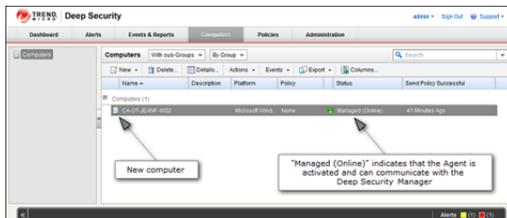
- The wizard will confirm that it will activate the Agent on the computer and apply a Security Policy (if one was selected).



- On the final screen, de-select "Open Computer Details on 'Close'" and click **Close**.



- The Agent is now activated. In the Deep Security Manager, go to the **Computers** screen and check the computer's status. It should display "Managed (Online)".



## Enabling Relay Functionality

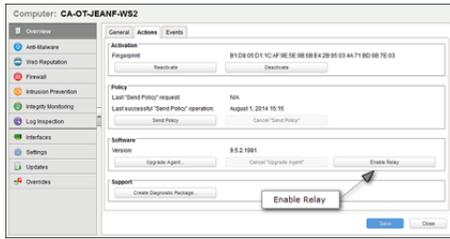
Any activated 64-bit Windows or Linux Agent can be configured to act as a Relay, downloading and distributing Security and Software Updates.

**Note:** Once enabled on an Agent, Relay functionality cannot be disabled.

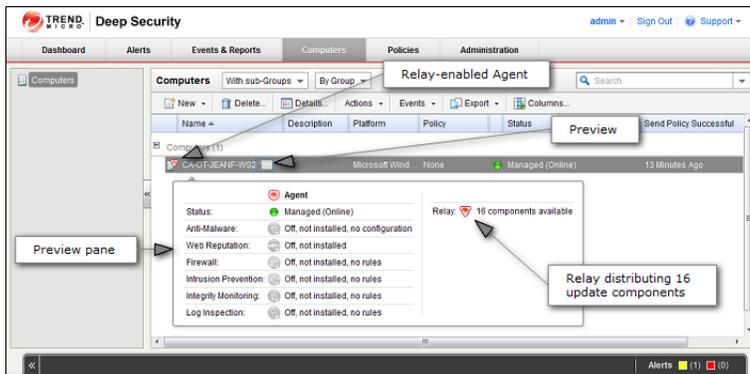
### To enable Relay functionality:

- In the Deep Security Manager, go to the **Computers** page, double-click the computer with the newly-activated Agent to display its **Details** editor window.

- In the computer editor, go to the **Overview > Actions > Software** area and click **Enable Relay**. Click **Close** to close the editor window.



- In the Deep Security Manager on the Computers page, the computer's icon will change from ordinary computer (  ) to computer with Relay-enabled Agent (  ). Click the **Preview** icon to display the Preview Pane where you can see the number of Update components the Relay Module is ready to distribute.



## Considerations for Windows 2012 Server Core

There are a few things you should keep in mind when running a Deep Security Agent with 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.

# Installing and Configuring a Relay-enabled Agent

A Relay is a Deep Security Agent with Relay functionality enabled. Relays download and distribute Security and Software Updates to your Deep Security Agents and Appliances. You must have at least one Relay-enabled Agent to keep your protection up to date.

## Install and Activate a Deep Security Agent

If you do not already have an agent installed on a computer, do so by following the instructions in [Installing the Deep Security Agent \(page 33\)](#). You skip ahead to the section on "Manual Installation".

Once the Agent is installed, you need to Activate it.

### To Activate the Agent,

1. In the Deep Security Manager, go to the Computers page.
2. In the menu bar, click **New > New Computer...** to display the **New Computer** Wizard.
3. For **Hostname**, enter the hostname or IP address of the computer on which you just installed the Agent.
4. For **Policy**, select an appropriate policy.
5. For **Download Security Updates From**, leave the default setting (Default Relay Group).
6. Click **Finish**. Deep Security Manager will import the computer to its Computers page and activate the Agent.

## Enable Relay Functionality on a Deep Security Agent

### To enable Relay functionality on an installed Deep Security Agent:

1. The Adding a new computer and activation process should have finished by opening the Computer's **Editor** window. If it hasn't, follow step two (below) to open the window.
2. In the Deep Security Manager, go to the **Computers** screen, find the Agent on which you want to enable Relay functionality and double-click it to open its **Computer Editor** window.
3. In the **Computer Editor** window, go to **Overview > Actions > Software** and click **Enable Relay**.

---

**Note:** If you do not see the **Enable Relay** button, go to **Administration > Updates > Software > Local** to check whether the corresponding package has been imported. Also ensure that the computer running a 64-bit version of the Agent.

---

Deep Security Manager will install the plug-ins required by the Relay Module, and the Agent will begin to function as a Relay.

---

**Note:** If you are running Windows Firewall or iptables, you also need to add a Firewall Rule that allows TCP/IP traffic on port 4122 on the Relay-enabled Agents.

---



---

**Note:** Relay-enabled Agents are organized into **Relay Groups**. New Relay-enabled Agents are automatically assigned to the **Default Relay Group**. The Default Relay Group is configured to retrieve Security and Software Updates from the Primary Security Update Source defined in the Deep Security Manager on the **Administration > System Settings > Updates** tab. (The Primary Update Source by default is Trend Micro's Update Servers, but this configurable.)

---

# Deploying Agentless Protection in an NSX Environment

## Requirements

### Deep Security Requirements

The following Trend Micro Deep Security software must be installed or imported:

- **The Deep Security Manager 9.6 SP1 must be installed.** (See [Installing the Deep Security Manager \(page 26\)](#).)

---

*Note:* The Deep Security Manager should ideally be installed on a dedicated ESXi in the same datacenter.

---

- **A Deep Security Agent with Relay functionality enabled must be installed and activated, and all Updates must have completed downloading.** (For instructions on installing and configuring an Agent with a Relay, see [Installing the Deep Security Agent \(page 33\)](#) and [Installing and Configuring a Relay-enabled Agent \(page 44\)](#).)
- **The Deep Security Virtual Appliance software package must be imported into Deep Security Manager.** Once the Virtual Appliance is running in the datacenter, it will need to connect to a Relay-enabled Agent to have access to the latest Security and Software Updates.

**To import the Deep Security Virtual Appliance software:**

1. Download the Deep Security Virtual Appliance software package from the Trend Micro Download Center (<http://downloadcenter.trendmicro.com>) to the Deep Security Manager host machine.
2. In the Deep Security Manager, go to the **Administration > Updates > Software > Local** page and click **Import...** in the toolbar and import the software package to Deep Security. (The Deep Security manager will then automatically download the latest 64-bit Red Hat agent software package which will later be used to upgrade the Virtual Appliance's Protection Modules.)

#### Installing the Deep Security Agent

In an NSX environment, the Deep Security Virtual Appliance provides Anti-Malware, Integrity Monitoring, Web Reputation Service, Firewall, and Intrusion Prevention for your virtual machines, without requiring an Agent. This is the recommended deployment method.

If you decide to also install a Deep Security Agent on your virtual machines, the Deep Security Virtual Appliance will only provide Anti-Malware and Integrity Monitoring. The Deep Security Agent will provide Web Reputation Service, Firewall, Intrusion Prevention, and also Log Inspection. This is known as "Combined Mode".

## VMware Requirements

**You must be running the following VMware software:**

- **VMware vSphere 5.5 or 6.0**
  - **VMware vCenter 5.5 or 6.0**
  - **VMware ESXi 5.5 or 6.0**
  - **VMware vSphere Web Client** (requires a Flash-enabled web browser)
- **VMware NSX Manager 6.1.5 or 6.2**

**Your NSX datacenter must meet the following configuration requirements:**

- **The datacenter must be using a vSphere Distributed Switch (vDS).** (For a quick guide to installing a vSphere Distributed Switch, see [Installing a vSphere Distributed Switch \(page 89\)](#).)

- **ESXi servers must be connected to the Distributed Switch.**
- **Your ESXi servers must be grouped into clusters, even if you only have a single ESXi in a single cluster.** (The ESXi servers must be connected to the vDS *before* they are moved into clusters.)
- **Your cluster must be prepared by installing the drivers that will allow network traffic inspection on all ESXi servers.** (For a quick guide to host preparation, see [Preparing ESXi servers \(page 90\)](#).)
- **Guest Introspection service must be installed on the cluster that you want to protect.** (For a quick guide to installing Guest Introspection service, see [Installing Guest Introspection service \(page 91\)](#).)
- **Virtual machines must belong to an NSX Security Group.** (For a quick guide to creating NSX Security Groups, see [Creating NSX Security Groups \(page 93\)](#).)
- **Virtual machines must have the latest VMware Tools installed, including the VMware Guest Introspection Driver.**

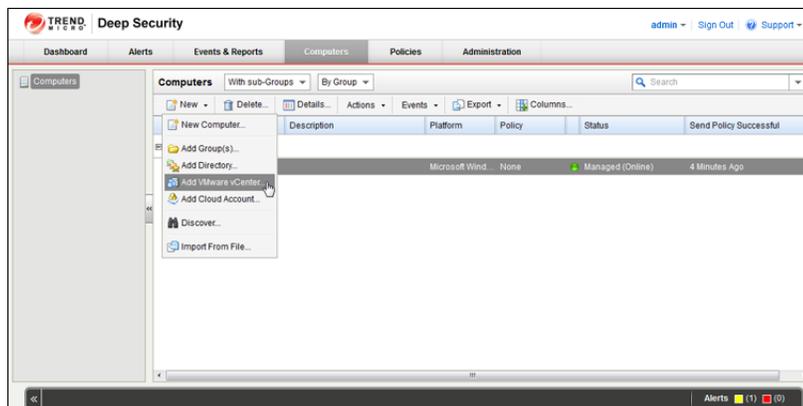
Consult your VMware documentation for more detailed information on configuring your NSX environment to meet the above requirements.

## Add the vCenter to Deep Security Manager

To manage the security of the virtual machines in your datacenter with Deep Security, you must first add the vCenter to the Deep Security Manager.

**To add the vCenter to Deep Security Manager:**

1. In the Deep Security Manager, go to the **Computers** page and click **New... > Add VMware vCenter...**



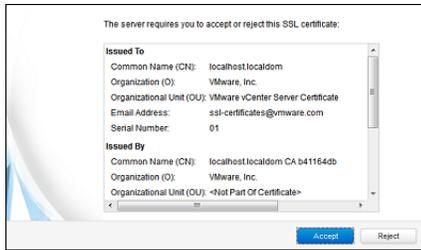
2. In the **Add VMware vCenter Wizard**, enter the following:
  - **Server:** the IP address or hostname and port to connect to the vCenter
  - **Name:** a name and description of the datacenter (for display purposes only)
  - **Credentials:** a username and password to access the vCenter

 A screenshot of the 'Add VMware vCenter Wizard' form. The form is titled 'Please provide the following information for the vCenter being added.' and is divided into three sections:
 

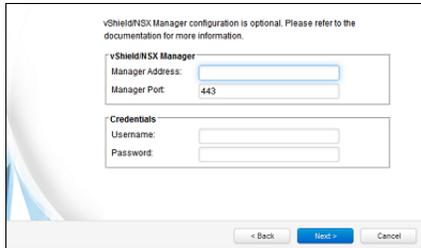
- Server:** Contains two input fields: 'Server Address' and 'Server Port' (with '443' pre-filled).
- Name:** Contains two input fields: 'Name' and 'Description'.
- Credentials:** Contains two input fields: 'Username' and 'Password'.

 At the bottom of the form, there are three buttons: '< Back', 'Next >', and 'Cancel'.

3. Accept the SSL certificate if required.



4. Enter the NSX Manager Server Address, and the required credentials.

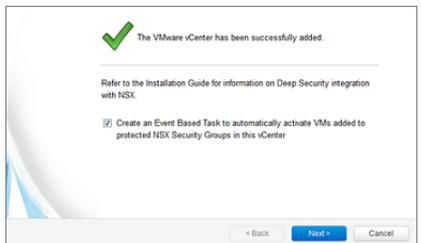
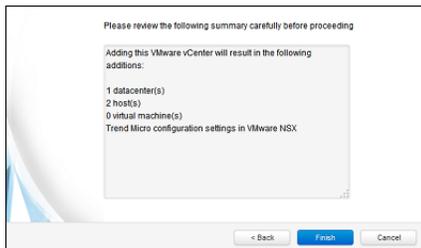



---

**Note:** *If the vCenter was previously added to another Deep Security Manager, the wizard displays a message reminding you to remove all Deep Security Virtual Appliances from your ESXi servers and to delete any old NSX Security Policies. If you have performed those actions, select "I have removed all Deep Security services and NSX Security Policies that reference the previous deployment. I want to overwrite the previous deployment settings." and then click **Next**.*

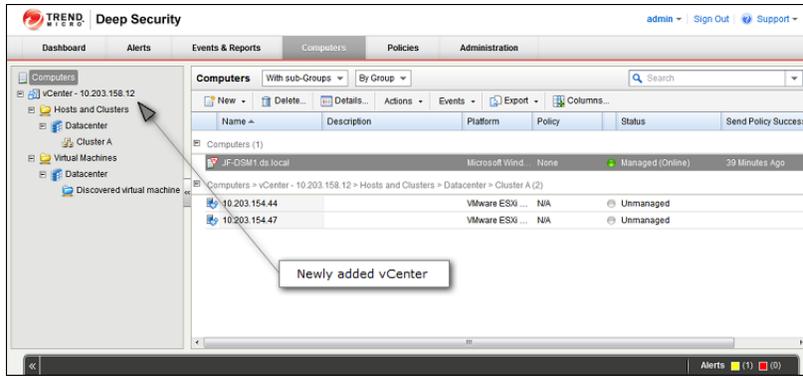
---

5. Accept the SSL certificate if required.
6. The **Add VMware vCenter Wizard** will display a successful result message when the vCenter has been imported. Click **Finish** and then **Close** to close the wizard.



If selected, the option shown in the image above creates two Event-Based Tasks. One activates VMs when protection is added and the other deactivates VMs when protection is removed. For more information, see "Event-Based Tasks Created When Adding a vCenter to Deep Security Manager" in [Automated Policy Management in NSX Environments \(page 60\)](#).

When Deep Security Manager adds the vCenter to its inventory, it also registers the Deep Security service within NSX Manager. This permits the deployment of the Deep Security service to the ESXi servers.



## Synchronize Deep Security Policies with NSX

There are two ways to protect your VMs with Deep Security:

- Use event-based tasks to activate and deactivate VMs in Deep Security and apply or remove a default policy. For more information, see "Event-Based Tasks Created When Adding a vCenter to Deep Security Manager" in [Automated Policy Management in NSX Environments \(page 60\)](#).
- Synchronize your Deep Security policies with NSX. This method is described below.

Each VM that you want to protect must belong to an NSX Security Group, which has an NSX Security Policy assigned to it. When you set up an NSX Security Policy, one of the options that you select is the NSX Service Profile. With Deep Security 9.6 or earlier, there was only one NSX Service Profile for use with Deep Security. As of Deep Security 9.6 SP1, you can choose to synchronize all of your Deep Security policies with NSX. This creates a matching NSX Service Profile (which we call a "Mapped Service Profile" in Deep Security) for each of your Deep Security policies.

### To enable policy synchronization:

---

**Note:** *All of the policies in Deep Security Manager must have a unique name before they are synchronized with NSX.*

---

1. In the Deep Security Manager, go to the **Computers** page and right-click the vCenter where you want to enable synchronization.
2. Click **Properties**.
3. On the **NSX Configuration** tab, select **Synchronize Deep Security Policies with NSX Service Profiles**. Click **OK**.

### Next steps:

1. Create an NSX Security Policy, as described in the "Create an NSX Security Policy" section later in this chapter. Select a Mapped Service Profile as the Service Profile for the **Guest Introspection Service** and the Inbound and Outbound **Network Introspection Services**.

---

**Note:** *If you select the "Default (EBT)" service profile, the VMs in groups that use this policy will be handled by the "NSX Security Group Change" event-based tasks.*

---

2. Assign the NSX Security Policy to the NSX Security Groups containing the VMs that you want to protect, as described in the "Apply the NSX Security Policy to the NSX Security Group" section later in this chapter. Any VMs in the NSX Security Group will be activated and assigned the corresponding Deep Security policy automatically, without the use of event-based tasks.

### Changing or removing the policy assigned to a VM

When a VM is protected by a Mapped Service Profile, the policy assignment cannot be changed from within Deep Security Manager:

To change the profile used to protect a VM, you must change the NSX Security Policy or NSX Security Group from your vSphere Web Client.

If you unassign an NSX Security Policy from a group, any VMs in that group will be deactivated in Deep Security Manager.

### Changing the name of a policy

If you rename a policy in Deep Security Manager, the NSX Service Profile Name will also be changed.

### Deleting a policy

If you delete a policy in Deep Security Manager and the corresponding NSX Service Profile is not in use, it will be deleted. If the corresponding NSX Service Profile is in use, the NSX Service Profile will no longer be synchronized with Deep Security Manager and its name will be changed to indicate that it is no longer valid. If the NSX Service Profile becomes unused later, it will be deleted.

### VMware vRealize

If you are configuring a blueprint with VMware vRealize, you can assign either a NSX Security Group or an NSX Security Policy to the blueprint. The Security Group or Security Policy can both use Mapped Service Profiles.

## Install the Deep Security service

---

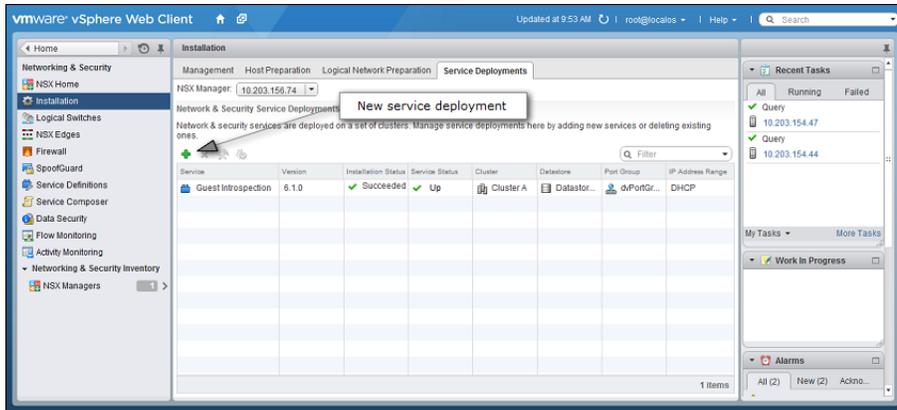
**Note:** Before installing the Deep Security service, you must first import a Deep Security Virtual Appliance into the Deep Security Manager. You must also ensure that the Guest Introspection service is installed in vSphere. (For a quick guide to installing Guest Introspection service, see [Installing Guest Introspection service \(page 91\)](#).)

