TREND MICRO

9.6 Deep Security

Service Pack 1

Installation Guide (VMware vCloud)

Advanced Protection for Physical, Virtual, and Cloud Servers

Cloud & Data Center

Complete End User

Cyber Threats

Document version: 1.4
Document number: APEM97212_150921
Release date: November 2015
Document last updated: January 19, 2017

Table of Contents

Introduction 5

About This Document 6

About Deep Security 7

What's New 11

System Requirements 14

Preparation 16

Get Deep Security Software and Activation Codes 17

Check Permissions and Communication 18

Database Considerations 20

Deep Security Manager Considerations 23

High Availability Environments 24

Choosing Agentless Protection or Combined Mode 25

Installation 26

Installing the Deep Security Manager 27

Deploying Agentless Protection in a vShield Environment 32

Deploying Agent-based Protection 40

Installing the Deep Security Notifier 54

Upgrading 56

Upgrade to Deep Security Manager 9.6 SP1 57

Appendices 60

Deep Security Manager Memory Usage 61

Deep Security Manager Performance Features 62

Silent Install of Deep Security Manager 64

Upgrade Multi-Node Deep Security Manager 66

Deep Security Manager Settings Properties File 67

Enable Multi-Tenancy 73

Multi-Tenancy (Advanced) 81

Installing a Database for Deep Security (Multi-Tenancy Requirements) 83

Creating an SSL Authentication Certificate 87

Uninstalling Deep Security 90

Introduction

About This Document

This document describes how to use Agentless and Agent-based protection to secure your VMware vCloud computing resources with Deep Security.

Intended Audience

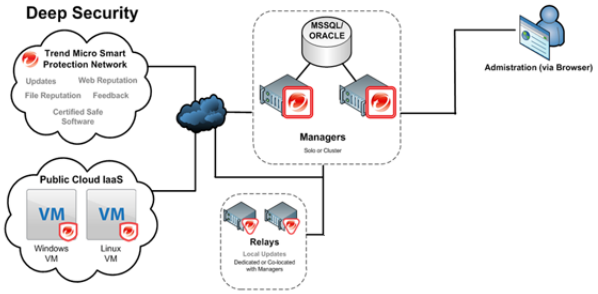
This document is intended for anyone who wants to implement Agent-based Deep Security protection in a VMware vCloud environment. The information is intended for experienced cloud administrators who have good experience with deployments, operations, and scripting languages in VMware vCloud environments.

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. When you install the AWS Marketplace version of Deep Security Manager, a Relay-enabled Agent is also installed.

- **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 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. When you install the AWS Marketplace version of Deep Security Manager, a Relay-enabled Agent is also installed. 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 SP2 (64-bit), Windows 2003 Server R2 (64-bit) with latest service pack or patch
  - Red Hat Linux 5/6 (64-bit)
- **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

    Note: SQL Server Express is not recommended for production systems, especially in multi-tenant environments.
- **Web Browser:** Firefox 24+, InternetExplorer 9.x, InternetExplorer 10.x, InternetExplorer 11.x, Chrome 33+, 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) 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 (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 SP1 (32-bit and 64-bit) with patch "Windows Server 2003 Scalable Networking Pack"
- Windows Server 2003 SP2 (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)
  - CentOS 5 (32-bit and 64-bit)
  - CentOS 6 (32-bit and 64-bit)
  - CentOS 7 (64-bit)
  - SUSE 10 SP3 and SP4 (32-bit and 64-bit)
  - SUSE 11 SP1, SP2, and SP3 (32-bit and 64-bit)
  - CloudLinux 5 (32-bit and 64-bit)
  - CloudLinux 6 (32-bit and 64-bit)
  - Oracle Linux 5 (64-bit) Unbreakable Kernel
  - Oracle Linux 6 (64-bit) Unbreakable Kernel
  - 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**.*

Preparation

Get Deep Security Software and Activation Codes

Deep Security Manager

Download a copy of the Deep Security Manager install package from the Trend Micro Download Center:

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.*

Deep Security Agents

You will need to import the Deep Security Agent software packages for the platforms you are going to protect. Import the Deep Security Agents and their supporting software packages from within the Deep Security Manager on the **Administration > Updates > Software > Download Center** page.

To import the Deep Security Agent software, see ***Installing the Deep Security Agent (page 40)***.

Note:	*Any Deep Security installation 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.*

Additional Deep Security Software

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.

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.

Check Permissions and Communication

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.

Proxy Server Information

If 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.

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 "heartbeat" port, used by Deep Security Agents and Appliances to communicate with Deep Security Manager (configurable).
- **Port 443:** In AWS Marketplace Instances, this port is used by your browser to connect to Deep Security Manager.
- **Port 4119:** In standard Deep Security installations, this port is used by your browser to connect to Deep Security Manager. Also used for communication from ESXi.
- **Port 1521:** Bi-directional Oracle Database server port.
- **Ports 1433 and 1434:** Bi-directional Microsoft SQL Server Database ports.
- **Ports 389, 636, and 3268:** Connection to an LDAP Server for Active Directory integration (configurable).
- **Port 25:** Communication to a SMTP Server to send email alerts (configurable).
- **Port 53:** For DNS Lookup.
- **Port 514:** Bi-directional communication with a Syslog server (configurable).
- **Port 443:** Communication with VMware vCloud, vCenter, vShield/NSX Manager and Amazon AWS.

Note: *For more details about how each of these ports are used by Deep Security, see **Ports Used** 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 and hypervisors uses DNS hostnames by default. In order for Deep Security Agent 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 62)***.

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.

Database Considerations

Before you install Deep Security Manager, you must install database software and create a database and user account for Deep Security Manager to use. 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.)

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.

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.

Microsoft SQL Server

- Enable "Remote TCP Connections". (See 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. The AWS Marketplace version of Deep Security Manager does not support 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. (The "Advanced" option is not available with the AWS Marketplace version of Deep Security Manager.)

Avoid special Characters for the database user name (Oracle)

Although Oracle Database allows special characters when configuring the database user object, if they are surrounded by quotes. Deep Security does not support special characters for the database user.

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 Support

Deep Security supports:

- SUSE Linux Enterprise Server 11 SP1 with Oracle RAC 11g R2 (v11.2.0.1.0)
- Red Hat Linux Enterprise Server 5.8 with Oracle RAC 11g R2 (v11.2.0.1.0)

Note:	*Applying the default Linux Server Deep Security Policy to the Oracle RAC nodes should not cause any communication issues with Oracle Automated Storage Management (ASM) and cluster services. However if you experience issues, try customizing the Firewall settings according to the port requirements found in Oracle RAC documentation, or disabling the Firewall altogether.* *http://docs.oracle.com/cd/E11882_01/install.112/e41962/ports.htm#BABECFJF*

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.

Deep Security Manager Considerations

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.*

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.*

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.*

Choosing Agentless Protection or Combined Mode

In Deep Security 9.6 SP1, there are two options for protecting your virtual machines: Agentless Protection or Combined Mode.

Agentless Protection

In pre-9.6 versions of Deep Security, the Deep Security Virtual Appliance (DSVA) and Filter Driver worked together to protect virtual machines without requiring an in-guest Agent. The Virtual Appliance is installed on the ESXi server and uses VMware's VMsafe-NET API to intercept network traffic at the hypervisor. Security policies are applied per virtual machine.

Deep Security 9.6 SP1 does not include a Filter Driver and you cannot use an older Filter Driver with the 9.6 SP1 DSVA. Without the Filter Driver, the 9.6 SP1 DSVA is limited to providing Anti-Malware and Integrity Monitoring protection for your VMs.

Alternatively, if you want full Agentless protection for your virtual machines, you can use Deep Security 9.0, 9.5, or 9.5 SP1 versions of the Filter Driver and DSVA with Deep Security Manager 9.6 SP1.

Combined Mode

If you are using a 9.6 SP1 version of the DSVA and you require more than the Anti-Malware and Integrity Monitoring modules, you will need to install the Deep Security Agent on each of your virtual machines. This way of protecting virtual machines using both the DSVA and Agent is know as "Combined Mode".

With Combined Mode, the DSVA provides the Anti-Malware and Integrity Monitoring functionality. The Deep Security Agent provides Web Reputation, Firewall, Intrusion Prevention, and Log Inspection.

Note:	*If a Virtual Machine is running Linux, Anti-Malware support will be provided by Deep Security Agent, rather than DSVA.*

Note:	*Deep Security 9.5 SP1 and earlier included the ability to protect virtual machines using the "Coordinated Approach". With the Coordinated Approach, primary protection was provided by the Deep Security Agent, with the DSVA available as failover protection in case the Agent went offline. The Coordinated Approach is not available using Deep Security 9.6 SP1. If you are upgrading from a system that used the Coordinated Approach, your system will be migrated to Combined Mode.*

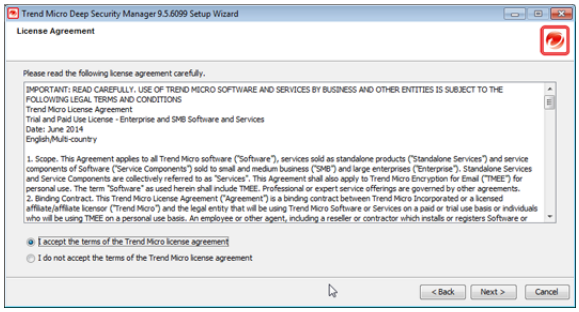
Installation

Installing the Deep Security Manager

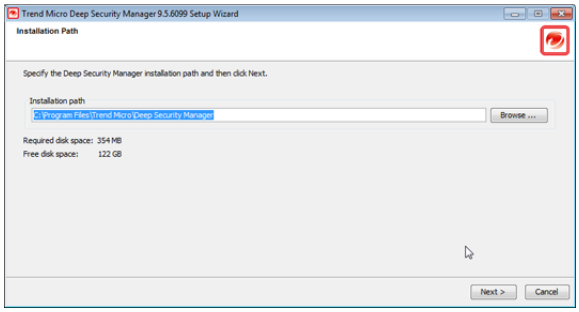
Install the Deep Security Manager for Windows

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

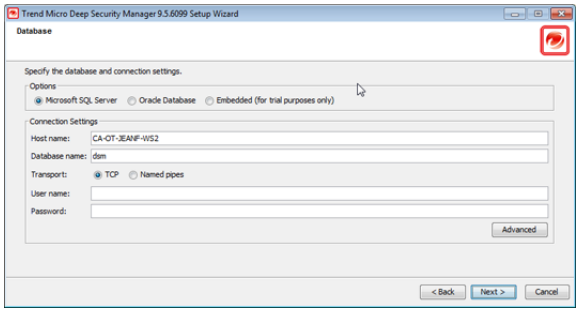
2. **License Agreement:** If you agree to the terms of the license agreement, select **I accept the terms of the Trend Micro license agreement**.