---

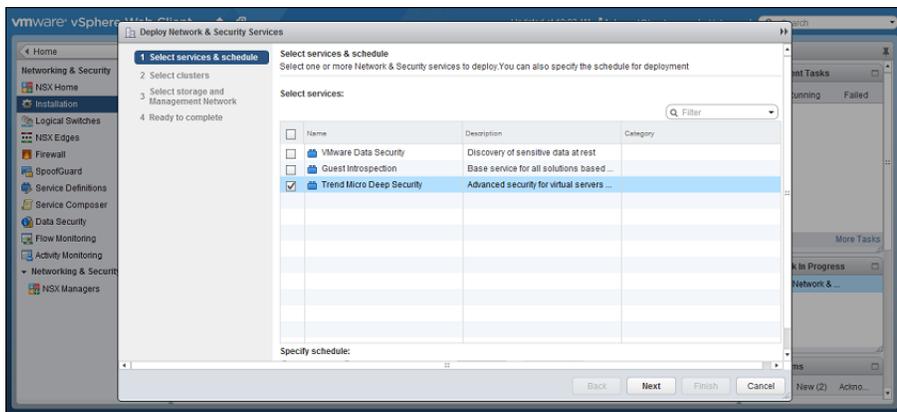
To provide agentless protection to the virtual machines on your ESXi servers, you must install the Deep Security service (the Deep Security Virtual Appliance) on the cluster that your ESXi servers belong to.

### To install the Deep Security service:

1. In the vSphere Web Client, go to **Home > Networking and Security > Installation > Service Deployments** and click the green plus sign (  ) to display the **Deploy Network & Security Services** window:

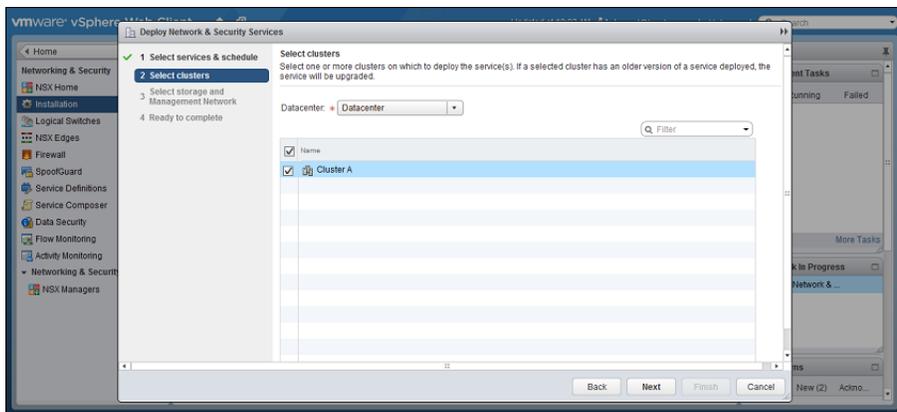


2. **Select services & schedule:** select the **Trend Micro Deep Security** service:



Click **Next**.

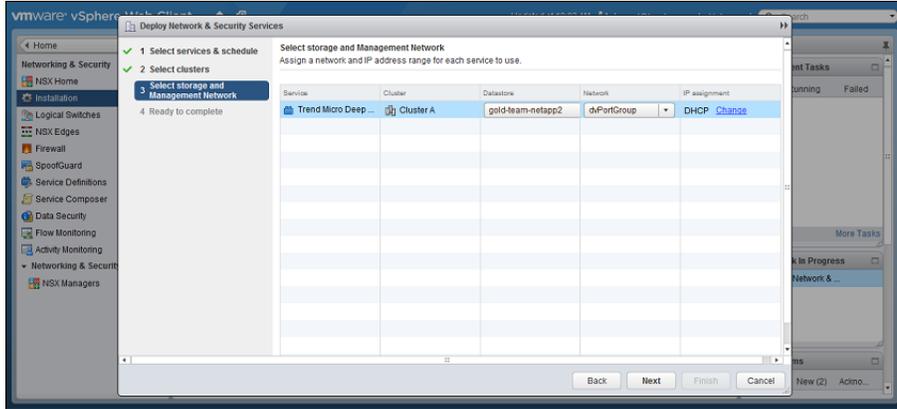
3. **Select clusters:** select the cluster(s) that includes the ESXi servers on which to deploy the Deep Security service:



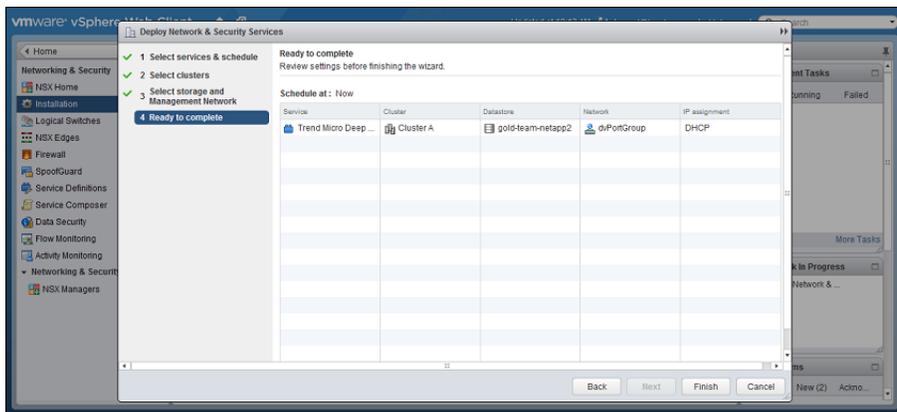
Click **Next**.

4. **Select storage and Management Network:** For each cluster, select a datastore on which to store the Deep Security Virtual Appliance, the network (the distributed port group used by the vDS on the datacenter) and the IP assignment method for the Deep Security service to use.

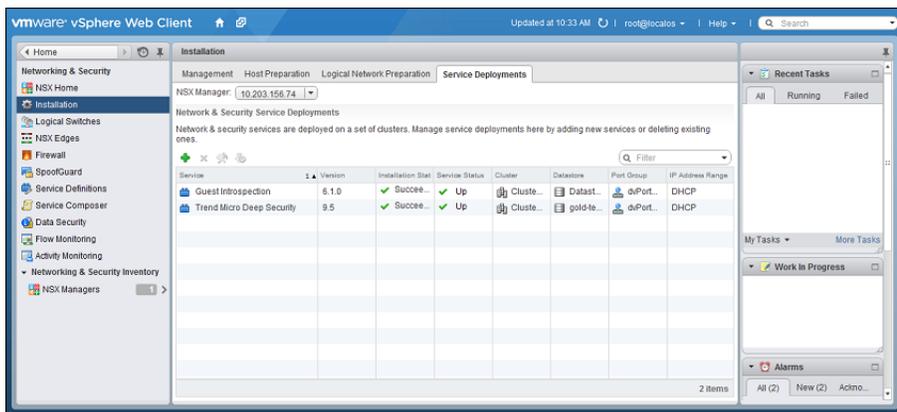
**Note:** *If you are assigning static IP pools in the "IP Assignment" column to the Deep Security service or Guest Introspection service, make sure your default gateway and DNS is reachable/resolvable and the prefix length is correct. If you do not, the Deep Security and Guest Introspection service VMs will not get activated and they will not be able to talk to NSX manager or Deep Security Manager because their IPs are not on the same network as the Deep Security Manager or the NSX Manager.*



5. Click **Next**.
6. **Ready to complete:** click **Finish** to complete the deployment of the Deep Security service:



7. When deployment is complete, you'll see the Trend Micro Deep Security service in the list of **Network & Security Service Deployments**:



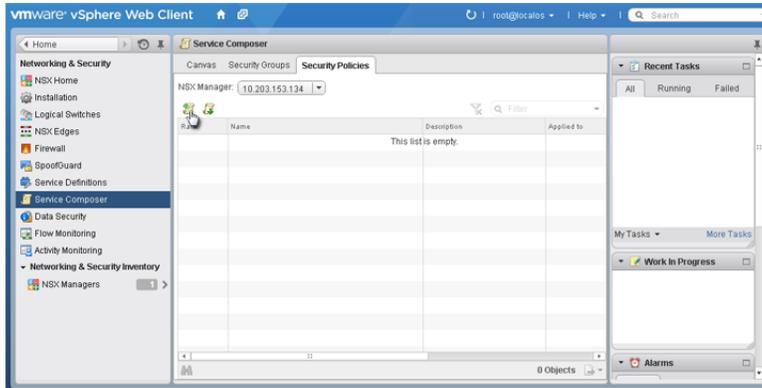
The Deep Security service is now deployed to the cluster.

## Create an NSX Security Policy

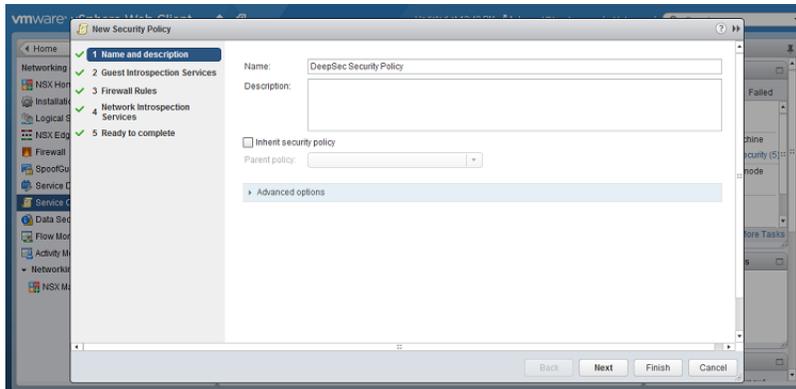
Next, you need to create a **NSX Security Policy** with Deep Security enabled as both an **Endpoint Service** and as a **Network Introspection service**.

To create a NSX Security Policy for Deep Security:

1. In your vSphere Web Client, go to **Home > Networking and Security > Service Composer** and click on the **Security Policies** tab, and click the **New Security Policy** icon (📄).

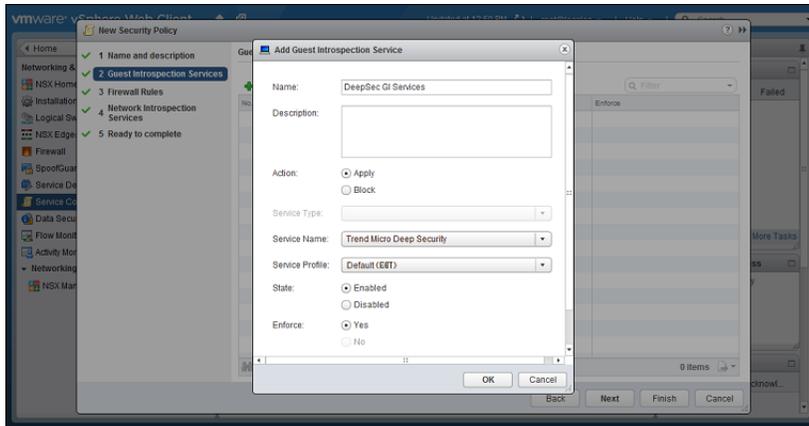


2. **Name and Description:** give a name to the new policy:



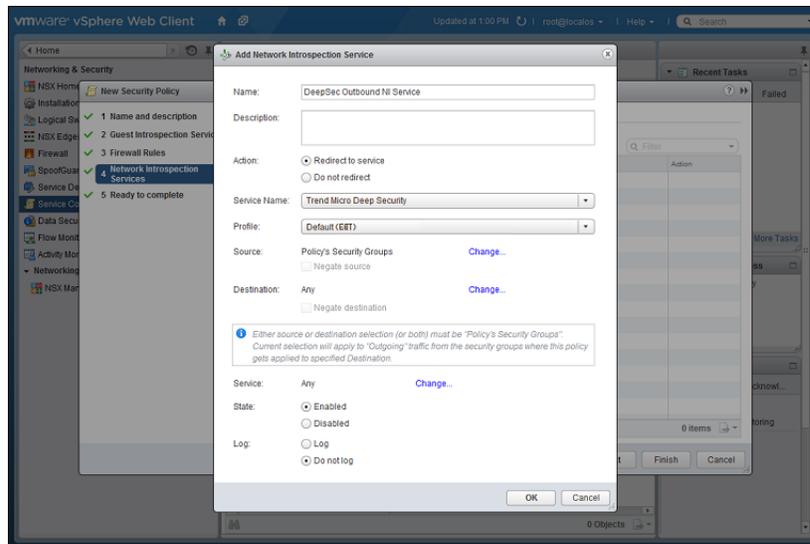
Click **Next**.

3. **Guest Introspection Services:** click the green plus sign (+) to add an **Endpoint Service**. Provide a name for the Endpoint Service and select the following settings:
  - **Action:** Apply
  - **Service Name:** Trend Micro Deep Security
  - **Service Profile:** If you are using event-based tasks to handle the creation and protection of VMs, select "Default (EBT)". If you have synchronized your Deep Security policies with NSX Service Profiles, select the Service Profile that matches the Deep Security policy that you want to apply.
  - **State:** Enabled
  - **Enforce:** Yes



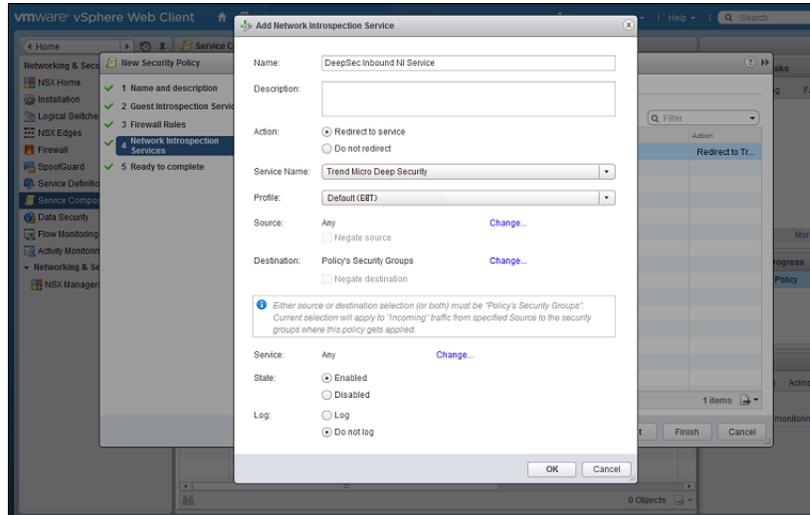
Click **OK**, then click **Next**.

4. **Firewall Rules:** do not make any changes. Click **Next**.
5. **Network Introspection Services:** You will be adding *two* Network Introspection Services to the NSX Security Policy: a first one for *outbound* traffic, and a second one for *inbound* traffic.
  1. For the first, *outbound*, service, in the **Network Introspection Services** options, click the green plus sign to create a new service. In the **Add Network Introspection Service** window, provide a name for the service (preferably one that includes the word "Outbound") and select the following settings:
    - **Action:** Redirect to service
    - **Service Name:** Trend Micro Deep Security
    - **Profile:** Select the same NSX Service Profile as you did in step 3.
    - **Source:** Policy's Security Groups
    - **Destination:** Any
    - **Service:** Any
    - **State:** Enabled
    - **Log:** Do not log



2. For the second, *inbound*, service, in the **Network Introspection Services** options, click the green plus sign to create a new service. In the **Add Network Introspection Service** window, provide a name for the service (preferably one that includes the word "Inbound") and select the following settings:

- **Action:** Redirect to service
- **Service Name:** Trend Micro Deep Security
- **Profile:** Select the same NSX Service Profile as you did in step 3.
- **Source:** Any
- **Destination:** Policy's Security Groups
- **Service:** Any
- **State:** Enabled
- **Log:** Do not log



3. Click **OK** in the **Add Network Inspection Service** window, and then click **Finish** to complete and close the **New Security Policy** window.

You have now created your NSX Security Policy for Deep Security.

## Apply the NSX Security Policy to the NSX Security Group

You must now apply the Security Policy to the Security Group containing the VMs you want to protect.

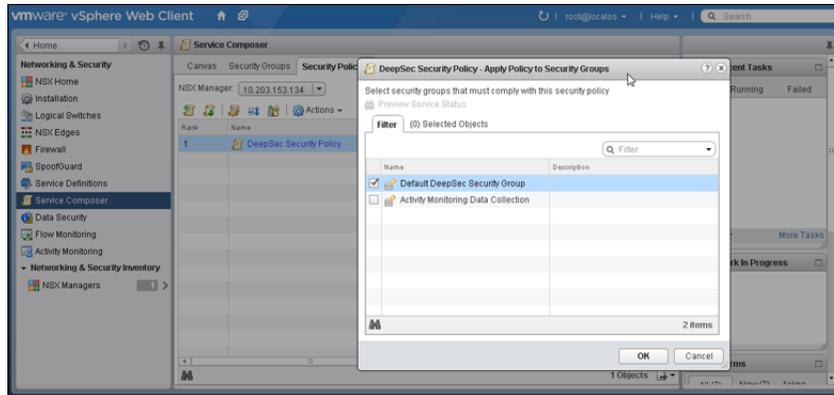
---

**Note:** *The virtual machines you want to protect with Deep Security must belong to a NSX Security Group. (For a quick guide to creating NSX Security Groups, see [Creating NSX Security Groups \(page 93\)](#).)*

---

### To apply the Security Policy to the Security Group:

1. Stay on the **Security Policies** tab of the **Home > Networking & Security > Service Composer** page in your vSphere Web Client. With the new Security Policy selected, click the **Apply Security Policy** icon ()
2. In the **Apply Policy to Security Groups** window, select the Security Group that contains the VMs you want to protect and click **OK**.



The NSX Security Policy is now applied to the VMs in the NSX Security Group.

## Adding Additional ESXi Servers to Your NSX Cluster After Deep Security Integration

Adding a new ESXi server to a NSX cluster that is protected by Deep Security must be done in the following sequence:

1. Add Host to the DataCenter *but not directly to the cluster*.
2. Connect the Host to the Distributed Switch.
3. Move the Host into the cluster.

Once the Host is moved into the cluster, the Deep Security service will be deployed automatically.

## Apply Deep Security Protection to Your VMs

You can now return to the Deep Security Manager console where you can activate the VMs in the imported vCenter and apply Deep Security Policies to them. For information on using Deep Security to protect your VMs, see the User's Guide section of the Deep Security Manager's online help, in particular, the **Adding Computers** and **Deploying Protection** sections.