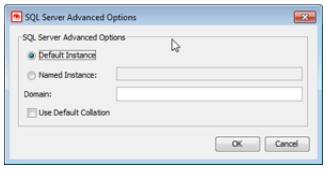
3. **Installation Path:** Select the folder where Deep Security Manager will be installed and click **Next**.



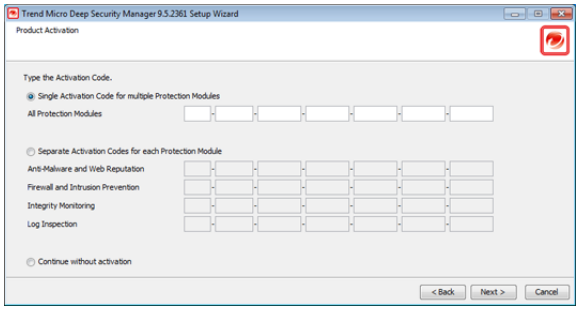
4. **Database:** Select the database you installed previously.



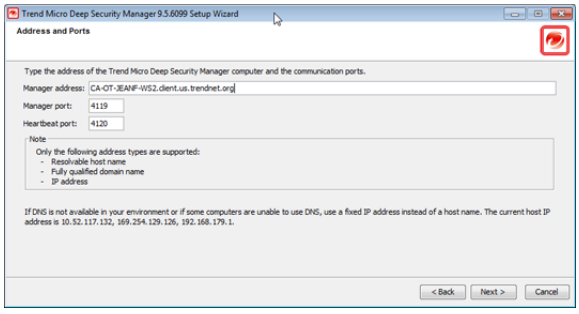
If your database is SQL Server, click **Advanced** to specify a **Named Instance**, a **Domain**, or the use of **Default Collation**. Collation determines how strings are sorted and compared. The default is "unselected", which means that Deep Security will use Latin1_General_CS_AS for collation on text-type 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**.)



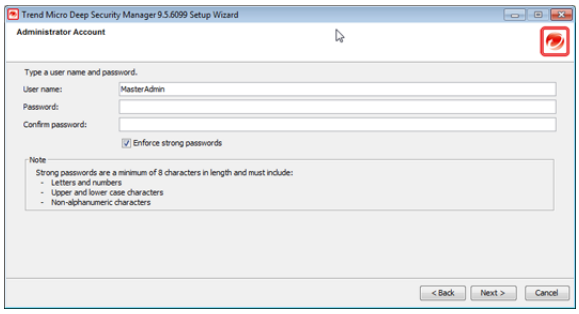
6. **Address and Ports:** Enter the hostname, URL, or IP address of this computer. The Manager Address must be either a resolvable hostname, a fully qualified domain name, or an IP address. If DNS is not available in your environment, or if some computers are unable to use DNS, a fixed IP address should 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.



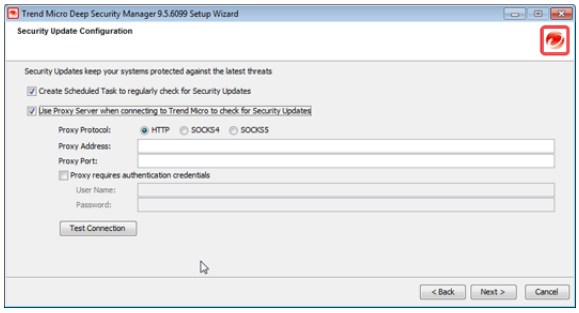
7. **Administrator Account:** Enter a username and password for the Master Administrator account. Selecting the Enforce strong passwords (recommended) requires this and future administrator passwords to include upper and lower-case letters, non-alphanumeric characters, and numbers, and to require a minimum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

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

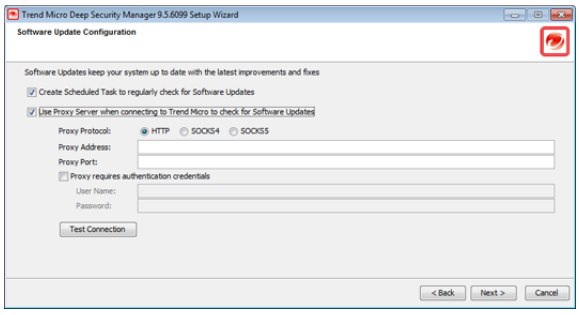
   Note: *If you have admin rights on the Manager host machine, you can reset an account password using the* `dsm_c -action unlockout -username USERNAME -newpassword NEWPASSWORD [-disablemfa]` *command.*



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 to use a proxy to 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.

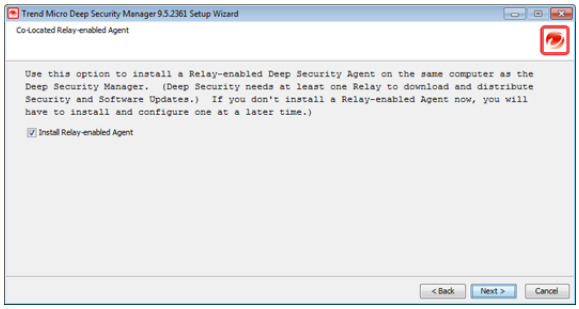


9. **Configure Software Updates:** The options for software updates are the same as those for security updates in the previous step.

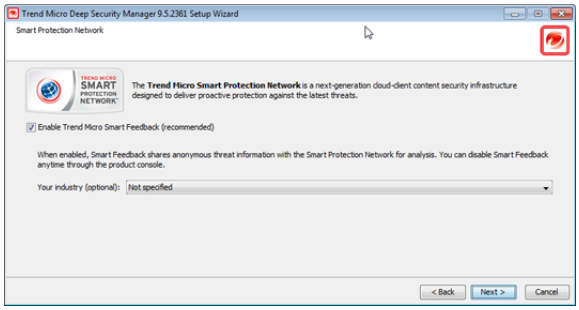


10. **Co-Located Relay-enabled Agent:** If an Agent install package is available either in the local folder or from the Trend Micro Download Center, you will be given the option to install a co-located Relay-enabled Agent. Any Deep Security installation requires at least one Relay to download and distribute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

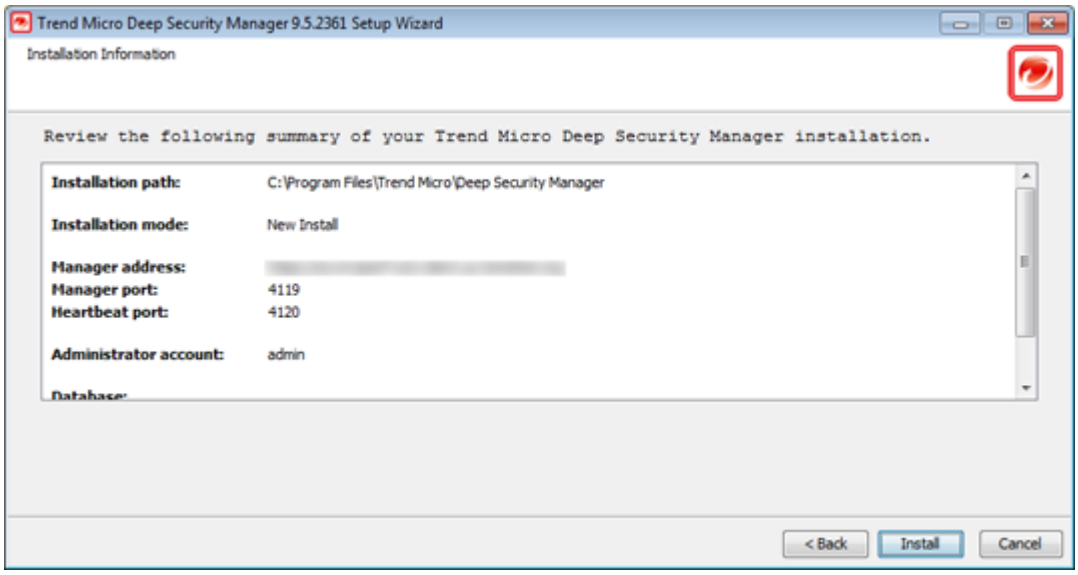
    Note: *Installing a co-located Relay-enabled Agent is strongly recommended.*



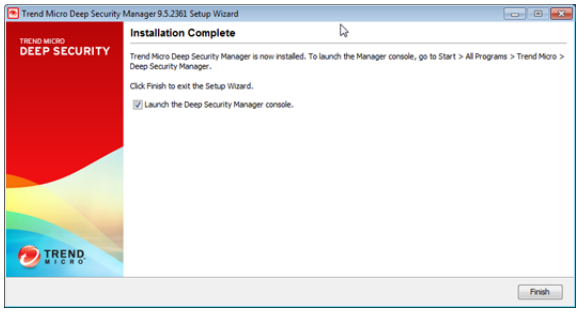
11. **Smart Protection Network:** Select whether you want to enable Trend Micro Smart Feedback (recommended). (You can enable or configure Smart Feedback later using the Deep Security Manager). Optionally enter your industry by selecting from the drop-down list.