---

**Note:** *If you selected the checkbox at the end of the "Add the vCenter to Deep Security Manager" procedure, an Event-Based Task will activate the VMs in the Security Group. For more information, see "Event-Based Tasks Created When Adding a vCenter to Deep Security Manager" in [Automated Policy Management in NSX Environments \(page 60\)](#).*

---

**Note:** *This step is not necessary if you are using Mapped NSX Service Profiles, as described in "Synchronize Deep Security Policies with NSX".*

---

## VMware NSX Security Tags

Deep Security can apply **NSX Security Tags** to protected VMs upon detecting a malware threat. NSX Security Tags can be used with NSX Service Composer to automate certain tasks such as, for example, quarantining infected VMs. Consult your VMware NSX documentation for more information on NSX Security Tags and dynamic NSX Security Group assignment.

---

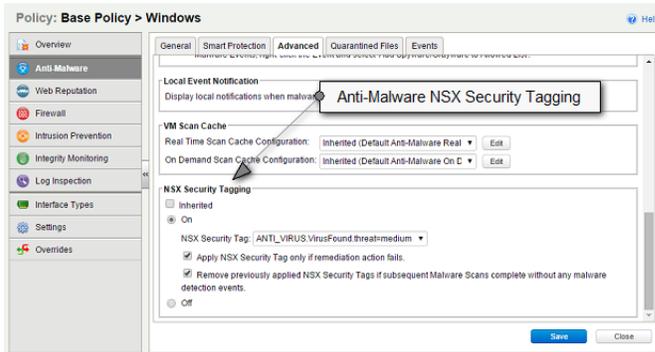
**Note:** *NSX Security Tags are part of the VMware vSphere NSX environment and are not to be confused with Deep Security Event Tags. For more information on Deep Security Event Tagging, see [Event Tagging](#) in the User's Guide section of the online help.*

---

The **Anti-Malware** and **Intrusion Prevention System** protection modules can be configured to apply NSX Security Tags.

## Anti-Malware NSX Security tags

To configure the application of NSX Security Tags, go to **Computer/Policy Editor > Anti-Malware > Advanced > NSX Security Tagging**.

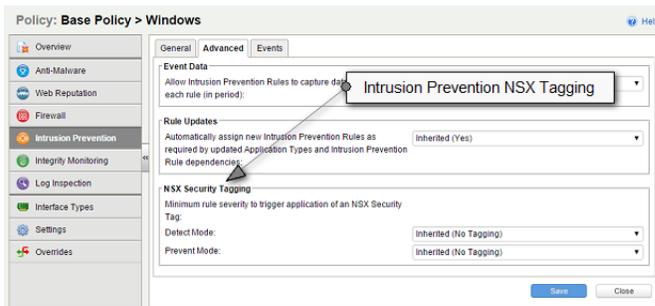


You can choose to only apply the NSX Security Tag if the remediation action attempted by the Anti-Malware engine fails. (The remediation action is determined by the Malware Scan Configuration that is in effect. To see which Malware Scan Configuration is in effect, go to the **Computer/Policy Editor > Anti-Malware > General** tab and check the **Real-Time Scan, Manual Scan, and Scheduled Scan** areas.)

You can also choose to have the Security Tag removed if a subsequent Malware Scan does not detect any malware. You should only use this setting if all Malware Scans will be of the same kind.

## Intrusion Prevention NSX Security Tags

To configure the application of NSX Security Tags, go to **Computer/Policy Editor > Intrusion Prevention > Advanced > NSX Security Tagging**.



Intrusion Prevention Events have a severity level that is determined by the severity level of the Intrusion Prevention Rule that caused it.

**Note:** The severity level of an Intrusion Prevention Rule is configurable on the **Rule Properties > General** tab.

Intrusion Prevention Rule severity levels map to NSX tags as follows:

IPS Rule Severity	NSX Security Tag
Critical	IDS_IPS.threat=high
High	IDS_IPS.threat=high
Medium	IDS_IPS.threat=medium
Low	IDS_IPS.threat=low

You can configure the sensitivity of the tagging mechanism by specifying the minimum Intrusion Prevention severity level that will cause an NSX security tag to be applied to a VM.

The options for the **Minimum rule severity to trigger application of an NSX Security Tag** setting are:

- **Default (No Tagging):** No NSX tag is applied.
- **Critical:** An NSX tag is applied to the VM if an Intrusion Prevention Rule with a severity level of **Critical** is triggered.
- **High:** An NSX tag is applied to the VM if an Intrusion Prevention Rule with a severity level of **High** or **Critical** is triggered.
- **Medium:** An NSX tag is applied to the VM if an Intrusion Prevention Rule with a severity level of **Medium**, **High**, or **Critical** is triggered.
- **Low:** An NSX tag is applied to the VM if an Intrusion Prevention Rule with a severity level of **Low**, **Medium**, **High**, or **Critical** is triggered.

Separate settings are provided for Rules that are operating in Prevent mode and for Rules that operating in Detect-only mode.

---

**Note:** *Whether an IPS Rule is operating in Prevent or Detect-only mode is determined not only by the Intrusion Prevention module setting (**Computer/Policy Editor > Intrusion Prevention > General tab**), but also by the configuration of the individual Rule itself (**Rule Properties > General tab > Details**).*

---

# Installing the Deep Security Notifier

The Deep Security Notifier is a utility for physical or virtual Windows machines which provides local notification when malware is detected or malicious URLs are blocked. The Deep Security Notifier is automatically installed as part of the Deep Security Agent on Windows machines. The stand-alone installation described here is intended for use on Agentless Windows VMs being protected by the Deep Security Virtual Appliance.

## Copy the Installation Package

Copy the installation file to the target machine.

## Installing the Deep Security Notifier for Windows

---

**Note:** Remember that you must have administrator privileges to install and run the Deep Security Notifier on Windows machines.

---

1. Double-click the installation file to run the installer package. Click **Next** to begin the installation.



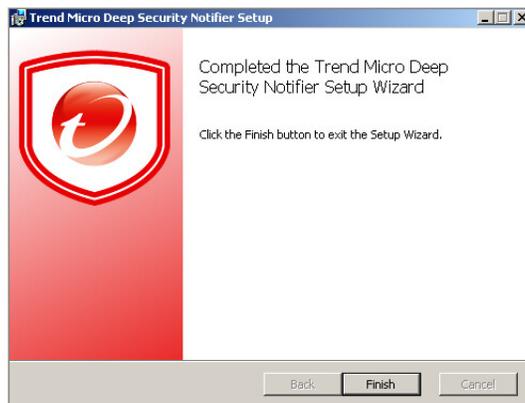
2. Read the license agreement and click **Next**.



3. Click **Install** to proceed with the installation.



4. Click **Finish** to complete the installation.



The Deep Security Notifier is now installed and running on this computer, and the Notifier icon appears in the Windows System Tray. The Notifier will automatically provide pop-up notifications when malware is detected or a URL has been blocked. (You can manually disable notifications by double-clicking the tray icon to open the Notifier status and configuration window).

---

**Note:** On VMs protected by a Virtual Appliance, the Anti-Malware module must be licensed and enabled on the VM for the Deep Security Notifier to display information.

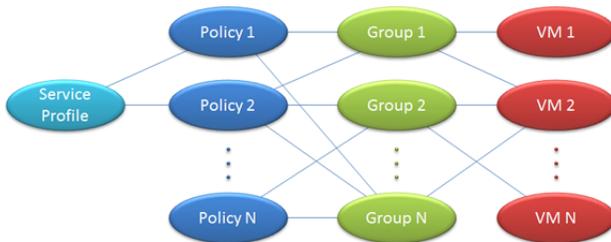
---

# Automated Policy Management in NSX Environments

**Note:** If you have enabled synchronization of Deep Security policies to NSX, you will not need to use the **NSX Security Group Change EBT**. For information on policy synchronization, see "Synchronize Deep Security Policies with NSX" in [Deploying Agentless Protection in an NSX Environment \(page 45\)](#).

The security configuration of a VM in an NSX environment can be automatically modified based changes to the VM's NSX Security Group. The automation of security configuration is done using the **NSX Security Group Change** Event-Based Task.

VMs are associated with NSX Security Groups, NSX Security Groups are associated with NSX Security Policies, and NSX Security Policies are associated with NSX Service Profiles.

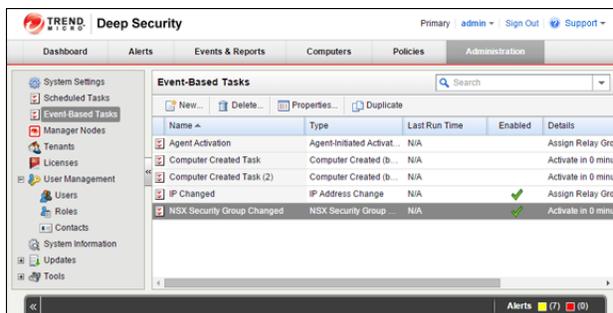


## "NSX Security Group Change" Event-Based Task

Deep Security has **Event-Based Tasks (EBTs)** that can be configured to perform actions when specific Events with specific conditions are detected. The **NSX Security Group Change** EBT exists to let you modify the protection settings of a VM if changes to the NSX Security Group that a VM belongs to are detected.

**Note:** The **NSX Security Group Change** EBT only detects changes to NSX Security Groups that are associated with the **Default (EBT)** NSX Service Profile. Similarly, a VM may be associated with many Groups/Policies, but Deep Security will only monitor and report changes that involve Groups/Policies associated with the **Default (EBT)** NSX Service Profile.

Event-Based Tasks are located in the Deep Security Manager on the Administration tab:



The **NSX Security Group Change** EBT is triggered when any of the following events occur:

- A VM is added to an NSX Group that is (indirectly) associated with the **Default (EBT)** NSX Service Profile.
- A VM is removed from an NSX Group that is associated with the **Default (EBT)** NSX Service Profile.
- An NSX Policy associated with the **Default (EBT)** NSX Service Profile is applied to an NSX Group.

- An NSX Policy associated with the **Default (EBT)** NSX Service Profile is removed from an NSX Group.
- An NSX Policy is associated with the **Default (EBT)** NSX Service Profile.
- An NSX Policy is removed from the **Default (EBT)** NSX Service Profile.
- An NSX Group that is associated with an **Default (EBT)** NSX Service Profile changes name.

An Event is triggered for each individual VM affected by a change.

## Conditions Under Which to Perform Tasks

The following conditions are applicable to the **NSX Security Group Change** Event-Based Task and can be tested against before performing an action:

- **Computer Name:** The hostname of the VM.
- **ESXi Name:** The Hostname of the ESXi the VM is a guest on.
- **Folder Name:** The name of the VM's folder in the ESXi folder structure.
- **NSX Security Group Name:** The name of the NSX Security Group that has undergone a change.
- **Platform:** the operating system of the VM.
- **vCenter name;** The name of the vCenter the VM is a part of.
- **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".
- **Last Used IP Address:** The current or last known IP address of the computer.

---

**Note:** For information on these conditions and Event-Based Tasks in general, see the online help for the **Administration > Event-Based Tasks** page.

---

The **NSX Security Group Name** condition is explicitly for changes to the **NSX Security Group Change** Event-Based Task.

It accepts a java regular expression match to the NSX Security Group the VM belongs to whose properties have changed. Two special cases are considered:

- A match for membership in any Group. In this case the recommended regular expression is "+".
- A match for membership in no Groups. In this case the recommended regular expression is "^\$".

Other regular expressions can include a specific Group name or partial name (to match more than one Group) as desired.

---

**Note:** The list of potential Groups in this condition refers only to Groups associated with Policies associated with the **Default (EBT)** NSX Service Profile.

---

## Actions Available

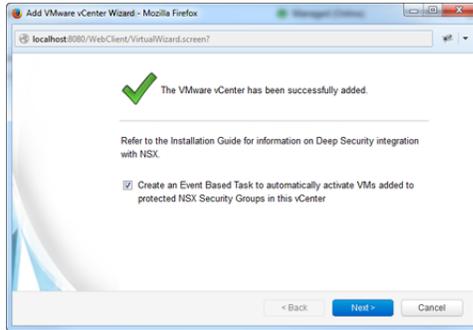
The following actions can be performed on a VM when Deep Security detects a change to the NSX Security Group the VM belongs to:

- **Activate Computer:** Activate Deep Security protection by the Deep Security Virtual Appliance. Use this when a VM is moved into a Deep Security-protected NSX Security Group.
- **Deactivate Computer:** Deactivate Deep Security protection by the Deep Security Virtual Appliance. Use this when moving a VM out of a Deep Security-protected NSX Security Group. An Alert will be raised if this action is not performed when a VM is moved out a NSX Security Group protected by Deep Security because the VM can no longer be protected.
- **Assign Policy:** Assign a Deep Security Policy to a VM.

- **Assign Relay Group:** Assign a Relay Group to a VM.

## Event-Based Tasks Created When Adding a vCenter to Deep Security Manager

Two Event Based Tasks can be created when adding an NSX vCenter to DSM. The last page of the **Add vCenter** wizard displays a checkbox:



If selected, this option creates two Event-Based Tasks. One to activate VMs when protection is added and the other to deactivate VMs when protection is removed.

The first Event-Based Task is configured as follows:

- **Name:** Activate <vCenter Name>, where <vCenter Name> is the value seen in the Name field on the vCenter properties.
- **Event:** NSX Security Group Changed
- **Task Enabled:** True
- **Action:** Activate Computer after a delay of five minutes
- **Conditions:**
  - **vCenterName:** <vCenter Name> Must match because the EBT is vCenter-specific.
  - **Appliance Protection Available:** True. Must have an activated DSVA deployed on the same ESXi.
  - **Appliance Protection Activated:** False. This only applies to unactivated VMs.
  - **NSX Security Group:** ".+ ". Must be a member of one or more Deep Security Groups.

You can modify the actions associated with this Event-Based Task, for example by applying a Deep Security protection Policy or assigning a different Relay Group. The actions (and other properties) of any existing Event-Based Tasks can be edited on the **Administration > Event-Based Tasks** page in the Deep Security Manager.

The second Event-Based Task is configured as follows:

- **Name:** Deactivate <vCenter Name>, where <vCenter Name> is the value seen in the Name field on the vCenter properties.
- **Event:** NSX Security Group Changed
- **Task Enabled:** False
- **Action:** Deactivate Computer
- **Conditions:**
  - **vCenterName:** <vCenter Name>. Must match because the Event-Based Task is vCenter-specific.
  - **Appliance Protection Activated:** True. This only applies to activated VMs.
  - **NSX Security Group:** "^\$". Must not be a member of any Deep Security Group.

---

**Note:** This Event-Based Task is disabled by default. You can enable it and customize it as desired after the vCenter installation is complete.

---

---

**Note:** *If multiple Event-Based Tasks are triggered by the same condition, the Tasks are executed in alphabetical order by Task name.*

---

## Removal of a vCenter from Deep Security Manager

Whenever a vCenter is removed from Deep Security Manager disables all Event-Based Tasks that meet the following criteria:

1. The **vCenter Name** condition matches the name of the vCenter being removed.

---

**Note:** *This must be an exact match. Event-Based Tasks which match multiple vCenter names will not be disabled.*

---

2. The Event-Based Task **Event Type** is "NSX Security Group Changed". Event-Based Tasks with other event types are not disabled.

# Upgrading

# Upgrading to Deep Security 9.6 SP1 in an NSX Environment

The steps for upgrading from Deep Security 9.5, 9.5 SP1, or 9.6 to Deep Security 9.6 SP1 in an NSX environment are:

1. Upgrade to Deep Security Manager 9.6 SP1.
2. Import version 9.6 SP1 of the Deep Security Virtual Appliance and Deep Security Agent.
3. Upgrade your Deep Security Relay-enabled Agent.
4. Upgrade your Deep Security Virtual Appliance.

For instructions on upgrading your vShield environment to NSX 6.1.5 or 6.2, please consult your VMware documentation.

## Upgrade to Deep Security Manager 9.6 SP1

---

**Note:** *Deep Security 9.6 included improvements to scalability and efficiency. Because of these changes, the upgrade from a pre-9.6 version to 9.6 SP1 can potentially take quite a long time (up to several hours depending on the size of your database). As usual, backup your database before upgrading and consider performing the upgrade during off-hours. To back up your 9.5 SP1 Deep Security data, see "Database Backup and Recovery" in the your Deep Security 9.5 SP1 online help or Administrator's Guide. Your Deep Security Agents and Appliances will continue to provide protection during the upgrade process.*

---

### To upgrade to Deep Security Manager 9.6 SP1:

1. Download the Deep Security Manager 9.6 SP1 install package from the Trend Micro Download Center web site (<http://downloadcenter.trendmicro.com/>) to a local directory.
2. Run the installer package as described in [Installing Deep Security Manager \(page 26\)](#), but choose **Upgrade** instead of **Change** when given the option.

When the Deep Security Manager installer detects an older version of Deep Security Manager on your system, it will give you the option to "upgrade the existing installation", or to "change the existing installation". Upgrading the installation will upgrade the Deep Security Manager to the latest version but will not overwrite your policies, IPS Rules, Firewall Rules, Application Types, etc. or change any of the security settings that were applied to the computers on your network. Changing the existing installation will erase all data associated with the previous installation and then install the new rules, policies, etc.

---

**Note:** *Do not delete any vCenters from the Deep Security Manager if you wish to continue providing the same protection as you did with version 9.5.*

---

## Import 9.6 SP1 versions of your Deep Security software

### To download 9.6 SP1 versions of your Deep Security software:

1. In Deep Security Manager, go to **Administration > Updates > Software > Download Center**. The **Download Center** page displays the latest versions all software available from Trend Micro.
2. To import the Deep Security Virtual Appliance software, select the latest version and click **Import**.

---

**Note:** *The latest version of the Virtual Appliance software will be 9.5. Once you import the 9.5 Virtual Appliance, Deep Security Manager will automatically import the latest 9.6 SP1 Red Hat 6 Agent package which it will use to upgrade the Virtual Appliance's Protection Module plug-ins to version 9.6 SP1.*

---

3. To import the Deep Security Agent software, select the latest version and click **Import**. You can use this software to upgrade a Deep Security Agent or a Relay-enabled Agent.

---

**Note:** 9.0 Deep Security Relays will be upgraded to Deep Security 9.6 SP1 Relay-enabled Agents.

---

- When the software has finished downloading, a green check mark will appear in the **Imported** column for that package.

## Upgrade to a version 9.6 SP1 Relay-enabled Agent

### Upgrade your 9.5 SP1 Relay-enabled Agent

---

**Note:** Deep Security Agents and Relays must be of the same version or less than the Deep Security Manager being used to manage it. The Deep Security Manager must always be upgraded before the Deep Security Agents and Relays.

---



---

**Note:** When planning the upgrade of your Agents and Relays to version 9.6 SP1, ensure that your 9.6 SP1 Agents are assigned to Relay Groups that contain only 9.6 SP1 Relays. You should upgrade all Relays in a Group to 9.6 SP1 (or create a new 9.6 SP1 Group) before configuring any 9.6 SP1 Agents to receive updates from the group.

---

#### To upgrade your 9.5 or 9.5 SP1 Relay-enabled Agent:

- In the Deep Security Manager, go to the **Computers** page.
- Find the computer on which you want to upgrade the Relay-enabled Agent.
- Right-click the Deep Security Relay and click **Actions > Upgrade Agent Software**.
- Follow the onscreen prompts.

---

**Note:** You can manually upgrade the Relays locally on a computer. To do this, follow the instructions in [Installing the Deep Security Agent \(page 33\)](#).

---

## Upgrade your 9.0 Deep Security Relay

Deep Security 9.0 *Windows* Relays can be upgraded to 9.6 SP1 Relay-enabled Agents using the Deep Security Manager console or by manual local upgrade. Deep Security 9.0 *Linux* Relays cannot be upgraded. They must be uninstalled and replaced with a fresh install of a 9.6 SP1 Linux Agent. (See "Upgrade a Relay on Linux", below, for instructions.)

#### To upgrade a Deep Security 9.0 Relay on Windows:

- In the Deep Security Manager, go to the **Computers** page.
- Right-click the Deep Security Relay and click **Actions > Upgrade**.
- Follow the onscreen prompts. The 9.0 Deep Security Relay will be upgraded to a 9.5 SP1 Relay-enabled Agent.

#### To upgrade a Deep Security 9.0 Relay on Linux:

- Upgrade Deep Security Manager to version 9.6 SP1.
- Import `Agent-platform-9.6.build.zip` into Deep Security Manager.
- Deactivate the Relay that you want to upgrade and then uninstall it.
- Install `Agent-Core-platform-9.6.build.rpm` on the Agent computer.
- Activate the Agent.
- After re-enabling the computer, enable the Relay.

#### To convert a 9.0 Relay to a 9.6 SP1 Agent on Linux:

- Upgrade Deep Security Manager to version 9.6 SP1.

2. Import `Agent-platform-9.6.build.zip` into Deep Security Manager.
3. Deactivate the Relay that you want to upgrade.
4. Delete the Relay from Deep Security Manager.
5. Uninstall the Relay.
6. Install `Agent-Core-platform-9.6.build.rpm` on the Agent computer.
7. In Deep Security Manager, add the computer (**Computers > New > New Computer**).

## Upgrade your Deep Security Virtual Appliance

Your Deep Security Virtual Appliance uses the 64-bit Red Hat Enterprise Linux 6 Agent as a resource for upgrades.

### To upgrade your Virtual Appliance:

1. In the Deep Security Manager, go to **Administration > Updates > Software > Download Center** and locate the latest build of the 64-bit Red Hat Enterprise Linux 6 Agent.
2. Select the Agent and click **Import** on the toolbar.
3. Once the Agent has been imported to Deep Security Manager, go to the **Computers** page and locate the Virtual Appliance.
4. Right-click the Virtual Appliance, select **Actions > Upgrade Appliance Software**, and follow the onscreen instructions until the upgrade is complete.

## Upgrade your NSX environment

If you want to upgrade your NSX environment at the same time as your Deep Security upgrade, follow these steps. Refer to your VMware documentation for details about how to perform the upgrade steps.

1. Perform all of the Deep Security upgrade steps.
2. Upgrade NSX Manager to 6.1.5 or 6.2.
3. Upgrade Endpoint Drivers for the Host.
4. Upgrade vCenter from 5.x to 6.0.
5. Upgrade the ESXi Host to 6.0.
6. Delete and re-install the Guest Introspection Service .
7. Delete and re-install the Trend Micro Deep Security Service.
8. Optionally, reboot the ESXi Host. This step is recommended to avoid potential errors after the VMs return to being online.

# Upgrading from a pre-9.6 vShield to a 9.6 SP1 NSX Environment

The steps for upgrading from Deep Security 9.0 or 9.5 SP1 in a vShield environment to Deep Security 9.6 SP1 in an NSX environment are:

1. Upgrade to Deep Security Manager 9.6 SP1.
2. Import version 9.6 SP1 of the Deep Security Virtual Appliance and Deep Security Agent.
3. Install or upgrade at least one Deep Security 9.6 SP1 Relay-enabled Agent.
4. Remove Deep Security from the vShield vCenter.
5. Upgrade the vCenter environment to NSX 6.1.5 or 6.2.
6. Re-deploy Deep Security 9.6 SP1 in the newly upgraded NSX environment. See [Deploying Agentless Protection in an NSX Environment \(page 45\)](#).

For instructions on upgrading your vShield environment to NSX 6.1.5 or 6.2, please consult your VMware documentation.

---

**Note:** *The upgrade process does not delete or overwrite any data but backing up your system before an upgrade is always a good idea. To back up your 9.5 Deep Security data, see "Database Backup and Recovery" in the your Deep Security 9.5 online help or Administrator's Guide.*

---

## Upgrade to Deep Security Manager 9.6 SP1

---

**Note:** *Deep Security 9.6 included improvements to scalability and efficiency. Because of these changes, the upgrade from pre-9.6 versions to 9.6 SP1 can potentially take quite a long time (up to several hours depending on the size of your database). As usual, backup your database before upgrading and consider performing the upgrade during off-hours. To back up your 9.5 SP1 Deep Security data, see "Database Backup and Recovery" in the your Deep Security 9.5 SP1 online help or Administrator's Guide. Your Deep Security Agents and Appliances will continue to provide protection during the upgrade process.*

---

### To upgrade to Deep Security Manager 9.6 SP1:

1. Download the Deep Security Manager 9.6 SP1 install package from the Trend Micro Download Center web site (<http://downloadcenter.trendmicro.com/>) to a local directory.
2. Run the installer package as described in [Installing Deep Security Manager \(page 26\)](#), but choose **Upgrade** instead of **Change** when given the option.

When the Deep Security Manager installer detects an older version of Deep Security Manager on your system, it will give you the option to "upgrade the existing installation", or to "change the existing installation". Upgrading the installation will upgrade the Deep Security Manager to the latest version but will not overwrite your policies, IPS Rules, Firewall Rules, Application Types, etc. or change any of the security settings that were applied to the computers on your network. Changing the existing installation will erase all data associated with the previous installation and then install the new rules, policies, etc.

---

**Note:** *Do not delete any vCenters from the Deep Security Manager if you wish to continue providing the same protection as you did with version 9.5.*

---

## Import 9.6 SP1 versions of your Deep Security software

### To download 9.6 SP1 versions of your Deep Security software:

1. In Deep Security Manager, go to **Administration > Updates > Software > Download Center**. The **Download Center** page displays the latest versions all software available from Trend Micro.
2. To import the Deep Security Virtual Appliance software, select the latest version and click **Import**.

---

**Note:** The latest version of the Virtual Appliance software will be 9.5. Once you import the 9.5 Virtual Appliance, Deep Security Manager will automatically import the latest 9.6 SP1 Red Hat 6 Agent package which it will use to upgrade the Virtual Appliance's Protection Module plug-ins to version 9.6 SP1.

---

3. To import the Deep Security Agent software, select the latest version and click **Import**. You can use this software to upgrade a Deep Security Agent or a Relay-enabled Agent.

---

**Note:** 9.0 Deep Security Relays will be upgraded to Deep Security 9.6 SP1 Relay-enabled Agents.

---

4. When the software has finished downloading, a green check mark will appear in the **Imported** column for that package.

## Upgrade to a version 9.6 SP1 Relay-enabled Agent

### Upgrade your 9.5 or 9.5 SP1 Relay-enabled Agent

---

**Note:** Deep Security Agents and Relays must be of the same version or less than the Deep Security Manager being used to manage it. The Deep Security Manager must always be upgraded before the Deep Security Agents and Relays.

---



---

**Note:** When planning the upgrade of your Agents and Relays from 9.0 or 9.5 SP1 to version 9.6 SP1, ensure that your 9.6 SP1 Agents are assigned to Relay Groups that contain only 9.6 SP1 Relays. You should upgrade all Relays in a Group to 9.6 SP1 (or create a new 9.6 SP1 Group) before configuring any 9.6 SP1 Agents to receive updates from the group.

---

#### To upgrade your 9.5 or 9.5 SP1 Relay-enabled Agent:

1. In the Deep Security Manager, go to the **Computers** page.
2. Find the computer on which you want to upgrade the Relay-enabled Agent.
3. Right-click the Deep Security Relay and click **Actions > Upgrade Agent Software**.
4. Follow the onscreen prompts.

---

**Note:** You can manually upgrade the Relays locally on a computer. To do this, follow the instructions in [Installing the Deep Security Agent \(page 33\)](#).

---

## Upgrade your 9.0 Deep Security Relay

Deep Security 9.0 *Windows* Relays can be upgraded to 9.6 SP1 Relay-enabled Agents using the Deep Security Manager console or by manual local upgrade. Deep Security 9.0 *Linux* Relays cannot be upgraded. They must be uninstalled and replaced with a fresh install of a 9.6 SP1 Linux Agent. (See "Upgrade a Relay on Linux", below, for instructions.)

#### To upgrade a Deep Security 9.0 Relay on Windows:

1. In the Deep Security Manager, go to the **Computers** page.
2. Right-click the Deep Security Relay and click **Actions > Upgrade**.
3. Follow the onscreen prompts. The 9.0 Deep Security Relay will be upgraded to a 9.5 SP1 Relay-enabled Agent.

#### To upgrade a Deep Security 9.0 Relay on Linux:

1. Upgrade Deep Security Manager to version 9.6 SP1.
2. Import `Agent-platform-9.6.build.zip` into Deep Security Manager.
3. Deactivate the Relay that you want to upgrade and then uninstall it.
4. Install `Agent-Core-platform-9.6.build.rpm` on the Agent computer.

5. Activate the Agent.
6. After re-enabling the computer, enable the Relay.

**To convert a 9.0 Relay to a 9.6 SP1 Agent on Linux:**

1. Upgrade Deep Security Manager to version 9.6 SP1.
2. Import `Agent-platform-9.6.build.zip` into Deep Security Manager.
3. Deactivate the Relay that you want to upgrade.
4. Delete the Relay from Deep Security Manager.
5. Uninstall the Relay.
6. Install `Agent-Core-platform-9.6.build.rpm` on the Agent computer.
7. In Deep Security Manager, add the computer (**Computers > New > New Computer**).

## Remove Deep Security 9.5 from the vShield vCenter

1. **Deactivate the guest VMs:** In the Deep Security Manager, go to the Computers page and select the protected guest virtual machines (only the VMs, not the Virtual Appliance(s)) in the vCenter you are going to upgrade to NSX 6.1.5 or 6.2. Right-click the selected VMs and select **Actions > Deactivate**.
2. **Deactivate the Virtual Appliance(s):** Still on the **Computers** page, select the Virtual Appliances in the vCenter you are going to upgrade, right-click and select **Actions > Deactivate**.
3. **Delete the Deep Security Virtual Appliance from the vCenter environment:** *In the VMware vSphere Web Client, go to to **Home > vCenter > Hosts and Clusters** and find and delete the deactivated Deep Security Virtual Appliances.*
4. **Uninstall vShield Endpoint:**
  1. *In the VMware vSphere Web Client, go to to **Home > vCenter > Hosts and Clusters***
  2. Select the ESXi host from the inventory tree.
  3. Click the **vShield** tab
  4. Click **Uninstall** for the vShield Endpoint service
5. **Remove the Filter Driver:** *In the Deep Security Manager, select each ESXi host in the vCenter you are going to upgrade, right-click and select **Actions > Remove Filter Driver**.*

---

**Note:** *Do not delete the vCenter from Deep Security Manager if you intend to protect the same vCenter with Deep Security after the upgrade to Deep Security 9.6 SP1 and NSX 6.1.5 or 6.2.*

---

## Upgrade your vShield Manager to the new NSX Manager

Please consult your VMware documentation for vCenter upgrade instructions.

## Remove the old vShield Manager from Deep Security and add the new NSX Manager

1. In the Deep Security Manager, go to the **Computers** screen and right-click the vCenter and select **Properties** to display its **Properties** window.
2. On the vShield Manager tab, in the vShield Manager area, click **Remove Manager**. This will remove the vShield Manager credentials (and retile the **vShield Manager** tab to **vShield/NSX Manager**.)
3. On the **vShield/NSX Manager** tab, enter the credentials of the newly upgraded NSX Manager.
4. Click **OK** to close the Properties window.

## Upgrade Your Deep Security Agents

---

**Note:** *Deep Security Agents must be of the same version or less than the Deep Security Manager being used to manage them. The Deep Security Manager must always be upgraded before the Deep Security Agents.*

---

**Note:** *When planning the upgrade of your Agents and Relays to version 9.6 SP1, ensure that your 9.6 SP1 Agents are assigned to Relay Groups that contain only 9.6 SP1 Relays. You should upgrade all Relays in a Group to 9.6 SP1 (or create a new 9.6 SP1 Group) before configuring any 9.6 SP1 Agents to receive updates from the group.*

---

### To upgrade Deep Security Agents using the Deep Security Manager:

1. In the Deep Security Manager, go to the **Computers** screen.
2. Find the computer on which you want to upgrade the Agent .
3. Right-click the computer and select **Actions > Upgrade Agent software**.
4. The new Agent software will be sent to the computer and the Agent will be upgraded.

---

**Note:** *You can also manually upgrade Agents locally on a computer. To do this, follow the instructions in [Installing the Deep Security Agent \(page 33\)](#).*

---

# Appendices

# Silent Install of Deep Security Manager

## To run a silent install of the Deep Security Manager:

1. In a Windows command prompt or Linux command line, go to the same directory as the install package.
2. If you are installing on Linux, grant execution permission to the install package.
3. Run the appropriate command for your platform:

### On Windows:

```
Manager-Windows-<Version>.x64.exe [-q] [-console] [-Dinstall4j.language=<ISO code>] [-varfile <PropertiesFile>]
```

### On Linux:

```
Manager-Linux-<Version>.x64.sh [-q] [-console] [-Dinstall4j.language=<ISO code>] [-varfile <PropertiesFile>]
```

See the "Parameters" section, below, for details on each of the command parameters.

## Parameters

**-q** forces install4j to execute in unattended (silent) mode.

**-console** forces messages to appear in the console (stdout).

**-Dinstall4j.language=<ISO code>** lets you override the default installation language (English) if other languages are available. Specify a language using standard ISO language identifiers:

- Japanese: **ja**
- Simplified Chinese: **zh\_CN**

**-varfile <PropertiesFile>**, where **<PropertiesFile>** is the full path to standard Java properties file with entries for the various settings you can apply during a Deep Security Manager install. Each property is identified by its equivalent GUI screen and setting in the Windows Deep Security Manager installation. For example, the Deep Security Manager address on the "Address and Ports" screen is specified as:

```
AddressAndPortsScreen.ManagerAddress=
```

Most of the properties in this file have acceptable defaults and may be omitted.

For a complete description of available settings, see [Deep Security Manager Settings Properties File \(page 75\)](#).

## Sample Properties File

This is an example of the content of a typical properties file:

```
AddressAndPortsScreen.ManagerAddress=10.201.111.91
AddressAndPortsScreen.NewNode=True
UpgradeVerificationScreen.Overwrite=False
LicenseScreen.License.-1=XY-ABCD-ABCDE-ABCDE-ABCDE-ABCDE-ABCDE
DatabaseScreen.DatabaseType=Oracle
DatabaseScreen.Hostname=10.201.xxx.xxx
DatabaseScreen.Transport=TCP
DatabaseScreen.DatabaseName=XE
```

```
DatabaseScreen.Username=DSM
DatabaseScreen.Password=xxxxxxx
AddressAndPortsScreen.ManagerPort=4119
AddressAndPortsScreen.HeartbeatPort=4120
CredentialsScreen.Administrator.Username=masteradmin
CredentialsScreen.Administrator.Password=xxxxxxx
CredentialsScreen.UseStrongPasswords=False
SecurityUpdateScreen.UpdateComponents=True
SoftwareUpdateScreen.Proxy=False
SoftwareUpdateScreen.ProxyType=""
SoftwareUpdateScreen.ProxyAddress=""
SoftwareUpdateScreen.ProxyPort=""
SoftwareUpdateScreen.ProxyAuthentication="False"
SoftwareUpdateScreen.ProxyUsername=""
SoftwareUpdateScreen.ProxyPassword=""
SoftwareUpdateScreen.UpdateSoftware=True
RelayScreen.Install=True
SmartProtectionNetworkScreen.EnableFeedback=False
```

# Deep Security Manager Settings Properties File

This section contains information about the contents of the properties file that can be used in a command-line installation (silent install) of the Deep Security Manager. (See [Silent Install of Deep Security Manager \(page 73\)](#).)

## Settings Properties File

The format of each entry in the settings properties file is:

```
<Screen Name>.<Property Name>=<Property Value>
```

The settings properties file has required and optional values.

---

**Note:** For optional entries, supplying an invalid value will result in the default value being used.

---

## Required Settings

### LicenseScreen

Property	Possible Values	Default Value
LicenseScreen.License.-1=<value>	<AC for all modules>	blank

OR

Property	Possible Values	Default Value
LicenseScreen.License.0=<value>	<AC for Anti-Malware>	blank
LicenseScreen.License.1=<value>	<AC for Firewall/DPI>	blank
LicenseScreen.License.2=<value>	<AC for Integrity Monitoring>	blank
LicenseScreen.License.3=<value>	<AC for Log Inspection>	blank

### CredentialsScreen

Property	Possible Values	Default Value
CredentialsScreen.Administrator.Username=<value>	<username for master administrator>	blank
CredentialsScreen.Administrator.Password=<value>	<password for the master administrator>	blank

## Optional Settings

### LanguageScreen

Property	Possible Values	Default Value	Notes
sys.languageId=<value>	en_US ja zh_CN	en_US	"en_US" = English, "ja" = Japanese, "zh_CN" = Simplified Chinese

## UpgradeVerificationScreen

**Note:** This screen/setting is not referenced unless an existing installation is detected.

Property	Possible Values	Default Value
UpgradeVerificationScreen.Overwrite=<value>	True False	False

**Note:** Setting this value to True will overwrite any existing data in the database. It will do this without any further prompts.

## DatabaseScreen

This screen defines the database type and optionally the parameters needed to access certain database types.

**Note:** The interactive install provides an "Advanced" dialog to define the instance name and domain of a Microsoft SQL server, but because the unattended install does not support dialogs these arguments are included in the DatabaseScreen settings below.