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 64)***.

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 87)****.*

Deploying Agentless Protection in a vShield Environment

VMware vCloud integration enables the primary Tenant in a Multi-Tenant installation to add a vCenter to their Deep Security Manager, configure the vShield connector, and to deploy and manage the Deep Security Virtual Appliance. The Tenants can import vCloud Organizations as Cloud Accounts and apply Agentless Deep Security protection to them.

Note:	*When applying Agentless protection to vCloud Organizations, only the Anti-Malware and Integrity Monitoring modules are supported and the vCloud Organizations must only be added to Tenants (not the primary Tenant). If you want to enable other protection modules, you will need to use Agent-based protection instead (see* ***Deploying Agent-based Protection) (page 40)****.*

For NSX instructions, see "Deploying Agentless Protection in a NSX Environment" in the *Deep Security 9.6 SP1 Installation Guide (VMware NSX)*.

Enabling Agentless Protection of vCloud VMs

To enable Agentless Protection of vCloud VMs:

1. In the Deep Security Manager console, go to **Administration** > **System Settings** > **Agents.**
2. Select the **Allow Appliance protection of vCloud VMs** checkbox.
3. Click **Save**.

Creating a Multi-Tenancy Environment

There are two main task required to create a multi-tenancy environment: you must enable Multi-Tenancy and then create Tenants. For step-by-step instructions on how to perform these tasks, as well as requirements and recommendations for a Multi-Tenant environment, see **Multi-Tenancy** in the User's Guide section of the Deep Security Manager Administrator's Guide or Online Help.

Adding a vCenter and Deploying the Deep Security Virtual Appliance

The primary Tenant must add a vCenter and deploy the Deep Security Virtual Appliance.

VMware Requirements

You must be running the following VMware software:

- **VMware vSphere 5.1, 5.5, or 6.0**
  - **VMware vCenter 5.1, 5.5, or 6.0**
  - **VMware ESXi 5.1, 5.5, or 6.0**
  - **VMware vSphere Web Client**
  - **vShield Manager:** If you are running vSphere 5.5, use vShield Manager 5.5.2 or higher. If you are running vSphere 6.0, use vShield Manager 5.5.4 or higher.

Your vShield datacenter must meet the following configuration requirements:

- **VMware vShield Endpoint service must be installed on all ESXi servers:**
  1. Login to vShield Manager by browsing to **https://<vSM-ip>**
  2. On the **Settings and Reports > Configuration** tab, enter your vCenter Server Information
  3. In the left navigation pane, select the ESXi hypervisor to be protected by Deep Security.

4. On the **Summary** tab, click the **Install** link for the **vShield Endpoint Service**
5. Select the services to install/upgrade, check **vShield Endpoint** and click the **Install** button at the top right of the screen. Click **OK**.
6. After installing, make sure the Service vShield Endpoint correctly displays the installed version (The **Install** link will have changed to **Uninstall**)

- **Virtual machines must have the latest VMware Tools installed, including the VMware Guest Introspection Driver:**
  1. Launch the VMware Tools installer and select to perform an Interactive Install.
  2. During VMware Tools installation, select **Custom Install**.
  3. Expand VMware Device Drivers.
  4. Expand VMCI Driver.
  5. Select vShield Drivers and choose **This feature will be installed on local drive**.
  6. Click **Yes** to restart the machine.

Consult your VMware documentation for more detailed information on configuring your vShield environment to meet the above 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, with a database**. (See ***Installing the Deep Security Manager (page 27)***.)

Note:	*Ideally, Deep Security Manager, the database, VMware vCenter, and vShield Manager should be installed on a dedicated infrastructure ESXi server in the same datacenter as your workload ESXi servers.*

- **A Deep Security Agent with Relay functionality enabled must be installed and activated, and all Updates must have completed downloading.** (For instructions on installing an Agent and enabling the Relay functionality, see ***Deploying Agent-based Protection (page 40)***.)
- **The Deep Security Virtual Appliance (DSVA) 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.

This section describes how to prepare the vShield environment for Agentless protection using the DSVA.

Add vCenter to the Deep Security Manager

Deep Security Manager configuration must be performed using a primary Tenant account with Full Access rights.

1. Log in to Deep Security Manager as the primary Tenant.
2. Click **Computers > New > Add VMware vCenter.**
3. Enter the vCenter Server IP Address (or hostname if DNS is configured and able to resolve FQDN to IP addresses), and the Username and Password for the vCenter. Click **Next**.
4. Accept the vCenter certificate.
5. Enter the vShield Manager Server Address, Username and Password. (You can also configure this information later from the Deep Security Manager). Click **Next**.
6. Accept the vShield Manager SSL certificate.
7. Review the vCenter information. Click **Finish**.
8. The **VMware vCenter has been successfully added** message will be displayed. Click **Close**.

Note: *In a large environment with more than 3000 machines reporting to a vCenter Server, this process may take 20 to 30 minutes to complete. You can check the vCenter's **Recent Task** section to verify if there are activities running.*

Note: *Real-time synchronization will be maintained with this VMware vCenter to keep the information displayed in the Deep Security Manager up-to-date (number of VMs, their status, etc.).*

Deploy Agentless Security

The next step is to deploy the Deep Security Virtual Appliance to the ESXi server. You can also install the Deep Security Filter Driver if it is supported by the version of vSphere that you are running.

Note: *If you are installing the Deep Security Filter Driver on vSphere 5.1 or 5.5, the ESXi will be placed in maintenance mode for this task. All virtual machines running on this ESXi must be stopped/paused or vMotioned to another ESXi server (make sure a cluster server with vMotion support is set up so that this can be done automatically).*

1. Log in to Deep Security Manager as the primary Tenant.
2. Click **Computers > vCenter**.
3. Find the ESXi server in the Computers list (its **Status** column should read **Unmanaged**), right-click and select **Actions > Deploy Agentless Security** to display the Deploy Agentless Security wizard. Click **Next**.

   Note: *You can select multiple ESXi servers if they are all the same version and all have the same Filter Driver status.*

4. On the next page, select the components that you want to deploy to the ESXi server(s). You can choose to deploy the Deep Security Virtual Appliance and/or the Deep Security Filter Driver. Click **Next**.

   Note: *If the ESXi server already has a Filter Driver installed, that checkbox will be unavailable.*

   Note: *This page will not appear if you are installing on vSphere 6.*

5. If you have chosen to install the Filter Driver, select **Yes** to allow the Deep Security Manager automatically bring the ESXi server(s) in and out of maintenance mode. If you select **No**, you will be responsible for putting the ESXi(s) into maintenance mode. Click **Next**.
6. If you have chosen to install the DSVA, enter an **Appliance Name** for the Appliance and select a **Datastore** for the Appliance. Select the **Folder** for the Datacenter and select the **Management Network** for the Appliance. Click **Next**.
7. If you have chosen to install the DSVA, define the Appliance Hostname. Enter the IPv4 Address and/or IPv6 Address for the Appliance. (DHCP is enabled by default). Click **Next**.
8. If you have chosen to install the DSVA, select a disk provisioning format. Click **Next**.
9. The next page summarized the actions that will be taken. Click **Finish**.
10. The Agentless Security deployment process will begin. When the process is complete, you will see a message stating that it was successful.
11. If you have chosen to install the DSVA and the installation was successful, you can choose to have the wizard activate the Deep Security Virtual Appliance now, or activate it later (the activation process is described later). Click **Next**.
12. Click **Close**.

The Virtual Appliance is now displayed along with the other computers in the **vCenter** Group in the Deep Security Manager **Computers > vCenter** list.

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 proactively 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 machine) is set to "Disabled", vCenter Server will 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 a local store as opposed to a shared store. When the Virtual Appliance is deployed onto a local store it cannot be vMotioned by DRS.) For further information on DRS and pinning virtual machines to a specific ESXi consult your VMware documentation.

Note: *The Deep Security Manager puts the ESXi into **maintenance mode** during an install or upgrade of the Deep Security Filter Driver. When an ESXi already hosting a Virtual Appliance is put into maintenance mode, the Deep Security Manager will automatically power the Virtual Appliance off and back on again when exiting maintenance mode. If the ESXi is put into maintenance mode by means other than through the Deep Security Manager, the Virtual Appliance is not powered off/on automatically.*

Activate the Deep Security Virtual Appliance

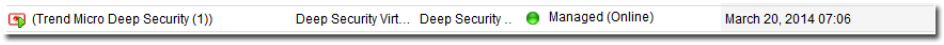
To activate the Virtual Appliance:

1. Log in to Deep Security Manager as the primary Tenant.
2. Click **Computers > vCenter**
3. Right-click on the DSVA machine and select **Actions > Activate Appliance**. In the wizard that appears, click **Next**.
4. For Policy, select **Deep Security Virtual Appliance**.
5. Select the **Relay Group** this Virtual Appliance will communicate with for Security and Software Updates, then click **Next** to start the activation process.
6. The DSVA will register itself with vShield Manager. You will see multiple tasks being executed in vCenter Console.

   Note: *The DSVA requires vShield Manager to configure the VMX file of each machine that is on the ESXi. Depending on the number of Virtual Machines, it could take several hours to complete the activation.*

   If vShield Manager is experiencing problems, the DSVA may fail to activate. Check whether you can open the vShield Manager web console. If it is not responding, you can reboot the vShield Manager and wait for a few minutes after vShield is back on line to attempt DSVA activation again.
7. In **Activate Virtual Machines**, select the virtual machines that you want to activate and **Finish**.

The Virtual Appliance is now activated. You can confirm this by finding the Virtual Appliance on the Deep Security Manager's **Computers** page and seeing that it is in the "Managed (Online)" state:



Now that the Virtual Appliance is activated, all the VMs on the ESXi can be protected by assigning Deep Security Polcies to them through the Deep Security Manager console.