Property	Possible Values	Default Value	Notes
DatabaseScreen.DatabaseType=<value>	Embedded Microsoft SQL Server Oracle	Embedded	None
DatabaseScreen.Hostname=<value>	The name or IP address of the database server Current host name	Current host name	None
DatabaseScreen.DatabaseName=<value>	Any string	dsm	Not required for Embedded
DatabaseScreen.Transport=<value>	Named Pipes TCP	Named Pipes	Required for SQL Server only
DatabaseScreen.Username=<value>	Any string	blank	Username used by the Manager to authenticate to the database server. Must match an existing database account. Note that the Deep Security Manager database permissions will correspond to this user's permissions. For example, if you choose a database account with read-only privileges, the Deep Security Manager will not be able to write to the database. Not required for Embedded. Mandatory for Microsoft SQL Server and Oracle.
DatabaseScreen.Password=<value>	Any string	blank	Password used by the Manager to authenticate to the database server. Not required for Embedded. Mandatory for Microsoft SQL Server and Oracle.
DatabaseScreen.SQLServer.Instance=<value>	Any string	blank	Used only with Microsoft SQL Server, which supports multiple instances on a single server or processor. Only one instance can be the default instance and any others are named instances. If the Deep Security Manager database instance is not the default, enter the name of the instance here. The value must match an existing instance or be left blank to indicate the default instance.
DatabaseScreen.SQLServer.Domain=<value>	Any string	blank	Used only with Microsoft SQL Server. This is the Windows domain used when authenticating to the SQL Server. The DatabaseScreen.Username and DatabaseScreen.Password described above are only valid within the appropriate domain.
DatabaseScreen.SQLServer.UseDefaultCollation=<value>	True False	False	Used only with Microsoft SQL Server. Collation determines how strings are sorted and compared. If the value is "False", Deep Security will use Latin1_General_CS_AS for collation on text-type columns. If the value is "True", Deep Security will use the

Property	Possible Values	Default Value	Notes
			collation method specified by your SQL Server database. For additional information on collation, refer to your SQL Server documentation.

## AddressAndPortsScreen

This screen defines the hostname, URL, or IP address of this computer and defines ports for the Manager. In the interactive installer this screen also supports the addition of a new Manager to an existing database, but this option is not supported in the unattended install.

Property	Possible Values	Default Value	Notes
AddressAndPortsScreen.ManagerAddress=<value>	<hostname, URL or IP address of the Manager host>	<current host name>	None
AddressAndPortsScreen.ManagerPort=<value>	<valid port number>	4119	None
AddressAndPortsScreen.HeartbeatPort=<value>	<valid port number>	4120	None
AddressAndPortsScreen.NewNode=<value>	True False	False	True indicates that the current install is a new node. If the installer finds existing data in the database, it will add this installation as a new node. (Multi-node setup is always a silent install). Note: The "New Node" installation information about the existing database to be provided via the DatabaseScreen properties.

## CredentialsScreen

Property	Possible Values	Default Value	Notes
CredentialsScreen.UseStrongPasswords=<value>	True False	False	True indicates the DSM should be set up to enforce strong passwords

## SecurityUpdateScreen

Property	Possible Values	Default Value	Notes
SecurityUpdateScreen.UpdateComponents=<value>	True False	True	True will instruct the Deep Security Manager to create a Scheduled Task to automatically check for Security Updates. The Scheduled Task will run when installation is complete.
SecurityUpdateScreen.Proxy=<value>	True False	False	True indicates that the Deep Security Manager uses a proxy to connect to the Internet to download Security Updates from Trend Micro.
SecurityUpdateScreen.ProxyType=<value>	HTTP SOCKS4 SOCKS5	blank	The protocol used by the proxy.
SecurityUpdateScreen.ProxyAddress=<value>	valid IPv4 or IPv6 address or hostname	blank	The IP or hostname of the proxy.
SecurityUpdateScreen.ProxyPort=<value>	integer	blank	The port number of the proxy.
SecurityUpdateScreen.ProxyAuthentication=<value>	True False	False	True indicates that the proxy requires authentication credentials.
SecurityUpdateScreen.ProxyUsername=<value>	any string	blank	The authentication username.
SecurityUpdateScreen.ProxyPassword=<value>	any string	blank	The authentication password.

## SoftwareUpdateScreen

Property	Possible Values	Default Value	Notes
SoftwareUpdateScreen.UpdateSoftware=<value>	True False	True	True will instruct the Deep Security Manager to create a Scheduled Task to automatically check for Software Updates. The Scheduled Task will run when installation is complete.
SoftwareUpdateScreen.Proxy=<value>	True False	False	True indicates that the Deep Security Manager uses a proxy to connect to the Internet to download Software Updates from Trend Micro.
SoftwareUpdateScreen.ProxyType=<value>	HTTP SOCKS4 SOCKS5	blank	The protocol used by the proxy.
SoftwareUpdateScreen.ProxyAddress=<value>	valid IPv4 or IPv6 address or hostname	blank	The IP or hostname of the proxy.
SoftwareUpdateScreen.ProxyPort=<value>	integer	blank	The port number of the proxy.
SoftwareUpdateScreen.ProxyAuthentication=<value>	True False	False	True indicates that the proxy requires authentication credentials.
SoftwareUpdateScreen.ProxyUsername=<value>	any string	blank	The authentication username.
SoftwareUpdateScreen.ProxyPassword=<value>	any string	blank	The authentication password.

## SmartProtectionNetworkScreen

This screen defines whether you want to enable Trend Micro Smart Feedback and optionally your industry.

Property	Possible Values	Default Value	Notes
SmartProtectionNetworkScreen.EnableFeedback=<value>	True False	False	True enables Trend Micro Smart Feedback.
SmartProtectionNetworkScreen.IndustryType=<value>	Not specified Banking Communications and media Education Energy Fast-moving consumer goods (FMCG) Financial Food and beverage Government Healthcare Insurance Manufacturing Materials Media Oil and gas Real estate Retail Technology Telecommunications Transportation Utilities Other	blank	blank corresponds to Not specified

## Sample Properties Files

The following is an example of the content of a typical properties file:

```
AddressAndPortsScreen.ManagerAddress=10.201.111.91
AddressAndPortsScreen.NewNode=True
UpgradeVerificationScreen.Overwrite=False
LicenseScreen.License.-1=XY-ABCD-ABCDE-ABCDE-ABCDE-ABCDE
DatabaseScreen.DatabaseType=Oracle
DatabaseScreen.Hostname=10.201.xxx.xxx
DatabaseScreen.Transport=TCP
DatabaseScreen.DatabaseName=XE
DatabaseScreen.Username=DSM
DatabaseScreen.Password=xxxxxxx
AddressAndPortsScreen.ManagerPort=4119
AddressAndPortsScreen.HeartbeatPort=4120
CredentialsScreen.Administrator.Username=masteradmin
CredentialsScreen.Administrator.Password=xxxxxxx
CredentialsScreen.UseStrongPasswords=False
SecurityUpdateScreen.UpdateComponents=True
SoftwareUpdateScreen.UpdateSoftware=True
RelayScreen.Install=True
SmartProtectionNetworkScreen.EnableFeedback=False
```

## Installation Output

The following is a sample output from a successful install, followed by an example output from a failed install (invalid license). The [Error] tag in the trace indicates a failure.

### Successful Install

```
Stopping Trend Micro Deep Security Manager Service...
Checking for previous versions of Trend Micro Deep Security Manager...
Upgrade Verification Screen settings accepted...
The installation directory has been set to C:\Program Files\Trend Micro\Deep Security Manager.
Database Screen settings accepted...
License Screen settings accepted...
Address And Ports Screen settings accepted...
Credentials Screen settings accepted...
Security Update Screen settings accepted...
Software Update Screen settings accepted...
Smart Protection Network Screen settings accepted...
All settings accepted, ready to execute...
Extracting files ...
Setting Up...
Connecting to the Database...
Creating the Database Schema...
Creating MasterAdmin Account...
Recording Settings...
Creating Temporary Directory...
Installing Reports...
Installing Modules and Plug-ins...
Creating Help System...
Validating and Applying Activation Codes...
Configure Localizable Settings...
Setting Default Password Policy...
Creating Scheduled Tasks...
Creating Asset Importance Entries...
Creating Auditor Role...
Optimizing...
Importing Software Packages...
Configuring Relay For Install...
```

```
Importing Performance Profiles...
Recording Installation...
Clearing Sessions...
Creating Properties File...
Creating Shortcut...
Configuring SSL...
Configuring Service...
Configuring Java Security...
Configuring Java Logging...
Cleaning Up...
Starting Deep Security Manager...
Finishing installation ...
```

## Failed Install

This example shows the output generated when the properties file contained an invalid license string:

```
Stopping Trend Micro Deep Security Manager Service...
Detecting previous versions of Trend Micro Deep Security Manager..
Upgrade Verification Screen settings accepted...
Database Screen settings accepted...
Database Options Screen settings accepted...
[ERROR] The license code you have entered is invalid.
[ERROR] License Screen settings rejected...
Rolling back changes...
```

# Deep Security Manager Memory Usage

## Configuring the Installer's Maximum Memory Usage

The installer is configured to use 1GB of contiguous memory by default. If the installer fails to run you can try configuring the installer to use less memory.

### To configure the amount of RAM available to the installer:

1. Go to the directory where the installer is located.
2. Create a new text file called "Manager-Windows-9.6.xxxx.x64.vmoptions" or "Manager-Linux-9.6.xxxx.x64.vmoptions", depending on your installation platform (where "xxx" is the build number of the installer).
3. Edit the file by adding the line: "-Xmx800m" (in this example, 800MB of memory will be made available to the installer.)
4. Save the file and launch the installer.

## Configuring the Deep Security Manager's Maximum Memory Usage

The Deep Security Manager default setting for heap memory usage is 4GB. It is possible to change this setting.

### To configure the amount of RAM available to the Deep Security Manager:

1. Go to the Deep Security Manager install directory (the same directory as Deep Security Manager executable).
2. Create a new file. Depending on the platform, give it the following name:
  - **Windows:** "Deep Security Manager.vmoptions".
  - **Linux:** "dsm\_s.vmoptions".
3. Edit the file by adding the line: "**-Xmx10g** " (in this example, "10g" will make 10GB memory available to the Deep Security Manager.)
4. Save the file and restart the Deep Security Manager.
5. You can verify the new setting by going to **Administration > System Information** and in the System Details area, expand **Manager Node > Memory**. The Maximum Memory value should now indicate the new configuration setting.

# Deep Security Virtual Appliance Memory Usage

For information on minimum recommended Deep Security Virtual Appliance memory allocation based on the number of VMs being protected, see the Deep Security 9.6 SP1 Best Practice Guide:

[http://docs.trendmicro.com/all/ent/ds/v9.6\\_sp1/en-us/Deep\\_Security\\_96\\_SP1\\_Best\\_Practice\\_Guide.pdf](http://docs.trendmicro.com/all/ent/ds/v9.6_sp1/en-us/Deep_Security_96_SP1_Best_Practice_Guide.pdf)

The default configuration of the DSVA is to use 4GB of RAM. If you expect to need more than the default 4GB, you will need to modify the DSVA's configuration yourself. There are two options:

- Modify the configuration of the Virtual Appliance prior to being imported to Deep Security Manager and then to the vCenter, thereby setting the default configuration for all subsequent Deep Security Virtual Appliance service deployments in that vCenter.
- Modify the memory allocation of the Virtual Appliance on a cases by case basis after it has been imported to the vCenter and deployed as a service on a ESXi.

## Configuring the DSVA's Memory Allocation (pre-deployment)

To change the Deep Security Virtual Appliance's default memory allocation, you must edit the allocation settings in the Appliance's OVF file before it gets imported to the vCenter.

**To configure the memory allocation of a Deep Security Virtual Appliance prior to deployment to the vCenter:**

1. Unzip the Virtual Appliance zip file you downloaded from the Trend Micro Download Center.
2. Open **dsva.ovf** in a text editor.
3. Edit the following section to modify the default memory allocation of 4096 MB to suit your environment ("4096" occurs in three locations):
 

```
<Item>
<rasd:AllocationUnits>byte * 2^20</rasd:AllocationUnits>
<rasd:Description>Memory Size</rasd:Description>
<rasd:ElementName          xmlns:rasd="http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/
CIM_ResourceAllocationSettingData">4096 MB of memory</rasd:ElementName>
<rasd:InstanceID          xmlns:rasd="http://schemas.dmtf.org/wbem/wscim/1/cim-schema/2/
CIM_ResourceAllocationSettingData">2</rasd:InstanceID>
<rasd:Reservation>4096</rasd:Reservation>
<rasd:ResourceType>4</rasd:ResourceType>
<rasd:VirtualQuantity>4096</rasd:VirtualQuantity>
</Item>
```
4. Save the ovf file and return it to the zip package.
5. Import the Virtual Appliance zip package to the Deep Security Manager from the **Administration > Updates Software > Local** page.

## Configuring the DSVA's Memory Allocation (post-deployment)

---

**Note:** *Changing the Deep Security Virtual Appliance's memory allocation settings requires powering off the DSVA virtual machine. Virtual machines normally protected by the Virtual Appliance will be unprotected until it is powered back on.*

---

**To configure the memory allocation of an already deployed Deep Security Virtual Appliance:**

1. In your VMware vSphere Web Client, right-click on the DSVA and select **Power > Shut Down Guest**.
2. Right-click on the DSVA again and select **Edit Settings...** The Virtual Machine **Properties** screen displays.
3. On the **Hardware** tab, select **Memory** and change the memory allocation to the desired value.
4. Click **OK**.
5. Right-click the DSVA again and select **Power > Power On**.

# Deep Security Manager Performance Features

## Performance Profiles

Deep Security Manager uses an optimized concurrent job scheduler that considers the impacts of each job on CPU, Database and Agent/Appliances. By default, new installations use the "Aggressive" performance profile which is optimized for a dedicated Manager. If the Deep Security Manager is installed on a system with other resource-intensive software it may be preferable to use the "Standard" performance profile. The performance profile can be changed by navigating to **Administration > Manager Nodes**. From this screen select a Manager node and open the **Properties** window. From here the Performance Profile can be changed via the drop-down menu.

The Performance Profile also controls the number of Agent/Appliance-initiated connections that the Manager will accept. The default of each of the performance profiles effectively balances the amount of accepted, delayed and rejected heartbeats.

## Low Disk Space Alerts

### Low Disk Space on the Database Host

If the Deep Security Manager receives a "disk full" error message from the database, it will start to write events to its own hard drive and will send an email message to all Users informing them of the situation. This behavior is not configurable.

If you are running multiple Manager nodes, the Events will be written to whichever node is handling the Event. (For more information on running multiple nodes, see Multi-Node Manager in the Reference section of the online help or the Administrator's Guide.)

Once the disk space issue on the database has been resolved, the Manager will write the locally stored data to the database.

### Low Disk Space on the Manager Host

If the available disk space on the Manager falls below 10%, the Manager generates a Low Disk Space Alert. This Alert is part of the normal Alert system and is configurable like any other. (For more information on Alerts, see **Alert Configuration** in the **Configuration and Management** section of the online help or the Administrator's Guide.)

If you are running multiple Manager nodes, the node will be identified in the Alert.

When the Manager's available disk space falls below 5MB, the Manager will send an email message to all Users and the Manager will shut down. The Manager cannot be restarted until the available disk space is greater than 5MB.

You must restart the Manager manually.

If you are running multiple nodes, only the node that has run out of disk space will shut down. The other Manager nodes will continue operating.

# Creating an SSL Authentication Certificate

The Deep Security Manager creates a 10-year self-signed certificate for the connections with Agents/Appliances, Relays, and Users' web browsers. However, for added security, this certificate can be replaced with a certificate from a trusted certificate authority (CA). (Such certificates are maintained after a Deep Security Manager upgrade.)

Once generated, the CA certificate must be imported into the .keystore in the root of the Deep Security Manager installation directory and have an alias of "tomcat". The Deep Security Manager will then use that certificate.

## Windows

### To create your SSL authentication certificate in a Windows environment:

1. Go to the Deep Security Manager installation directory (for the purpose of these instructions, we will assume it's "**C:\Program Files\Trend Micro\Deep Security Manager**") and create a new folder called **Backupkeystore**.
2. Copy **.keystore** and **configuration.properties** to the newly created folder **Backupkeystore**.
3. From a command prompt, go to the following location: **C:\Program Files\Trend Micro\Deep Security Manager\jre\bin**.
4. Run the following command, which will create a self-signed certificate:

```
C:\Program Files\Trend Micro\Deep Security Manager\jre\bin>keytool -genkey -alias tomcat -keyalg RSA -dname cn=dmsserver
```

---

**Note:** *NOTE: -dname is the common name of the certificate your CA will sign. Some CAs require a specific name to sign the Certificate Signing Request (CSR). Please consult your CA Admin to see if you have that particular requirement.*

---

5. When prompted, enter a password.
6. There is a new keystore file created under the user home directory. If you are logged in as "Administrator", You will see the **.keystore** file under **C:\Documents and Settings\Administrator**.
7. View the newly generated certificate using the following command:

```
C:\Program Files\Trend Micro\Deep Security Manager\jre\bin>keytool -list -v
```

8. Run the following command to create a CSR for your CA to sign:

```
C:\Program Files\Trend Micro\Deep Security Manager\jre\bin>keytool -certreq -keyalg RSA -alias tomcat -file certrequest.csr
```

9. Send the **certrequest.csr** to your CA to sign. In return you will get two files. One is a "certificate reply" (for example, **certresponse.txt**) and the second is the CA certificate itself (for example, **ca.cert.crt** or **certnew.cer**).
10. Copy the files to **C:\Program Files\Trend Micro\Deep Security Manager\jre\bin\**.
11. Run the following command to import the CA cert in JAVA trusted keystore:

```
C:\Program Files\Trend Micro\Deep Security Manager\jre\bin>keytool -import -alias root -trustcacerts -file cacert.crt -keystore "C:\Program Files\Trend Micro\Deep Security Manager\jre\lib\security\cacerts"
```

12. Run the following command to import the CA certificate in your keystore:

```
C:\Program Files\Trend Micro\Deep Security Manager\jre\bin>keytool -import -alias root -trustcacerts -file cacert.crt
```

(say yes to warning message)

- Run the following command to import the certificate reply to your keystore:

```
C:\Program Files\Trend Micro\Deep Security Manager\jre\bin>keytool -import -alias tomcat -
file certreply.txt
```

- Run the following command to view the certificate chain in you keystore:

```
C:\Program Files\Trend Micro\Deep Security Manager\jre\bin>keytool -list -v
```

- Copy the .keystore file from your user home directory **C:\Documents and Settings\Administrator** to **C:\Program Files\ Trend Micro \Deep Security Manager\**
- Open the configuration.properties file in folder **C:\Program Files\Trend Micro\Deep Security Manager**. It will look something like:

```
keystoreFile=C:\\\\Program Files\\\\Trend Micro\\\\Deep Security Manager\\\\.keystore
port=4119
keystorePass=$1$85ef650a5c40bb0f914993ac1ad855f48216fd0664ed2544bbec6de80160b2f
installed=true
serviceName= Trend Micro Deep Security Manager
```

- Replace the password in the following string:

```
keystorePass=xxxx
```

where "xxxx" is the password you supplied in step five

- Save and close the file.
- Restart the Deep Security Manager service.
- Connect to the Deep Security Manager with your browser and you will notice that the new SSL certificate is signed by your CA.

## Linux

### To create your SSL authentication certificate in a Linux environment:

- Go to the Deep Security Manager installation directory (for the purpose of these instructions, we will assume it's "**opt\dsm**") and create a new folder called **Backupkeystore**.
- Copy **.keystore** and **configuration.properties** to the newly created folder **Backupkeystore**.
- From a command prompt, go to the following location: **opt\dsm\jre\bin**.
- Run the following command, which will create a self-signed certificate:

```
opt/dsm/jre/bin# keytool -genkey -alias tomcat -keyalg RSA -dname cn=dmsserver
```

---

**Note:** *NOTE: -dname is the common name of the certificate your CA will sign. Some CAs require a specific name to sign the Certificate Signing Request (CSR). Please consult your CA Admin to see if you have that particular requirement.*

---

- When prompted, enter a password.
- There is a new **.keystore** file created under the user home directory. If you are logged in as "Administrator", You will see the **.keystore** file under **./root/**

If the file is hidden, use the following command: **find -type f -iname ".keystore" -ls**

7. View the newly generated certificate using the following command:

```
opt/dsm/jre/bin# keytool -list -v
```

8. Run the following command to create a CSR for your CA to sign:

```
opt/dsm/jre/bin# keytool -certreq -keyalg RSA -alias tomcat -file certrequest.csr
```

If you see "**Keytool unrecognized option '-keyalg'**", use '**-sigalg'** instead.

9. Send the **certrequest.csr** to your CA to sign. In return you will get two files. One is a "certificate reply" and the second is the CA certificate itself.
10. Run the following command to import the CA cert into the Java trusted keystore:

```
/opt/dsm/jre/bin/keytool -import -alias root -trustcacerts -file cacert.crt -keystore "/opt/dsm/jre/lib/security/cacerts
```

11. Run the following command to import the CA certificate in your keystore:

```
/opt/dsm/jre/bin/keytool -import -alias root -trustcacerts -file cacert.crt
```

(say yes to warning message)

12. Run the following command to import the certificate reply to your keystore:

```
/opt/dsm/jre/bin/keytool -import -alias tomcat -file certreply.txt
```

13. Run the following command to view the certificate chain in you keystore:

```
opt/dsm/jre/bin# keytool -list -v
```

14. Copy the .keystore file from your home directory to **/opt/dsm/**

```
cp $HOME/.keystore /opt/dsm/.keystore
```

15. Open the **opt/dsm/configuration.properties** file. It will look something like:

```
keystoreFile= opt/dsm/.keystore  
port=443  
keystorePass=xxxx  
installed=true  
serviceName= Trend Micro Deep Security Manager
```

16. Replace the password in the following string:

```
keystorePass=xxxx
```

where "**xxxx**" is the password you supplied in step five

17. Save and close the file.
18. Restart the Deep Security Manager service.
19. Connect to the Deep Security Manager with your browser and you will notice that the new TLS certificate is signed by your CA.

# Minimum VMware Privileges for DSVa Deployment (NSX)

**Account for NSX:** admin

**Account for vCenter:** Administrator of vCenter or a member of vCenter Administrators

# Installing a vSphere Distributed Switch

To use Deep Security in a VMware NSX virtual network environment, your vCenter Server must be using a vSphere Distributed Switch (vDS).

**To install a vDS on your datacenter:**

1. Open your vSphere Web Client and navigate to your datacenter in your networking inventory.
2. Right-click on the datacenter and select **New vSphere Distributed Switch** to display the **New Distributed Switch** wizard.
3. **Select Version:** Select **Distributed Switch Version: 5.5** or later.
4. **General Properties:** Give the distributed switch a name and select the number of uplink ports. Click **Next**.
5. **Add Hosts and Physical Adapters:** Select **Add now** and select one or more physical adapters. Click **Next**.
6. **Ready to complete:** Select **Automatically create a default port group**, confirm your settings, and click **Finish**.

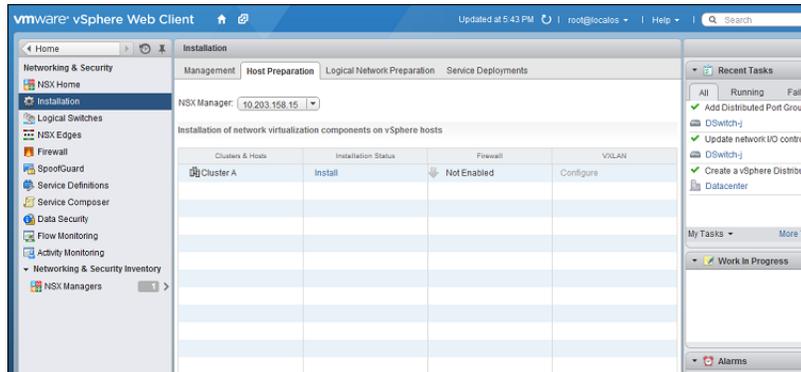
Your vSphere Distributed Switch is now installed.

# Preparing ESXi servers

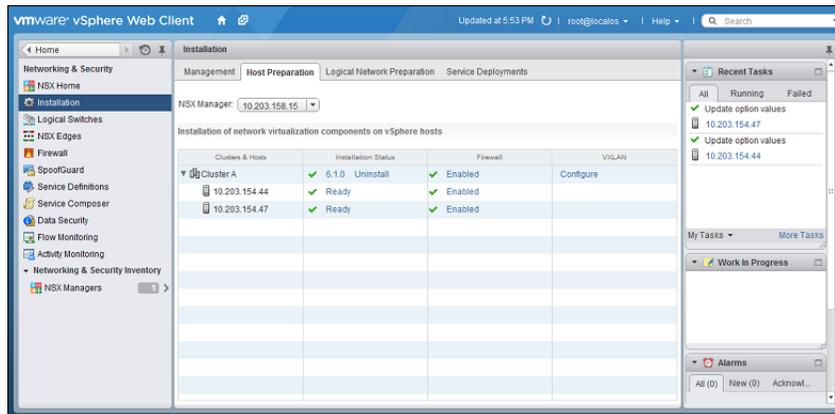
Before the Deep Security Virtual Appliance service can be deployed to your datacenter, your ESXi servers must first be prepared by installing the drivers necessary for network traffic inspection. This operation is performed on the cluster.

## To prepare your cluster:

1. In your vSphere Web Client, go to **Home > Networking & Security > Installation** and click on the **Host Preparation** tab:



2. Locate the NSX cluster you are going to protect with Deep Security in the **Clusters & Hosts** list and click **Install** in the **Installation Status** column. The installation will complete and the driver version will be displayed in the **Installation Status** column:



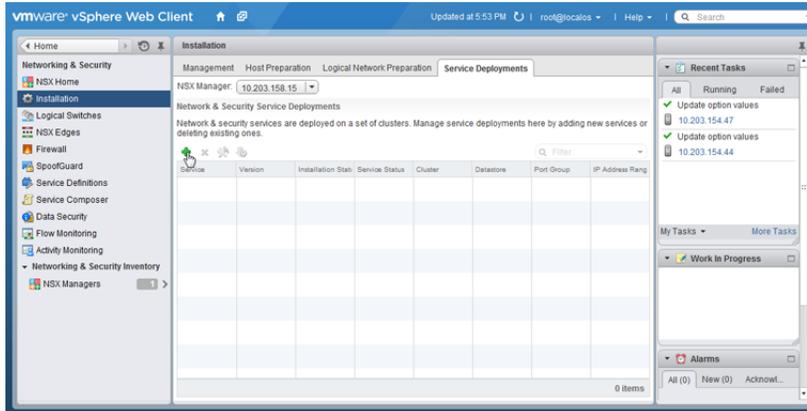
Host preparation is now complete. For more complete instructions on host preparation please consult your VMware documentation.

# Installing the Guest Introspection Service

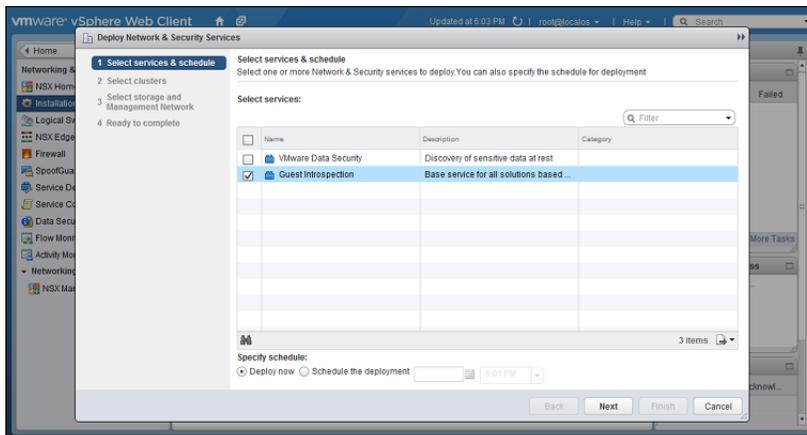
To protect your VMs with Deep Security, you must install the Guest Introspection service on the cluster that contains your ESXi servers.

To install the Guest Introspection service:

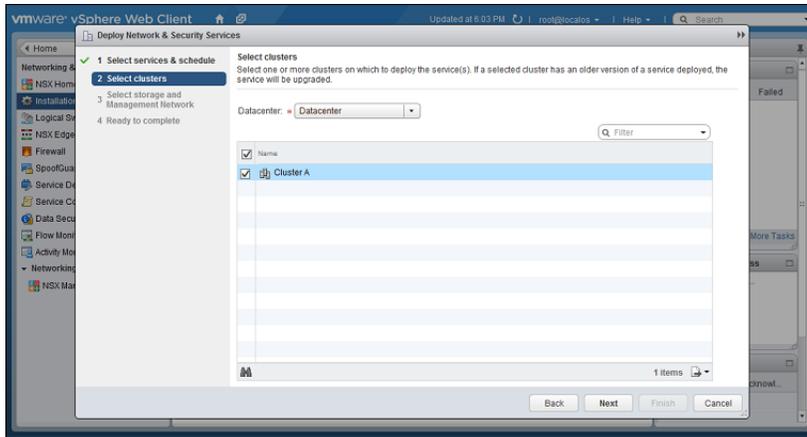
1. In your vSphere Web Client, go to the **Service Deployments** tab on the **Home > Networking & Security > Installation** page and click on the green plus sign (+) to display the **Deploy Network & Security Services** window.



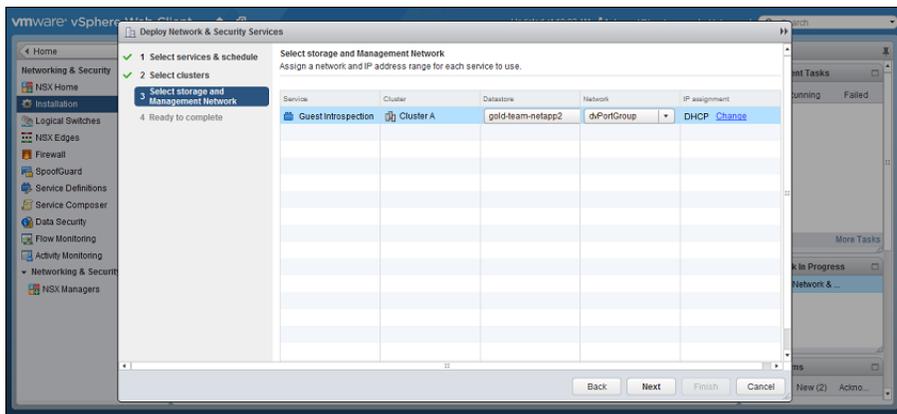
2. **Select services & schedule:** Select **Guest Introspection**:



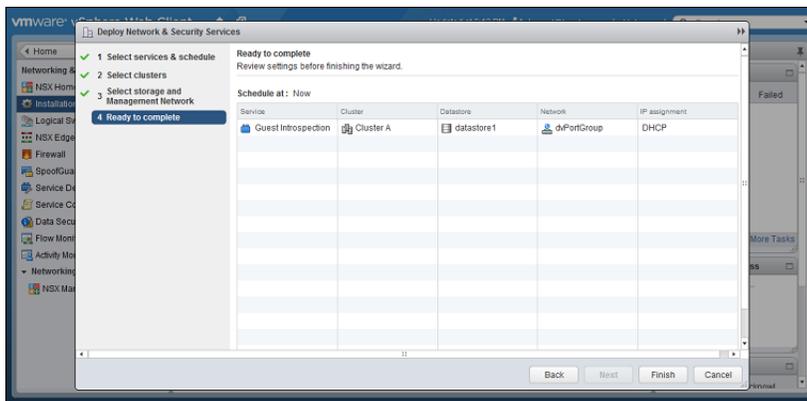
3. **Select Clusters:** Select the cluster that contains the ESXi servers and VMs that you want to protect:



4. **Select storage and Management Network:** Select the datastore, the distributed port group used by your NSX cluster, and IP assignment method:



5. **Ready to complete:** Review your settings and click **Finish**:



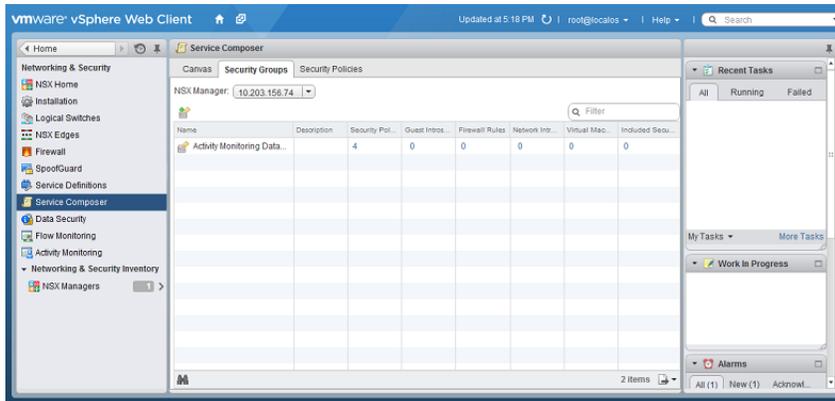
It may take some time for the Guest Introspection Service to install. When it is finished, the **Installation Status** will display as "Succeeded". You may need to refresh the vSphere Web Client (  ) to update the status.

# Creating NSX Security Groups

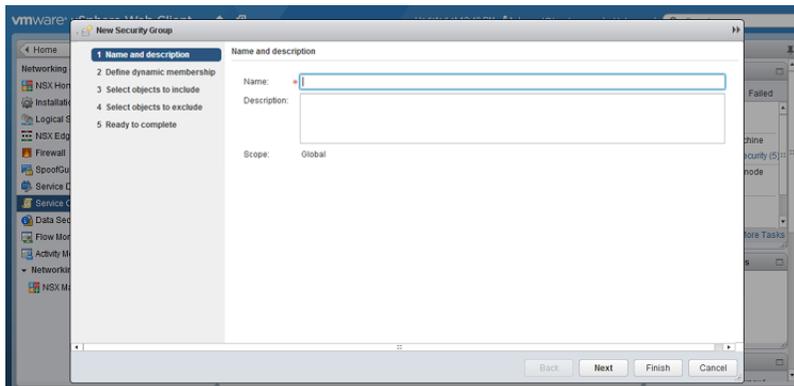
Your VM resources must be organized into a NSX Security Group before a vSphere Security Policy can be assigned to them.

## To create a new NSX Security Group:

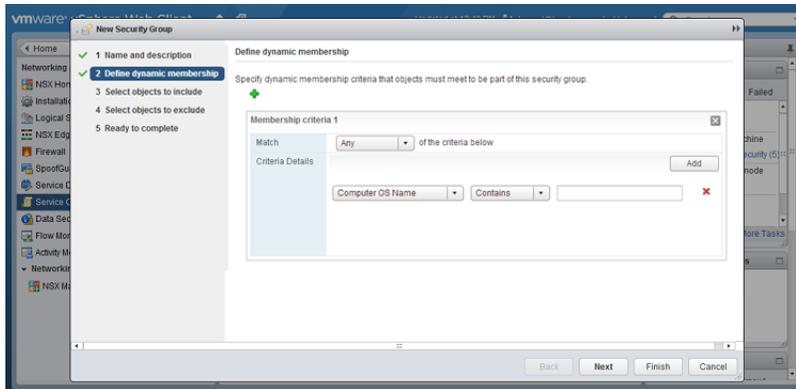
1. In your vSphere Web Client, go to the **Security Groups** tab on the **Home > Networking & Security > Service Composer** page and click on the **New Security Group** icon (  ):



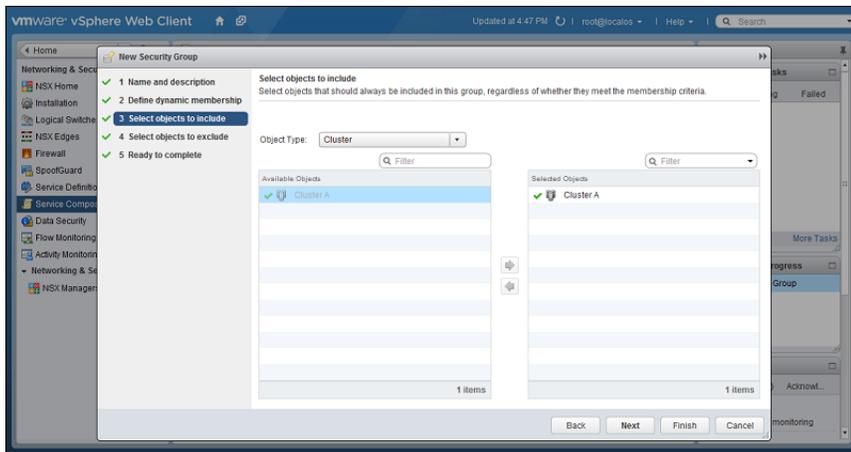
2. In the **Name and description** options, give a name to your Security Group.



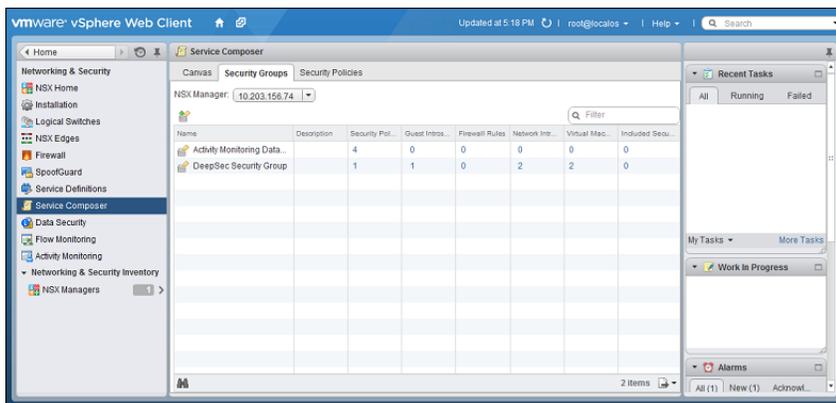
3. **Define Dynamic Membership:** If you wish to restrict membership in this group based on certain filtering criteria, enter those criteria here.