Once the Virtual Appliance is activated, any virtual machines that are added to the ESXi server afterwards can be automatically activated and a Policy can be automatically applied. New virtual machines can automatically be assigned Policies when detected. For details on how to perform these automatic operations, see "Event-Based Tasks" in the Deep Security Manager Help.

Note: *The Virtual Appliance requires that all VMs that are to be protected have been assigned unique UUIDs by the vCenter. A situation with duplicate UUIDs can occur if you copy a VM. After copying a VM, you are asked by vCenter whether the new VM is a copy or whether it was moved. If you select the **I copied it** option, vCenter will assign it a new UUID. However, if you select the **I moved it** option (when in fact it was copied), vCenter will not assign it a new UUID. You will then have two VMs with the same UUID which will cause problems for the Virtual Appliance. If the Virtual Appliance is instructed to protect multiple VMs with the same UUID, an Alert will be raised and the operation will fail.*

Configuring VMware vCloud Resources for Integration with Deep Security

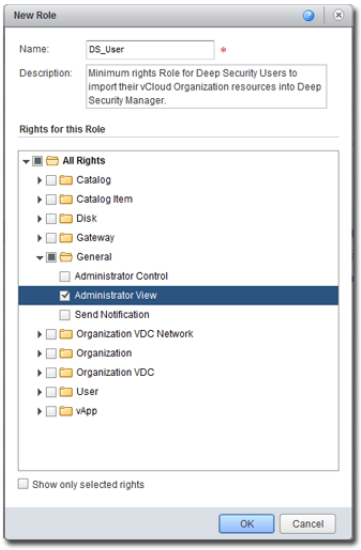
To enable vCloud integration, you must assign a minimum set of rights to the user accounts Tenants will use to import their vCloud "Cloud Accounts" and you must configure the vCenter database to assign unique UUIDs to new virtual machines.

Creating a Minimum Rights Role for vCloud Account Tenant Users

The User accounts you create in vCloud director that the Deep Security Tenants will use to add their Cloud Accounts to their Deep Security Manager require only the **All Rights > General > Administrator View** right.

To create a minimum rights role:

1. Log in to vCloud Director.
2. In the **System** tab, click on **Administration**.
3. In the navigation panel on the left, click on **Roles**.
4. Click the "plus" sign to create a new Role (for example, "DS_User").
5. Select the **Administrator View** right in the **All Rights > General** folder:



6. Click **Ok**.

You can now assign this Role to the user accounts you will give to Deep Security Users to import their vCloud resources into the Deep Security Manager.

Note: *When providing a Deep Security User with their credentials, you must include the IP address of the vCloud Organization and instruct them that when importing the vCloud resources into their Deep Security Manager, their username must include "@orgName". For example if the vCloud account's username is* ***kevin*** *and the vCloud Organization you've given the account access to is called* ***CloudOrgOne****, then the Deep Security User must enter* ***kevin@CloudOrgOne*** *as their username when importing the vCloud resources. (For a vCloud administrator view, use* ***@system****.)*

Note: *You can configure Deep Security Manager to use a proxy server specifically for connecting to instances being protected in Cloud Accounts. The proxy setting can be found in* ***Administration > System Settings > Proxies > Proxy Server Use > Deep Security Manager (Cloud Accounts)****.*

Configuring the vCenter Database to Assign Unique UUIDs to New Virtual Machines

Deep Security requires that all protected virtual machines have unique UUIDs. Virtual Machines created from a vApp template can be assigned duplicate UUIDs which can cause problems. However, you can configure your database to assign unique UUIDs to these VMs created from a template.

Note: *The following information is taken from a VMware Knowledge Base article, "BIOS UUIDs in vCloud Director are not unique when virtual machines are deployed from catalog templates (2002506).*

To configure the database to assign unique UUIDs to new virtual machines that are created from a template, you must set the **CONFIG** table of the database, with the parameter **backend.cloneBiosUuidOnVmCopy**, to **0**.

To set this parameter in Oracle Database, launch Oracle Database Enterprise Manager and run the following commands:

Note: *In this example, "VCLOUD" is the name of the data base you created for vCloud.*

```
set feedback on echo on
set linesize 120
update "VCLOUD"."CONFIG" set VALUE = '0' where NAME='backend.cloneBiosUuidOnVmCopy';
commit;
select * from "VCLOUD"."CONFIG" where VALUE = '0' and NAME='backend.cloneBiosUuidOnVmCopy';
```

To set this parameter in Microsoft SQL Server, launch SQL Server Management Studio and run the following commands:

```
USE VCLOUD
GO
update config set value = '0' where name='backend.cloneBiosUuidOnVmCopy'
select * from dbo.config where value = 0 and name='backend.cloneBiosUuidOnVmCopy';
```

When the parameter has been set, restart all cells in vCloud Director.

Note: *This change does not affect previously existing virtual machines.*

Enabling the OVF Environment Transport for VMware Tools on your guest VMs

Enabling the OVF Environment Transport for VMware Tools on your guest VMs will expose the **guestInfo.ovfEnv** environment variable making it easier for Agents to uniquely identify their VMs to the Deep Security Manager. This will reduce the risk of VM misidentification.

To enable the OVF Environment Transport for VMware Tools on a guest VM:

1. In vCloud Director, open the VM's **Properties** screen, go the **Guest OS Customization** tab and select the **Enable guest customization** checkbox. Click **OK**.
2. In vCenter, select the same VM, open its **Properties** screen, go to the **Options** tab.
3. Click **vApp Options** and select the **Enabled** radio button. **OVF Settings** will now be exposed.
4. In **OVF Settings**, select the **VMware Tools** checkbox in the **OVF Environment Transport** area. Click **OK**.

If your VM is running, it must be restarted for the changes to take effect.

The data used by Deep Security are taken from the following properties: **vmware.guestinfo.ovfenv.vcenterid** and **vmware.guestinfo.ovfenv.vcloud.computername**.

Activating Virtual Appliance Protection on Virtual Machines

The Tenants can import vCloud Organizations as Cloud Accounts and apply Agentless Deep Security protection to them.

Importing Computers from a VMware vCloud Organization Account

To import VMware vCloud Organization resources:

1. In the Deep Security Manager, go to the **Computers** section, right-click **Computers** in the navigation panel and select **Add Cloud Account...** to display the **Add Cloud Account** wizard.
2. Select **vCloud** as the Cloud Provider Type.
3. Enter a **Name** and **Description** of the resources you are adding. (These are only used for display purposes in the Deep Security Manager.)
4. Enter the vCloud **Address**. (The hostname of the vCloud Director host machine.)
5. Enter your **User name** and **Password**.

   Note: *Your **User name** must be in the form **username@vcloudorganization**.*

6. Click **Next**.
7. Deep Security Manager will verify the connection to the cloud resources and display a summary of the import action. Click **Finish**.

The VMware vCloud resources now appear in the Deep Security Manager under their own branch under **Computers** in the navigation panel.

Importing Computers from a VMware vCloud Air Virtual Data Center

To import a VMware vCloud Air data center:

1. In the Deep Security Manager, go to the **Computers** section, right-click **Computers** in the navigation panel and select **Add Cloud Account...** to display the **Add Cloud Account** wizard.
2. Select **vCloud** as the Cloud Provider Type.
3. Enter a **Name** and **Description** of the VMware vCloud Air virtual data center you are adding. (These are only used for display purposes in the Deep Security Manager.)
4. Enter the **Address** of the VMware vCloud Air virtual data center.

   Note: ***To determine the address of the VMware vCloud Air virtual data center:***
   1. *Log in to your VMware vCloud Air portal.*
   2. *On the **Dashboard** tab, click on the data center you want to import into Deep Security. This will display the **Virtual Data Center Details** information page.*
   3. *In the Related Links section of the **Virtual Data Center Details** page, click on **vCloud Director API URL**. This will display the full URL of the vCloud Director API.*
   4. *Use the hostname only (not the full URL) as the Address of the VMware vCloud Air virtual data center that you are importing into Deep Security.*

5. Enter your **User name** and **Password**.

   Note: *Your **User name** must be in the form **username@virtualdatacenterid**.*

6. Click **Next** .
7. Deep Security Manager will verify the connection to the virtual data center and display a summary of the import action. Click **Finish**.

The VMware vCloud Air data center now appears in the Deep Security Manager under its own branch under **Computers** in the navigation panel.

Activating Virtual Appliance Protection on Virtual Machines

To activate Virtual Appliance protection on virtual machines:

1. Right-click on a virtual machine in the **Computers** list and select **Actions > Activate**.

2. The **Status** column for the virtual machine will change to "Managed (Online)".

The virtual machine is now protected by the Virtual Appliance even though no in-guest Agent is installed on the virtual machine. Policies can be assigned to this virtual machine like any other computer being managed by Deep Security Manager.

Deploying Agent-based Protection

Configuring VMware vCloud Resources for Integration with Deep Security

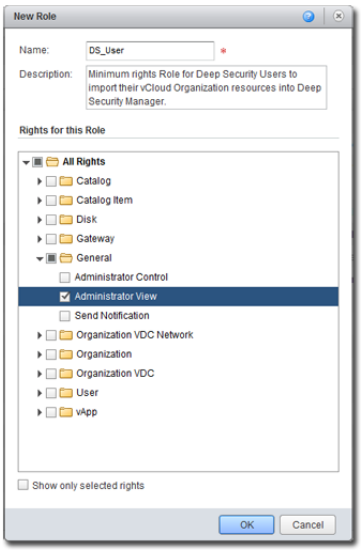
To enable vCloud integration, you must assign a minimum set of rights to the user accounts Tenants will use to import their vCloud "Cloud Accounts" and you must configure the vCenter database to assign unique UUIDs to new virtual machines.