- There are many ways to include or exclude objects in a NSX Security Group, but for this example, we will simply include the NSX cluster that contains the hosts and VMs that we want to protect. In the **Select objects to include** options, select **Cluster** from the **Object Type** menu, and move the NSX Cluster that contains the VMs to protect to the **Selected Objects** column.



- Click **Finish** to create the new Security Group and return to the **Security Groups** tab to see the newly listed Security Group:



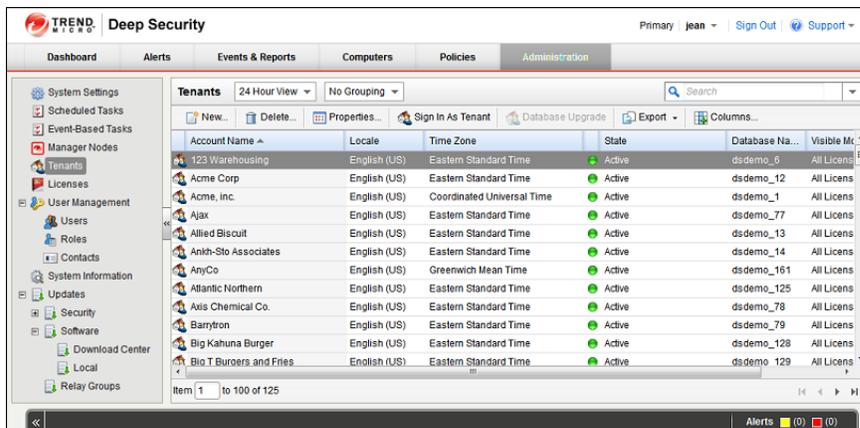
# Enable Multi-Tenancy

## To enable Multi-Tenancy:

1. In the Deep Security Manager, go to **Administration > System Settings > Advanced** and click **Enable Multi-Tenant Mode** in the **Multi-Tenant Options** area to display the **Multi-Tenant Configuration** wizard.
2. Enter the Activation Code and click **Next**.
3. Choose a license mode to implement:
  - **Inherit Licensing from Primary Tenant:** Gives all Tenants the same licenses as the Primary Tenant.
  - **Per Tenant Licensing:** In this mode, Tenants themselves enter a license when they sign in for the first time.
4. Click **Next** to finish enabling Multi-Tenancy in your Deep Security Manager.

## Managing Tenants

Once Multi-Tenant mode is enabled, Tenants can be managed from the **Tenants** page that now appears in the **Administration** section.



The screenshot shows the 'Tenants' page in the Deep Security Manager. The page has a navigation menu on the left with options like System Settings, Scheduled Tasks, Event-Based Tasks, Manager Nodes, Tenants, Licenses, User Management, Users, Roles, Contacts, System Information, Updates, Security, Software, Download Center, Local, and Relay Groups. The main content area displays a table of tenants with columns for Account Name, Locale, Time Zone, State, Database Name, and Visible Licenses. The table lists 12 tenants, all with 'Active' status and 'All Licenses' visible. The bottom of the page shows 'Alerts' with 0 yellow and 0 red indicators.

Account Name	Locale	Time Zone	State	Database Na...	Visible M...
123 Warehousing	English (US)	Eastern Standard Time	Active	dsdemo_6	All Licenses
Acme Corp	English (US)	Eastern Standard Time	Active	dsdemo_12	All Licenses
Acme, Inc.	English (US)	Coordinated Universal Time	Active	dsdemo_1	All Licenses
Ajax	English (US)	Eastern Standard Time	Active	dsdemo_77	All Licenses
Allied Biscuit	English (US)	Eastern Standard Time	Active	dsdemo_13	All Licenses
Ankh-Sto Associates	English (US)	Eastern Standard Time	Active	dsdemo_14	All Licenses
AnyCo	English (US)	Greenwich Mean Time	Active	dsdemo_161	All Licenses
Atlantic Northern	English (US)	Eastern Standard Time	Active	dsdemo_125	All Licenses
Avis Chemical Co.	English (US)	Eastern Standard Time	Active	dsdemo_78	All Licenses
Barrytron	English (US)	Eastern Standard Time	Active	dsdemo_79	All Licenses
Big Kahuna Burger	English (US)	Eastern Standard Time	Active	dsdemo_128	All Licenses
Bio T Burners and Fries	English (US)	Eastern Standard Time	Active	dsdemo_129	All Licenses

## Creating Tenants

### To create a new Tenant:

1. Go to the **Administration > Tenants** page and click **New** to display the **New Tenant** wizard.
2. Enter a Tenant Account Name. The account name can be any name except "Primary" which is reserved for the Primary Tenant.
3. Enter an Email Address. The email address is required in order to have a contact point per Tenant. It is also used for two of the three different user account generation methods in the next step.
4. Select the Locale. The Locale determines the language of the Deep Security Manager user interface for that Tenant.
5. Select a Time Zone. All Tenant-related Events will be shown to the Tenant Users in the time zone of the Tenant account.
6. If your Deep Security installation is using more than one database, you will have the option to let Deep Security automatically select a database server on which to store the new Tenant account ("Automatic -- No Preference") or you can specify a particular server.

**Note:** Database servers that are no longer accepting new Tenants will not be included in the drop-down list. The options will not appear if you only have a single database.

When you have made your selection, click **Next** to continue.

7. Enter a Username for the first User of the new Tenant account.
8. Select one of the three password options:
  - **No Email:** The Tenancy's first User's username and password are defined here and no emails are sent.
  - **Email Confirmation Link:** You set the Tenancy's first User's password. However the account is not active until the User clicks a confirmation link he will receive by email.
  - **Email Generated Password:** This allows the Tenant creator to generate a Tenant without specifying the password. This is most applicable when manually creating accounts for users where the creator does not need access

---

**Note:** *All three options are available via the REST API. The confirmation option provides a suitable method for developing public registration. A CAPTCHA is recommended to ensure that the Tenant creator is a human not an automated "bot". The email confirmation ensures that the email provided belongs to the user before they can access the account.*

---

9. Click **Next** to finish with the wizard and create the Tenant. (It may take from 30 seconds to four minutes to create the new Tenant database and populate it with data and sample Policies.)

## Examples of messages sent to Tenants

### Email Confirmation Link: Account Confirmation Request

Welcome to Deep Security! To begin using your account, click the following confirmation URL. You can then access the console using your chosen password.

Account Name: AnyCo  
Username: admin

Click the following URL to activate your account:  
<https://managename:4119/SignIn.screen?confirmation=1A16EC7A-D84F-D451-05F6-706095B6F646&tenantAccount=AnyCo&username=admin>

### Email Generated Password: Account and Username Notification

Welcome to Deep Security! A new account has been created for you. Your password will be generated and provided in a separate email.

Account Name: AnyCo  
Username: admin

You can access the Deep Security management console using the following URL:  
<https://managename:4119/SignIn.screen?tenantAccount=AnyCo&username=admin>

### Email Generated Password: Password Notification

This is the automatically generated password for your Deep Security account. Your Account Name, Username, and a link to access the Deep Security management console will follow in a separate email.

Password: z3IgrUQ0jaFi

## Managing Tenants

The **Tenants** page (**Administration > Tenants**) displays the list of all Tenants. A Tenant can be in any of the following **States**:

Tenants				
Account Name	Database Na...	Locale	State	Time Zone
AnyCo	dsmfuji_1	English (US)	Active	America/New_York
BetaCo	dsmfuji_2	English (US)	Pending deletion	America/New_York
CoMoTo	dsmfuji_3	Japanese	Active	Asia/Tokyo
DeltaCo	dsmfuji_4	English (US)	Confirmation Required	America/New_York
EvaMicro	dsmfuji_5	English (US)	Active	America/New_York
FireCo	dsmfuji_6	English (US)	Suspended	America/New_York

- **Created:** In the progress of being created but not yet active
- **Confirmation Required:** Created, but the activation link in the confirmation email sent to the Tenant User has not yet been clicked. (You can manually override this state.)
- **Active:** Fully online and managed
- **Suspended:** No longer accepting sign ins.
- **Pending Deletion:** Tenants can be deleted, however the process is not immediate. The Tenant can be in the pending deletion state for up to seven days before the database is removed.
- **Database Upgrade Failure:** For Tenants that failed the upgrade path. The Database Upgrade button can be used to resolve this situation

## Tenant Properties

Double-click on a Tenant to view the Tenant's **Properties** window.

### General

General Information

Account Name: 123 Warehousing

Description:

Locale: English (US)

Time Zone: (UTC-11:00) Niue Time

State: Active

Database Server: [Oracle ip3e4puk.cyp3e4puk1g.zonaws.com:DE](#)

Database Name: dsdemo\_6

Manager Node: ec2-23-20-13.compute-1.amazonaws.com

**NOTE** The manager node indicates which node is responsible for background jobs. Any tenant can use any manager node for the User Interface and Agent Heartbeats

Options

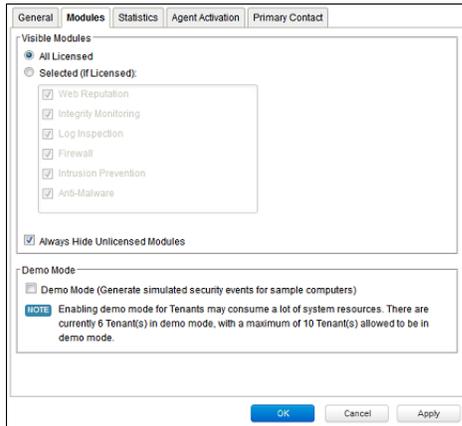
Sign In As Tenant Perform Database Upgrade

OK Cancel Apply

The Locale, Time zone and State of the Tenant can be altered. Be aware that changing the time zone and locale does not affect existing Tenant Users. It will only affect new Users in that Tenancy and Events and other parts of the UI that are not User-specific.

The Database Name indicates the name of the database used by this Tenancy. The server the database is running on can be accessed via the hyperlink.

## Modules



The **Modules** tab provides options for protection module visibility. By default all unlicensed modules are hidden. You can change this by deselecting **Always Hide Unlicensed Modules**. Alternatively, selected modules can be shown on a per-Tenant basis.

If you select **Inherit License from Primary Tenant**, all features that you as the Primary Tenant are licensed for will be visible to all Tenants. The selected visibility can be used to tune which modules are visible for which Tenants.

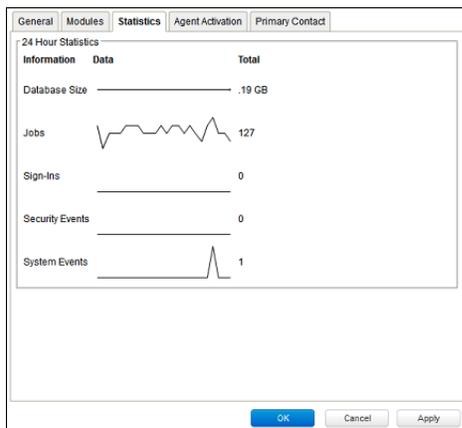
If using the "Per Tenant" licensing by default only the licensed modules for each Tenant will be visible.

If you are evaluating Deep Security in a test environment and want to see what a full Multi-Tenancy installation looks like, you can enable Multi-Tenancy Demo Mode.

When in Demo Mode, the Manager populates its database with simulated Tenants, computers, Events, Alerts, and other data. Initially, seven days worth of data is generated but new data is generated on an ongoing basis to keep the Manager's Dashboard, Reports and Events pages populated with data.

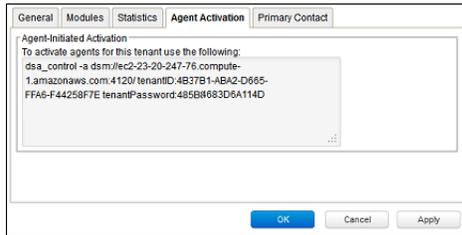
*Demo Mode is **not** intended to be used in a production environment!*

## Statistics



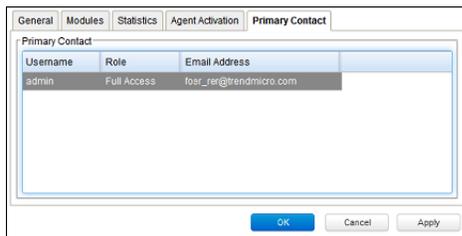
The statistics tab shows information for the current Tenant including database size, jobs processed, logins, security events and system events. The small graphs show the last 24 hours of activity.

## Agent Activation



The Agent Activation tab displays a command-line instruction, that can be run from the Agent install directory of this Tenant's computers which will activate the agent on the computer so that the Tenant can assign Policies and perform other configuration procedures from the Deep Security Manager.

## Primary Contact



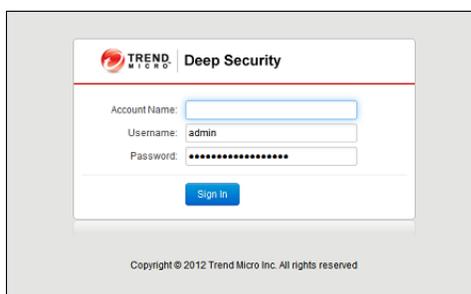
## Relay-enabled Agents

Each Deep Security Manager must have access to at least one Relay-enabled Agent, and this includes the Tenants in a Multi-Tenancy Deep Security installation. By default, the Relay-enabled Agents in the primary Tenant's "Default Relay Group" are available to the other Tenants. The setting is found in the primary Tenant's Deep Security Manager in the **Administration > System Settings > Tenants > Multi-Tenant Options** area. If this option is disabled, Tenants will have to install and manage their own Relay-enabled Agent.

## The Tenant Account User's View of Deep Security

### The Tenant "User experience"

When Multi-tenancy is enabled, the sign-in page has an additional **Account Name** text field:



Tenants are required to enter their account name in addition to their username and password. The account name allows Tenants to have overlapping usernames. (For example, if multiple Tenants synchronize with the same Active Directory server).

---

**Note:** When you (as the Primary Tenant) log in, leave the Account name blank or use "Primary".

---

When Tenants log in, they have a very similar environment to a fresh install of Deep Security Manager. Some features in the UI are not available to Tenant Users. The following areas are hidden for Tenants:

- Manager Nodes Widget
- Multi-Tenant Widgets
- Administration > System Information
- Administration > Licenses (If Inherit option selected)
- Administration > Manager Nodes
- Administration > Tenants
- Administration > System Settings:
  - Tenant Tab
  - Security Tab > Sign In Message
  - Updates Tab > Setting for Allowing Tenants to use Relay-enabled Agents from the Primary Tenant
  - Advanced Tab > Load Balancers
  - Advanced Tab > Pluggable
- Some of the help content not applicable to Tenants
- Some reports not applicable to Tenants
- Other features based on the Multi-Tenant settings you choose on the **Administration > System Settings > Tenants** tab
- Some Alert Types will also be hidden from Tenants:
  - Heartbeat Server Failed
  - Low Disk Space
  - Manager Offline
  - Manager Time Out Of Sync
  - Newer Version of Deep Security Manager available
  - Number of Computers Exceeds Database Limit
  - And when inherited licensing is enabled any of the license-related alerts

It is also important to note that Tenants cannot see any of the Multi-Tenant features of the primary Tenant or any data from any other Tenant. In addition, certain APIs are restricted since they are only usable with Primary Tenant rights (such as creating other Tenants).

For more information on what is and is not available to Tenant Users, see the online help for the **Administration > System Settings > Tenants** page in the Deep Security Manager.

All Tenants have the ability to use Role-Based Access Control with multiple user accounts to further sub-divide access. Additionally they can use Active Directory integration for users to delegate the authentication to the domain. The Tenant Account Name is still required for any Tenant authentications.

## Agent-Initiated Activation

Agent-initiated activation is enabled by default for all Tenants.

---

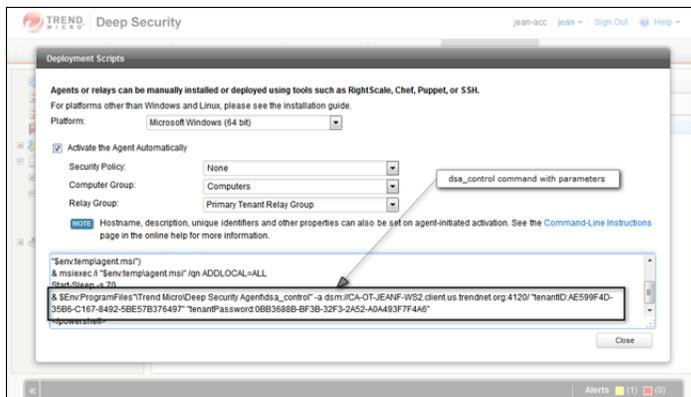
**Note:** Unlike Agent-initiated activation for the Primary Tenant, a password and Tenant ID are required to invoke the activation for Tenant Users.

---

Tenants can see the arguments required for agent-initiated activation by going to **Administration > Updates > Software > Local Software**, selecting an Agent install package, and selecting **Generate Deployment Scripts** from the toolbar:



This will display the deployment script generator. If Tenants select their platform from the **Platform** menu and the select **Activate Agent Automatically**, the generated deployment script will include the **dsa\_control** with the required parameters.



As an example, the script for Agent-Initiated Activation on a Windows machine might look as follows:

```
dsa_control -a dsm://manageraddress:4120/ "tenantID:7155A-D130-29F4-5FE1-8AFD102"
"tenantPassword:98785384-3966-B9-1418-3E7D0D5"
```

## Tenant Diagnostics

Tenants are not able to access manager diagnostic packages due to the sensitivity of the data contained within the packages. Tenants can still generate agent diagnostics by opening the Computer Editor and choosing **Agent Diagnostics** on the **Actions** tab of the **Overview** page.

## Usage Monitoring

Deep Security Manager records data about Tenant usage. This information is displayed in the **Tenant Protection Activity** widget on the Dashboard, the Tenant **Properties** window's **Statistics** tab, and the Chargeback report. This information can also be accessed through the Status Monitoring REST API which can be enabled or disabled by going to **Administration > System Settings > Advanced > Status Monitoring API**.