Creating a Minimum Rights Role for vCloud Account Tenant Users

The User accounts you create in vCloud director that the Deep Security Tenants will use to add their Cloud Accounts to their Deep Security Manager require only the **All Rights > General > Administrator View** right.

To create a minimum rights role:

1. Log in to vCloud Director.
2. In the **System** tab, click on **Administration**.
3. In the navigation panel on the left, click on **Roles**.
4. Click the "plus" sign to create a new Role (for example, "DS_User").
5. Select the **Administrator View** right in the **All Rights > General** folder:



6. Click **Ok**.

You can now assign this Role to the user accounts you will give to Deep Security Users to import their vCloud resources into the Deep Security Manager.

Note:	*When providing a Deep Security User with their credentials, you must include the IP address of the vCloud Organization and instruct them that when importing the vCloud resources into their Deep Security Manager, their username must include "@orgName". For example if the vCloud account's username is* ***kevin*** *and the vCloud Organization you've given the account access to is called* ***CloudOrgOne****, then the Deep Security User must enter* ***kevin@CloudOrgOne*** *as their username when importing the vCloud resources. (For a vCloud administrator view, use* ***@system****.)*

Note: *You can configure Deep Security Manager to use a proxy server specifically for connecting to instances being protected in Cloud Accounts. The proxy setting can be found in **Administration > System Settings > Proxies > Proxy Server Use > Deep Security Manager (Cloud Accounts)**.*

Configuring the vCenter Database to Assign Unique UUIDs to New Virtual Machines

Deep Security requires that all protected virtual machines have unique UUIDs. Virtual Machines created from a vApp template can be assigned duplicate UUIDs which can cause problems. However, you can configure your database to assign unique UUIDs to these VMs created from a template.

Note: *The following information is taken from a VMware Knowledge Base article, "BIOS UUIDs in vCloud Director are not unique when virtual machines are deployed from catalog templates (2002506).*

To configure the database to assign unique UUIDs to new virtual machines that are created from a template, you must set the **CONFIG** table of the database, with the parameter **backend.cloneBiosUuidOnVmCopy**, to **0**.

To set this parameter in Oracle Database, launch Oracle Database Enterprise Manager and run the following commands:

Note: *In this example, "VCLOUD" is the name of the data base you created for vCloud.*

```
set feedback on echo on
set linesize 120
update "VCLOUD"."CONFIG" set VALUE = '0' where NAME='backend.cloneBiosUuidOnVmCopy';
commit;
select * from "VCLOUD"."CONFIG" where VALUE = '0' and NAME='backend.cloneBiosUuidOnVmCopy';
```

To set this parameter in Microsoft SQL Server, launch SQL Server Management Studio and run the following commands:

```
USE VCLOUD
GO
update config set value = '0' where name='backend.cloneBiosUuidOnVmCopy'
select * from dbo.config where value = 0 and name='backend.cloneBiosUuidOnVmCopy';
```

When the parameter has been set, restart all cells in vCloud Director.

Note: *This change does not affect previously existing virtual machines.*

Enabling the OVF Environment Transport for VMware Tools on your guest VMs

Enabling the OVF Environment Transport for VMware Tools on your guest VMs will expose the **guestInfo.ovfEnv** environment variable making it easier for Agents to uniquely identify their VMs to the Deep Security Manager. This will reduce the risk of VM misidentification.

To enable the OVF Environment Transport for VMware Tools on a guest VM:

1. In vCloud Director, open the VM's **Properties** screen, go the **Guest OS Customization** tab and select the **Enable guest customization** checkbox. Click **OK**.
2. In vCenter, select the same VM, open its **Properties** screen, go to the **Options** tab.
3. Click **vApp Options** and select the **Enabled** radio button. **OVF Settings** will now be exposed.
4. In **OVF Settings**, select the **VMware Tools** checkbox in the **OVF Environment Transport** area. Click **OK**.

If your VM is running, it must be restarted for the changes to take effect.

The data used by Deep Security are taken from the following properties: **vmware.guestinfo.ovfenv.vcenterid** and **vmware.guestinfo.ovfenv.vcloud.computername**.

Import Computers from a VMware vCloud Organization Account

To import VMware vCloud Organization resources:

1. In the Deep Security Manager, go to the **Computers** section, right-click **Computers** in the navigation panel and select **Add Cloud Account...** to display the **Add Cloud Account** wizard.
2. Select **vCloud** as the Cloud Provider Type.
3. Enter a **Name** and **Description** of the resources you are adding. (These are only used for display purposes in the Deep Security Manager.)
4. Enter the vCloud **Address**. (The hostname of the vCloud Director host machine.)
5. Enter your **User name** and **Password**.

   Note: *Your **User name** must be in the form **username@vcloudorganization**.*

6. Click **Next**.
7. Deep Security Manager will verify the connection to the cloud resources and display a summary of the import action. Click **Finish**.

The VMware vCloud resources now appear in the Deep Security Manager under their own branch under **Computers** in the navigation panel.

After adding the Cloud Provider resources, you must install an Agent and assign a Policy to the computer (see ***Installing Deep Security Agents on your Virtual Machines (page 40)***.)

Import Computers from a VMware vCloud Air Virtual Data Center

To import a VMware vCloud Air data center:

1. In the Deep Security Manager, go to the **Computers** section, right-click **Computers** in the navigation panel and select **Add Cloud Account...** to display the **Add Cloud Account** wizard.
2. Select **vCloud** as the Cloud Provider Type.
3. Enter a **Name** and **Description** of the VMware vCloud Air virtual data center you are adding. (These are only used for display purposes in the Deep Security Manager.)
4. Enter the **Address** of the VMware vCloud Air virtual data center.

   Note: ***To determine the address of the VMware vCloud Air virtual data center:***
   1. *Log in to your VMware vCloud Air portal.*
   2. *On the **Dashboard** tab, click on the data center you want to import into Deep Security. This will display the **Virtual Data Center Details** information page.*
   3. *In the Related Links section of the **Virtual Data Center Details** page, click on **vCloud Director API URL**. This will display the full URL of the vCloud Director API.*
   4. *Use the hostname only (not the full URL) as the Address of the VMware vCloud Air virtual data center that you are importing into Deep Security.*

5. Enter your **User name** and **Password**.

   Note: *Your **User name** must be in the form **username@virtualdatacenterid**.*

6. Click **Next** .

7. Deep Security Manager will verify the connection to the virtual data center and display a summary of the import action. Click **Finish**.

The VMware vCloud Air data center now appears in the Deep Security Manager under its own branch under **Computers** in the navigation panel.

After adding the Cloud Provider resources, you must install an Agent and assign a Policy to the computer (see ***Installing Deep Security Agents on your Virtual Machines (page 40)***.)

Installing Deep Security Agents on Your Virtual Machines

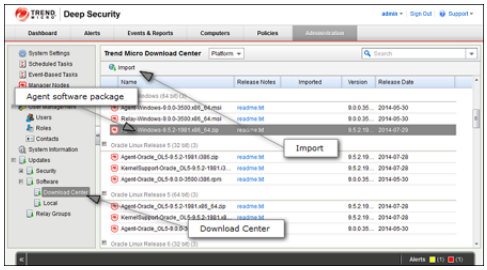
This section describes how to install and activate Deep Security Agents and how to enable Relay functionality (if required).

Importing Agent Software

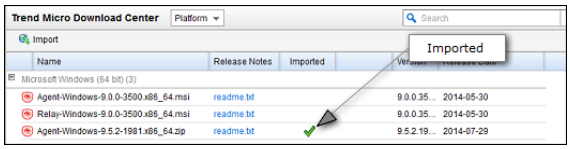
A Deep Security Agent is initially installed with core functionality only. It is only when a Protection Module is enabled on an Agent that the plug-ins required for that module are downloaded and installed. *For this reason, Agent software packages must be imported into Deep Security Manager before you 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.



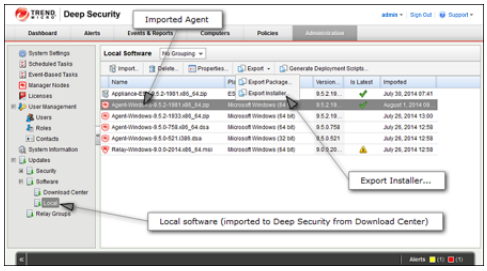
3. When the software has finished downloading, a green check mark will appear in the **Imported** column for that Agent.



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.*

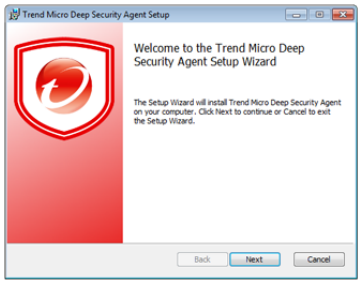
The Deep Security Agent "zip" files are made available on the Trend Micro Download Center for users who need to manually import the Agents into their Deep Security environment because their Deep Security Manager is air-gapped and cannot connect directly to the Download Center web site. Users whose Deep 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

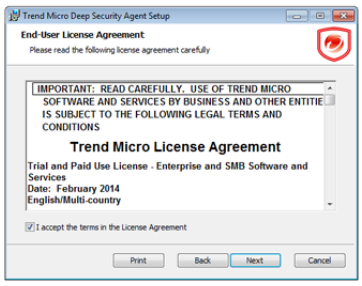
1. Copy the Agent installer file to the target machine and double-click the installation file to run the installer package. At the Welcome screen, click **Next** to begin the installation.

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`

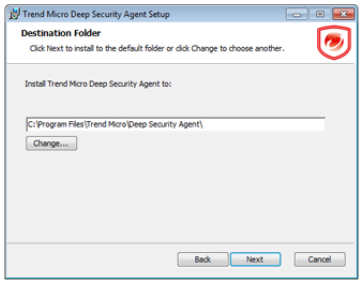
Note:	*When installing the Agent on Windows 2012 Server Core, the Notifier will not be included.*



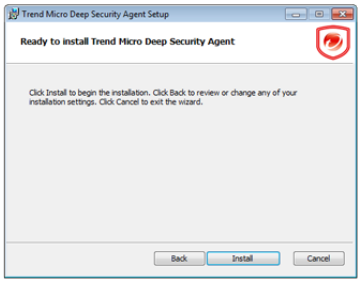
2. **End-User License Agreement:** If you agree to the terms of the license agreement, select **I accept the terms of the license agreement** and click **Next**.



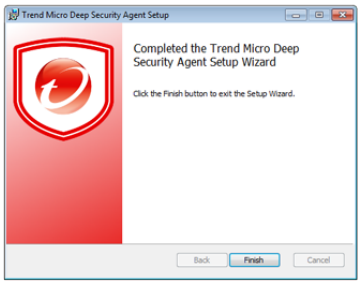
3. **Destination Folder:** Select the location where you would like Deep Security Agent to be installed and click **Next**.



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:

- Agent-Solaris_5.10_U7-9.0.0-xxxx.sparc.pkg
- Agent-Solaris_5.10_U5-9.0.0-xxxx.sparc.pkg

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:

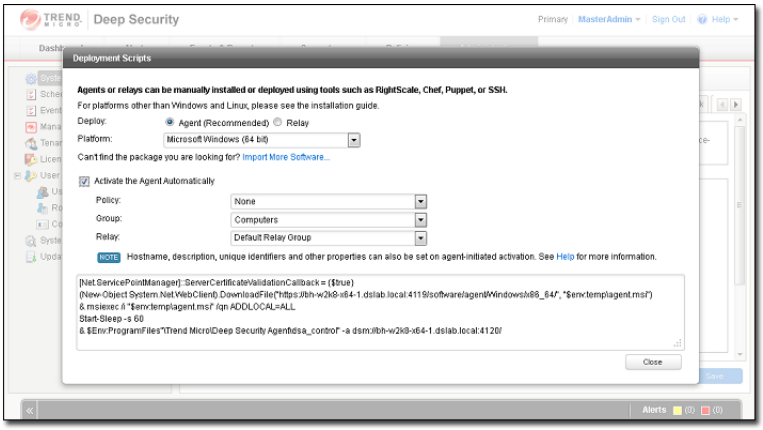
1. Start the Deployment Script generator by clicking **Deployment Scripts...** from the Deep Security Manager's Support menu (at the top right of the Deep Security Manager window).
2. Select the platform to which you are deploying the software.

   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

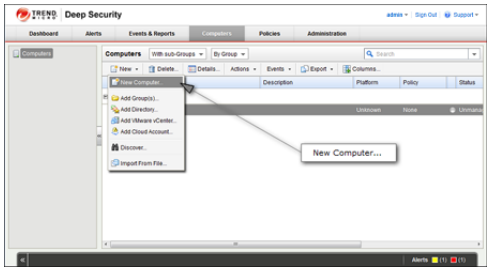
Deep Security 9.5 or later does not disable Linux iptables during installation. If the Firewall or Instrusion Prevention modules are enabled, iptables is disabled. If the Agent is disabled, iptables is enabled and the settings are reverted. For instructions on how to prevent the Deep Security Agent from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

Activating the Agent

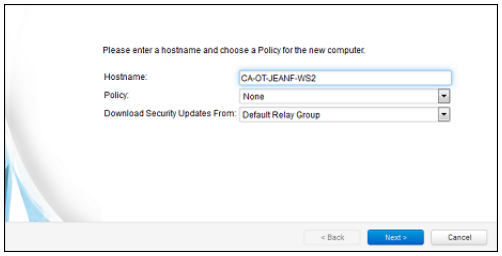
The Agent must be activated from the Deep Security Manager before it can be configured to act as a Relay or to protect the host computer.

To activate the newly installed Agent:

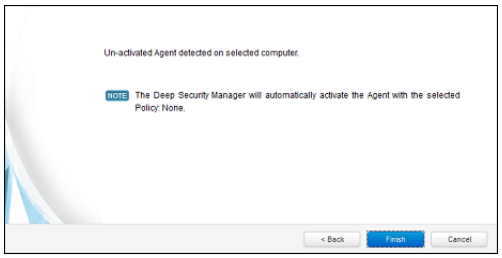
1. In the Deep Security Manager, go to the Computers page and click **New > New Computer...** to display the **New Computer Wizard**.



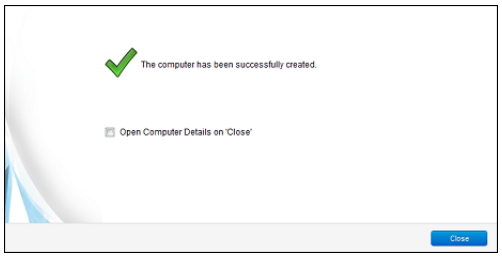
2. Enter the hostname or IP address of the computer. If you want to use the Agent to provide protection for the host computer as well as function as a Relay, select a Deep Security Policy from the **Policy** menu. Otherwise leave **Policy** set to "None".



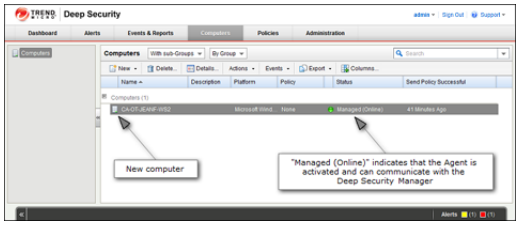
3. The wizard will confirm that it will activate the Agent on the computer and apply a Security Policy (if one was selected).



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



5. 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)".



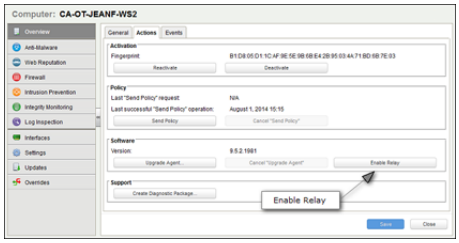
Enabling Relay Functionality

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

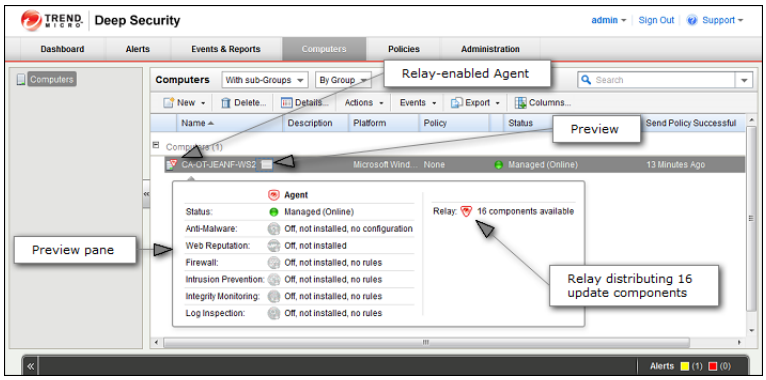
Note:	*Once enabled on an Agent, Relay functionality cannot be disabled.*

To enable Relay functionality:

1. 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.
2. In the computer editor, go to the **Overview > Actions > Software** area and click **Enable Relay**. Click **Close** close the editor window.



3. 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 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.

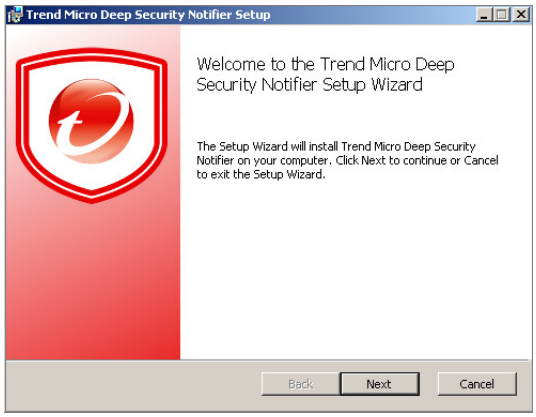
Copy the Installation Package

Copy the installation file to the target machine.

Installing the Deep Security Notifier for Windows

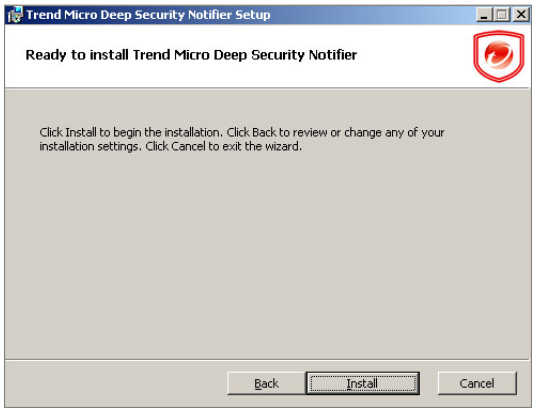
Note: *Remember that you must have administrator privileges to install and run the Deep Security Notifier on Windows machines.*

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

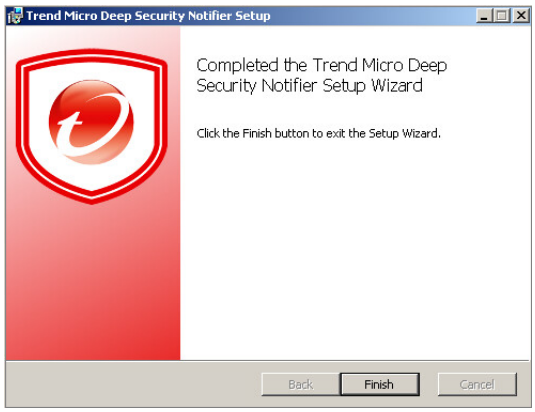


2. Read the license agreement and click **Next**.

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.*

Upgrading

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 existing Deep Security data, see "Database Backup and Recovery" in the Deep Security 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 27)***, 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 SP1.*

Upgrade to a version 9.6 SP1 Relay-Enabled Agent

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

Upgrade your 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, 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 Relay-enabled Agent to version 9.6 SP1:

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", located earlier in this guide.*

Upgrade the Deep Security Notifier

Note: *Upgrading the Deep Security Notifier is only required on virtual machines being protected Agentlessly by a Deep Security Virtual Appliance. On machines with an in-guest Agent, the Notifier will be upgraded along with the Deep Security Agent.*

To upgrade the Deep Security Notifier:

1. Uninstall the Deep Security Notifier that is currently installed
2. Install Deep Security Notifier 9.6 SP1 according to the procedures described in ***Installing the Deep Security Notifier (page 54)***.