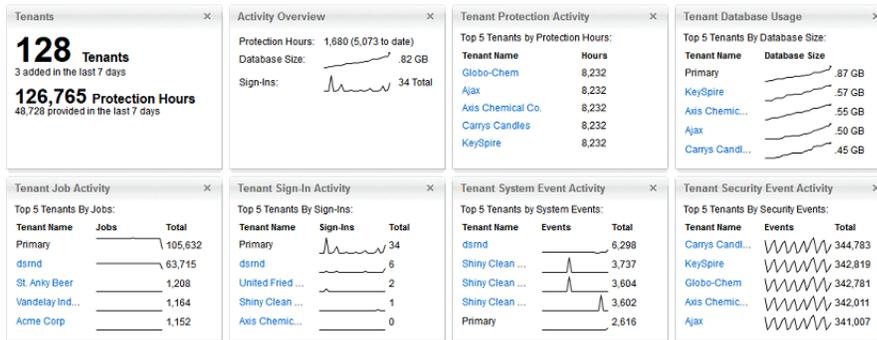
This chargeback (or viewback) information can be customized to determine what attributes are included in the record. This configuration is designed to accommodate various charging models that may be required in service provider environments. For enterprises this may be useful to determine the usage by each business unit.

## Multi-Tenant Dashboard/Reporting

When Multi-Tenancy is enabled, Primary Tenant Users have access to additional Dashboard widgets for monitoring Tenant activity:



Some examples of Tenant-related widgets:



The same information is available on the **Administration > Tenants** page (some in optional columns) and on the **Statistics** tab of a Tenant's **Properties** window.

This information provides the ability to monitor the usage of the overall system and look for indicators of abnormal activity. For instance if a single Tenant experiences a spike in **Security Event Activity** they may be under attack.

More information is available in the **Tenant Report** (in the **Events & Reports** section). This report details protection hours, the current database sizes, and the number of computers (activated and non-activated) for each Tenant.

# Multi-Tenancy (Advanced)

## APIs

Deep Security Manager includes a number of REST APIs for:

1. Enabling Multi-Tenancy
2. Managing Tenants
3. Accessing Monitoring Data
4. Accessing Chargeback (Protection Activity) Data
5. Managing Secondary Database Servers

In addition the legacy SOAP API includes a new **authenticate** method that accepts the Tenant Account Name as a third parameter.

For additional information on the REST APIs please see the REST API documentation.

## Upgrade

Upgrade is unchanged from previous versions. The installer is executed and detects an existing installation. It will offer an upgrade option. If upgrade is selected the installer first informs other nodes to shutdown and then begins the process of upgrading.

The primary Tenant is upgraded first, followed by the Tenants in parallel (five at a time). Once the installer finishes, the same installer package should be executed on the rest of the Manager nodes.

In the event of a problem during the upgrade of a Tenant, the Tenant's State (on the **Administration > Tenants** page) will appear as **Database Upgrade Required (offline)**. The Tenants interface can be used to force the upgrade process. If forcing the upgrade does not work please contact support.

## Supporting Tenants

In certain cases it may be required a Primary Tenant to gain access to a Tenant's user interface. The Tenants list and Tenant properties pages provide an option to "Authenticate As" a given Tenant, granting them immediate read-only access.

Users are logged in as a special account on the Tenant using the prefix "support\_". For example if Primary Tenant user jdoe logs on as a Tenant an account is created called "support\_jdoe" with the "Full Access" role. The user is deleted when the support user times out or signs out of the account.

The Tenant can see this user account created, sign in, sign out and deleted along with any other actions in the System events.

Users in the primary Tenant also have additional diagnostic tools available to them:

1. The **Administration > System Information** page contains additional information about Tenant memory usage and the state of threads. This may be used directly or helpful to Trend Micro support.
2. The `server0.log` on the disk of the Manager nodes contains additional information on the name of the Tenant (and the user if applicable) that caused the log. This can be helpful in determining the source of issues.

In some cases Tenants will require custom adjustments not available in the GUI. This usually comes at the request of Trend Micro support. The command line utility to alter these settings accepts the argument:

```
-Tenantname "account name"
```

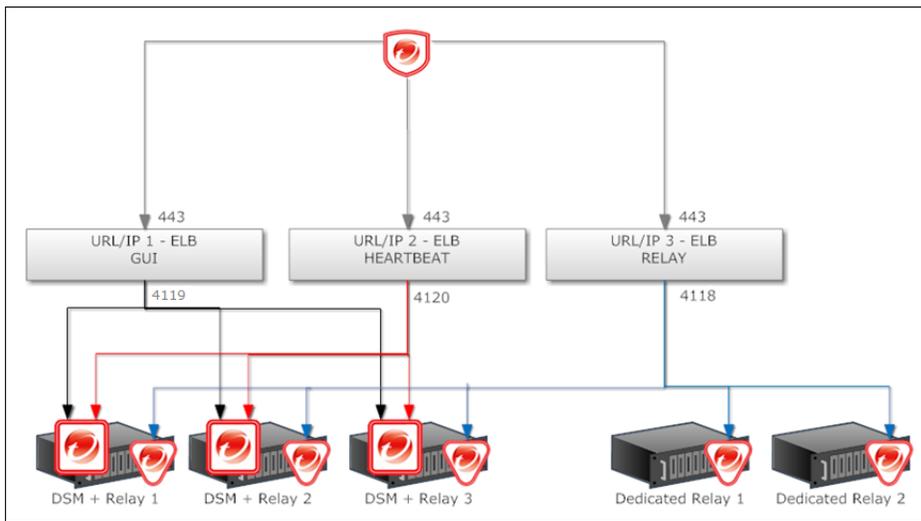
to direct the setting change or other command line action at a specific Tenant. If omitted the action is on the primary Tenant.

## Load Balancers

By default, a multi-node Manager provides the address of all Manager nodes to all agents and virtual appliances. The agents and virtual appliances use the list of addresses to randomly select a node to contact and continue to try the rest of the list until no nodes can be reached (or are all busy). If it can't reach any nodes it waits until the next heartbeat and tries again. This works very well in environments where the number of Manager nodes is fixed and avoids having to configure a load balancer in front of the Manager nodes for availability and scalability.

In Multi-Tenant environments it may be desirable to add and remove Manager nodes on demand (perhaps using auto-scaling features of cloud environments). In this case adding and removing Managers would cause an update of every agent and virtual appliance in the environment. To avoid this update the load balancer setting can be used.

Load balancers can be configured to use different ports for the different types of traffic, or if the load balancer supports port re-direction it can be used to expose all of the required protocols over port 443 using three load balancers:



In all cases, the load balancers should be configured as http/https load balancers (not SSL Terminating) This ensures a given communication exchange will occur directly between Agent/Virtual Appliance and the Manager from start to finish. The next connection may balance to a different node.

---

**Note:** Each Tenant database has an overhead of around 100MB of disk space (due to the initial rules, policies and events that populate the system).

---

**Note:** Tenant creation takes between 30 seconds and four minutes due to the creation of the schema and the population of the initial data. This ensures each new Tenant has the most up to date configuration and removes the burden of managing database templates (Especially between multiple database servers).

---

# Installing a Database for Deep Security (Multi-Tenancy Requirements)

## Configuring Database User Accounts

SQL Server and Oracle Database use different terms for database concepts described below.

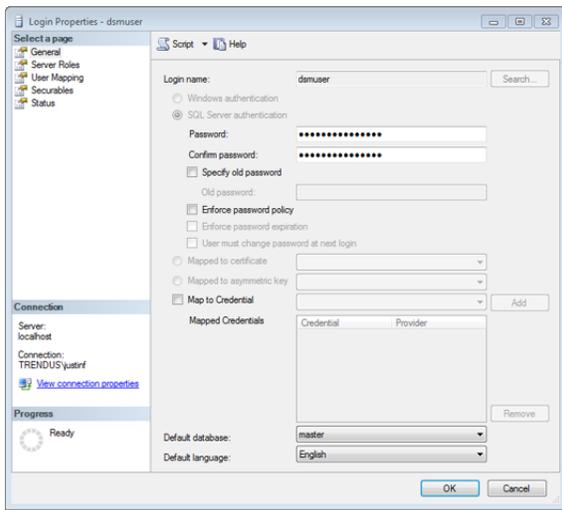
	SQL Server	Oracle Database
Process where multiple Tenants execute	Database Server	Database
One Tenant's set of data	Database	Tablespace/User

The following section uses the SQL Server terms for both SQL Server and Oracle Database.

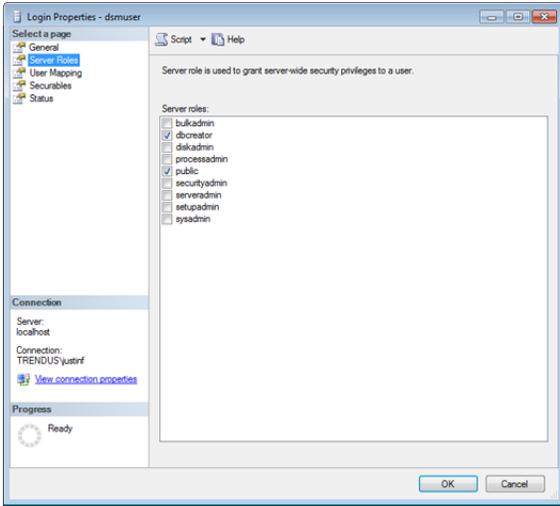
### SQL Server

**Note:** When using Multi-Tenancy, keeping the main database name short will make it easier to read the database names of your Tenants. (ie. If the main database is "MAINDB", the first Tenant's database name will be "MAINDB\_1", the second Tenant's database name will be "MAINDB\_2", and so on. )

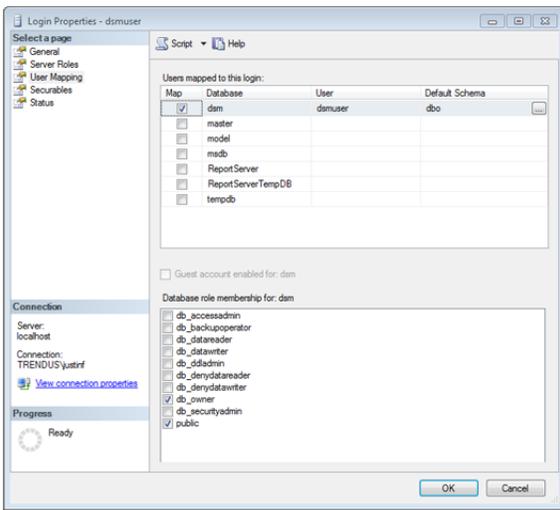
Since Multi-Tenancy requires the ability for the software to create databases, the **dbcreator** role is required on SQL Server. For example:



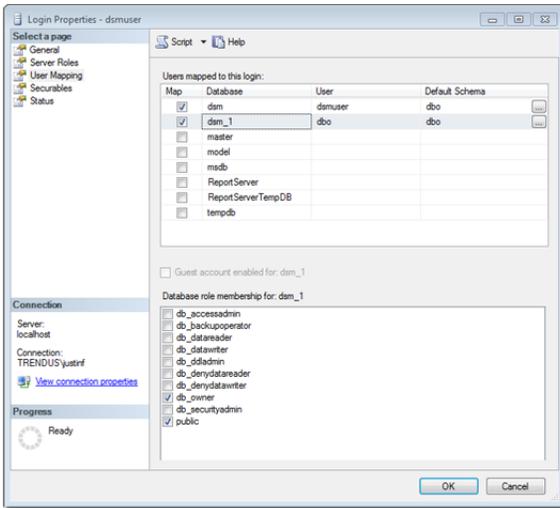
For the user role of the primary Tenant it is important to assign DB owner to the main database:



If desired, rights may be further refined to include only the ability to modify the schema and access the data.



With the **dbcreator** role the databases created by the account will automatically be owned by the same user. For example here are the properties for the user after the first Tenant has been created:



To create the first account on a secondary database server, only the **dbcreator** server role is required. No user mapping has to be defined.

## Oracle Database

Multi-Tenancy in Oracle Database is similar to SQL Server but with a few important differences. Where SQL Server has a single user account per database server, Oracle Database uses one user account per Tenant. The user that Deep Security was installed with maps to the primary Tenant. That user can be granted permission to allocate additional users and tablespaces.

**Note:** Although Oracle allows special characters in database object names if they are surrounded by quotes, Deep Security does not support special characters in database object names. This page on Oracle's web site describes the allowed characters in non-quoted names: [http://docs.oracle.com/cd/B28359\\_01/server.111/b28286/sql\\_elements008.htm#SQLRF00223](http://docs.oracle.com/cd/B28359_01/server.111/b28286/sql_elements008.htm#SQLRF00223)

**Note:** Deep Security derives Tenant database names from the main (Primary Tenant) Oracle database. For example, if the main database is "MAINDB", the first Tenant's database name will be "MAINDB\_1", the second Tenant's database name will be "MAINDB\_2", and so on. (Keeping the main database name short will make it easier to read the database names of your Tenants.)

If Multi-Tenancy is enabled, the following Oracle Database permissions must be assigned:

Roles		
Role	Admin Option	Default
CONNECT	N	Y
RESOURCE	N	Y

System Privileges	
System Privilege	Admin Option
ALTER USER	N
CREATE SEQUENCE	N
CREATE TABLE	N
CREATE TRIGGER	N
CREATE USER	N
DROP USER	N
GRANT ANY PRIVILEGE	N
GRANT ANY ROLE	N
UNLIMITED TABLESPACE	N

Object Privileges			
Object Privilege	Schema	Object	Grant Option
No items found			

Tenants are created as users with long random passwords and given the following rights:

Roles		
Role	Admin Option	Default
CONNECT	N	Y
RESOURCE	N	Y

System Privileges	
System Privilege	Admin Option
CREATE SEQUENCE	N
CREATE TABLE	N
CREATE TRIGGER	N
UNLIMITED TABLESPACE	N

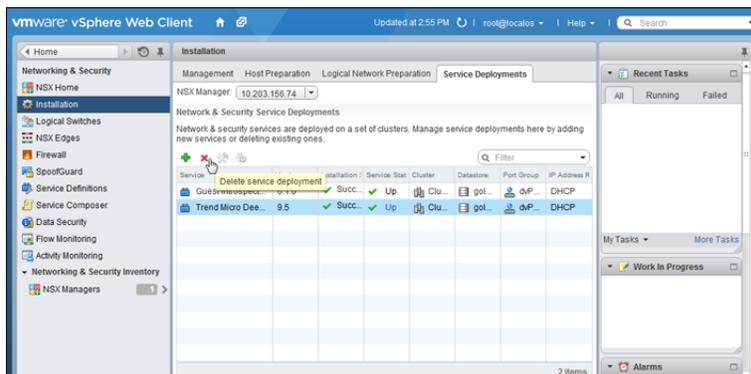
Object Privileges			
Object Privilege	Schema	Object	Grant Option
No items found			

For secondary Oracle Database servers, the first user account (a bootstrap user account) must be created. This user will have an essentially empty tablespace. The configuration is identical to the primary user account.

# Uninstalling Deep Security from your NSX Environment

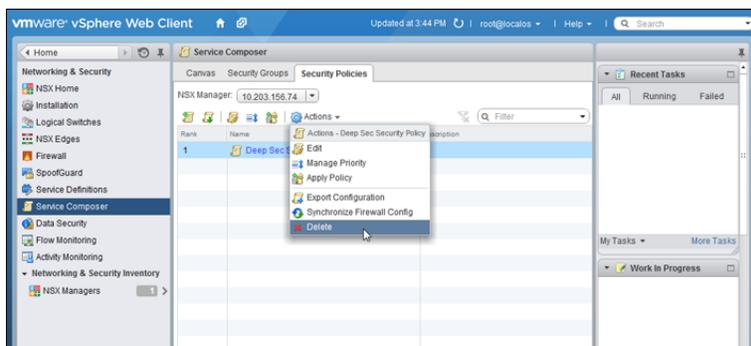
## Delete the Deep Security Service Deployment

To delete the Deep Security service deployment, in the vSphere Web Client, go to **Home > Networking and Security > Installation > Service Deployments** and delete the **Trend Micro Deep Security** service.



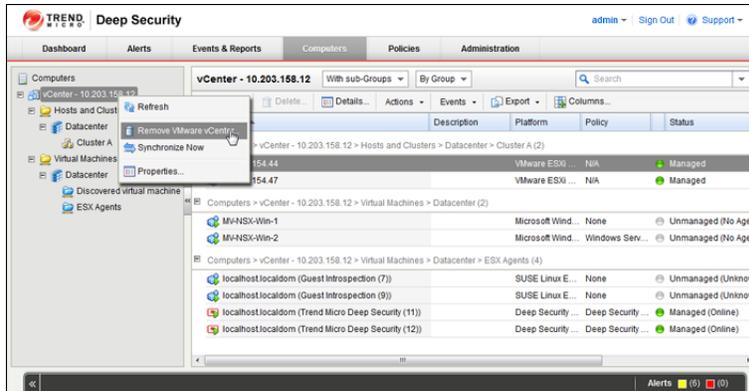
## Delete All "Deep Security" Security Policies

To delete all "Deep Security" Security Policies, go to **Home > Networking and Security > Service Composer > Security Policies** and delete the Deep Security Security Policies.

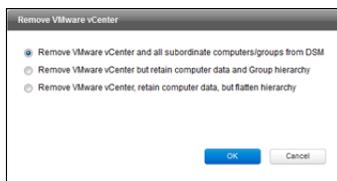


## Remove the vCenter from the Deep Security Manager

To remove the vCenter from the Deep Security Manager, in the Deep Security Manager, go to the **Computers** page, right-click the vCenter in the navigation tree and select **Remove VMware vCenter...**



This will display the **Remove VMware vCenter** modal window.



Select from the following options and click **OK**:

- **Remove VMware vCenter and all subordinate computers/groups from DSM:** Removes the vCenter and all records of the VMs including the Deep Security Policies and Rules assigned to them.
- **Remove VMware vCenter but retain computer data and Group hierarchy:** Removes the vCenter but retains its hierarchical structure and the records of the VMs including the Deep Security Policies and Rules assigned to them.
- **Remove VMware vCenter, retain computer data, but flatten hierarchy:** Removes the vCenter but retains the records of the VMs including the Deep Security Policies and Rules assigned to them. The hierarchical structure of the vCenter is flattened to a single group.

The vCenter is now removed from the Deep Security Manager.

---

**Note:** *If the Deep Security Manager has lost connectivity with the NSX Manager, you may get an error stating "Unable to remove Deep Security from VMware." To remove the vCenter from the Deep Security Manager, right-click the vCenter and select **Properties** to display its **Properties** window. On the **NSX Manager** tab in the **NSX Manager** area, click **Remove Manager**. This will remove the vCenter from the Deep Security Manager.*

---





**TREND MICRO INCORPORATED**

225 E. John Carpenter Freeway, Suite 1500  
Irving, Texas 75062 U.S.A.  
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736  
Email: support@trendmicro.com

[www.trendmicro.com](http://www.trendmicro.com)

Item Code: APEM97211/150921b