Note: *The Deep Security Notifier must always be the same version as the Deep Security Manager.*

Appendices

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 "xxxx" 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 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.

Scan Caching

Scan Caching improves the efficiency of on-demand scans performed by the Virtual Appliance. It eliminates the unnecessary scanning of identical content across multiple VMs in large VMware deployments.

In addition,

- Integrity Monitoring scan caching speeds up Integrity Monitoring scans by sharing Integrity Monitoring scan results
- Anti-Malware on-demand caching speeds up scans on subsequent cloned/similar VMs
- Anti-Malware Real-time caching speeds up VM boot and application access time

- Concurrent Scan feature allows further overall scan time improvement by allowing multiple VMs to be scanned concurrently

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 67)***.

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=xxxxxxxx
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
```

Upgrade Multi-Node Deep Security Manager

Upgrading a Multi-node Deep Security manager requires no special preparation.

To upgrade a Multi-node Manager:

1. Run the Deep Security Manager install package on any node.
   The installer will instruct the other nodes to shut down (there is no need to manually shut down the services).
   The installer will upgrade the local Deep Security Manager and update the database.
2. Run the Deep Security Manager installer on the remaining nodes.
   As each node is upgraded, the service will restart and the node will rejoin the network of Deep Security Managers.

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 64)***.)

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.ProxyAunthentication=<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.ProxyAunthentication=<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 exampe 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=xxxxxxxx
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...
```

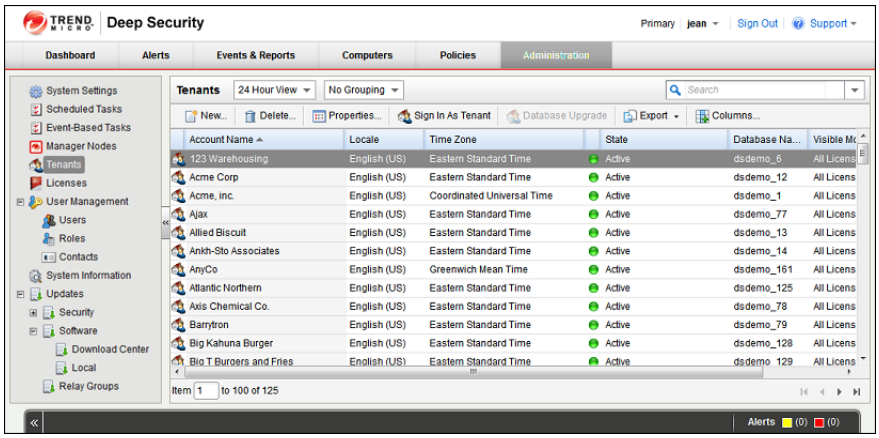
Enable Multi-Tenancy

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.



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://managername: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://managername:4119/SignIn.screen?tenantAccount=AnyCo&username=admin
```

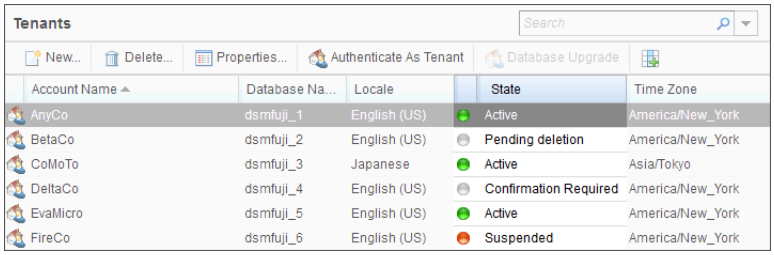
Email Generated Password: Password Notification

```
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**:

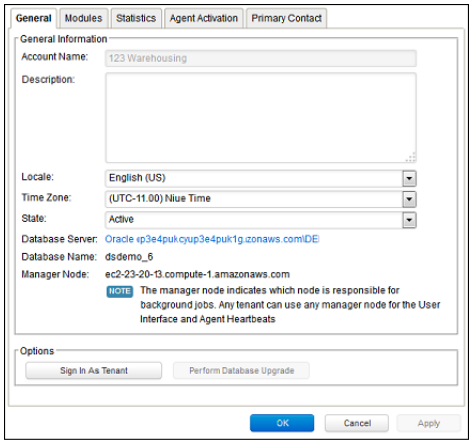


- **Created:** In the progress of being created but not yet active
- **Confirmation Required:** Created, but the activation link in the confirmation email sent to the Tenant User has not yet been clicked. (You can manually override this state.)
- **Active:** Fully online and managed
- **Suspended:** 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.

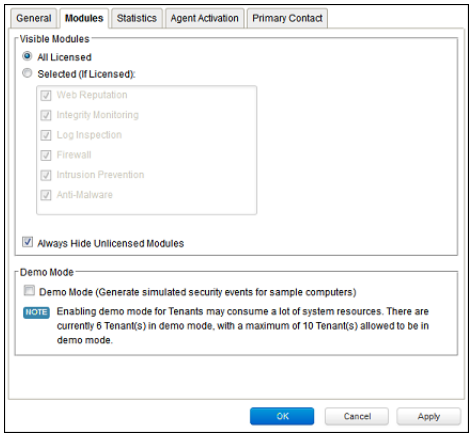
General



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.

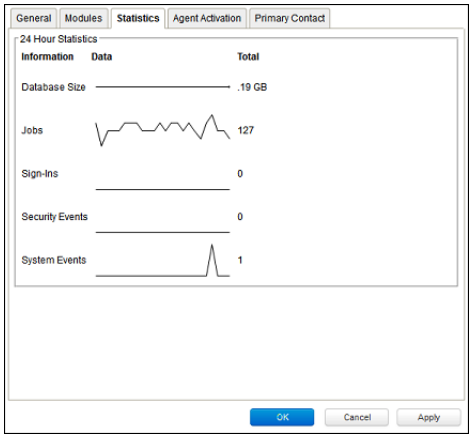
If using the "Per Tenant" licensing by default only the licensed modules for each Tenant will be visible.

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.

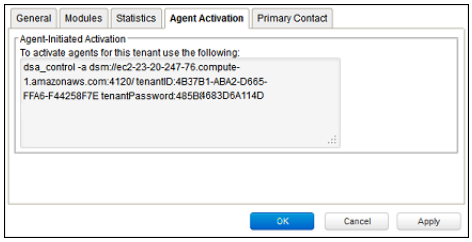
*Demo Mode is **not** intended to be used in a production environment!*

Statistics



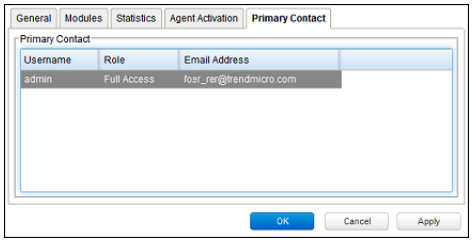
The statistics tab shows information for the current Tenant including database size, jobs processed, logins, security events and system events. The small graphs show the last 24 hours of activity.

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



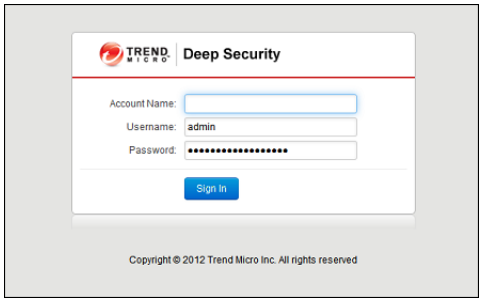
Relay-enabled Agents

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.

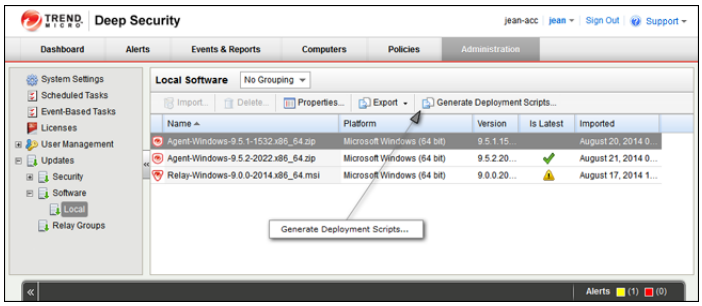
All Tenants have the ability to use Role-Based Access Control with multiple user accounts to further sub-divide access. Additionally they can use Active Directory integration for users to delegate the authentication to the domain. The Tenant Account Name is still required for any Tenant authentications.

Agent-Initiated Activation

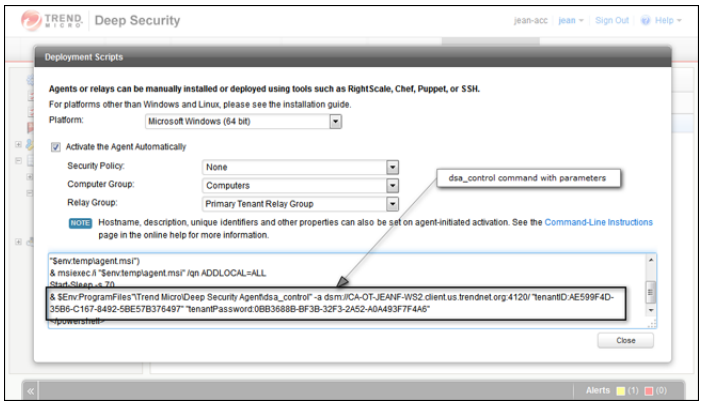
Agent-initiated activation is enabled by default for all Tenants.

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.

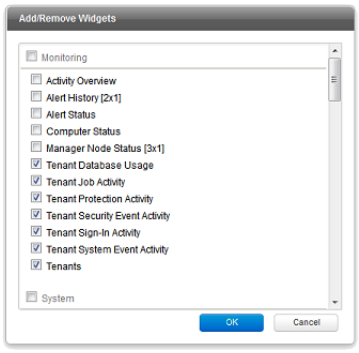
Usage Monitoring

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 enabled or disabled by going to **Administration > System Settings > Advanced > Status Monitoring API**.

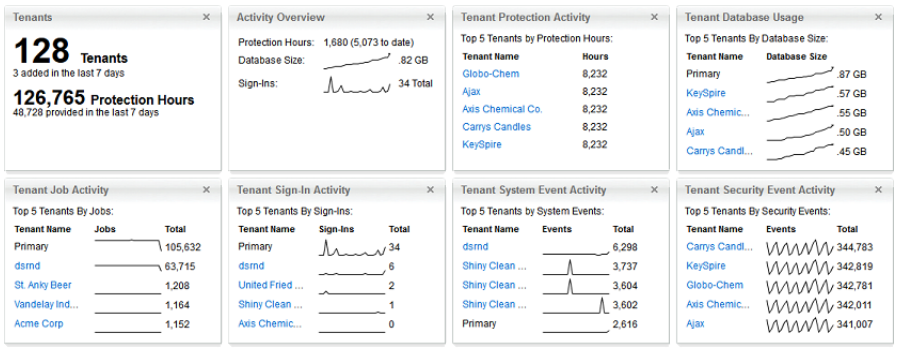
This chargeback (or viewback) information can be customized to determine what attributes are included in the record. This configuration is designed to accommodate various charging models that may be required in service provider environments. For enterprises this may be useful to determine the usage by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

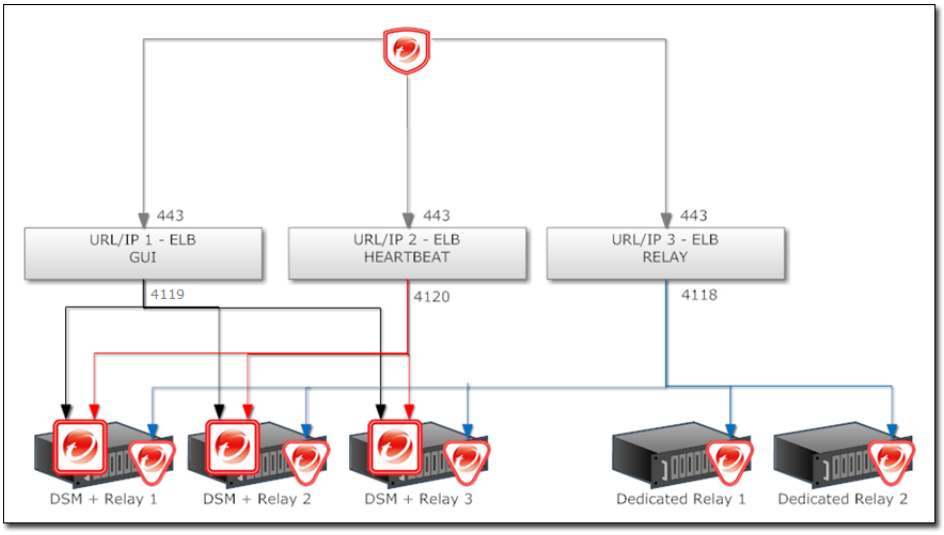
to direct the setting change or other command line action at a specific Tenant. If omitted the action is on the primary Tenant.

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.

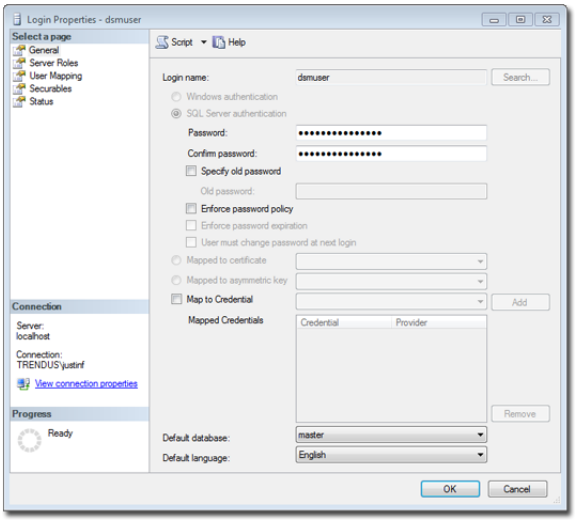
	SQL Server	**Oracle Database**
Process where multiple Tenants execute	Database Server	Database
One Tenant's set of data	Database	Tablespace/User

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

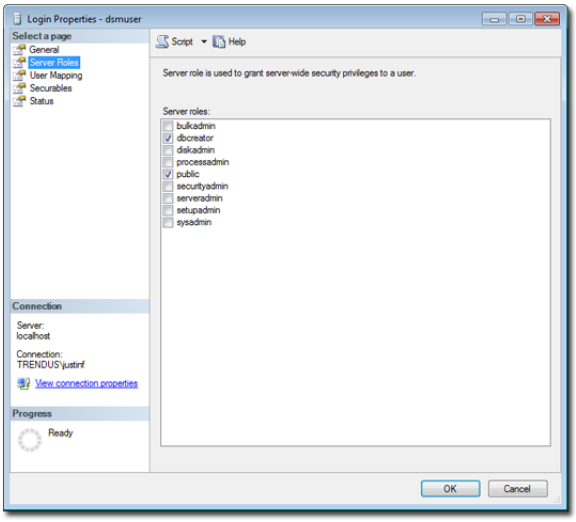
SQL Server

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.)*

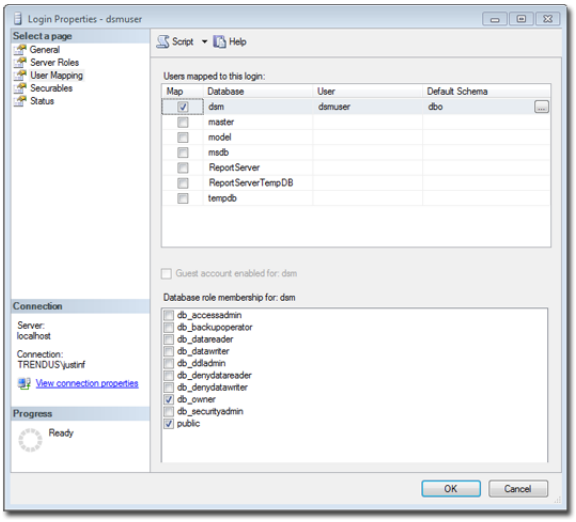
Since Multi-Tenancy requires the ability for the software to create databases, the **dbcreator** role is required on SQL Server. For example:



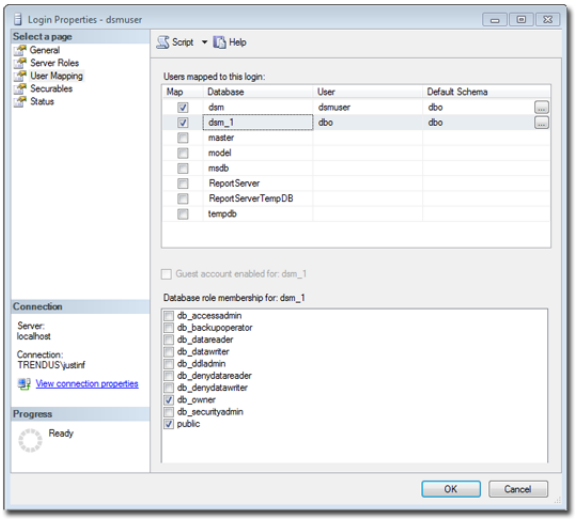
For the user role of the primary Tenant it is important to assign DB owner to the main database:



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*

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

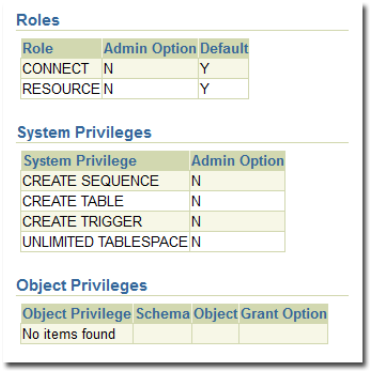
System Privileges

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.

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=dsmserver
   ```

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, **cacert.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)

13. 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
    ```

14. 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
    ```

15. Copy the .keystore file from your user home directory **C:\Documents and Settings\Administrator** to **C:\Program Files\ Trend Micro \Deep Security Manager**
16. 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
    ```

    Note: *The AWS Marketplace version of Deep Security Manager uses port 443 instead of 4119.*

17. Replace the password in the following string:

    ```
    keystorePass=xxxx
    ```

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

18. Save and close the file.
19. Restart the Deep Security Manager service.
20. 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:

1. 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**.
2. Copy **.keystore** and **configuration.properties** to the newly created folder **Backupkeystore**.
3. From a command prompt, go to the following location: **opt\dsm\jre\bin** .
4. Run the following command, which will create a self-signed certificate:

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

    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 **./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.

Uninstalling Deep Security

Note: *When you uninstall an activated Agent or a Relay-enabled Agent from a managed computer, the Deep Security Manager does not know that the software has been uninstalled. The computer will remain listed in the Computers list and its status will be listed as "Managed (Offline)" or something equivalent depending on the context. To avoid this, either deactivate the Agent or Relay-enabled Agent from the Manager before uninstallation, or simply delete the computer from the list.*

To uninstall the Relay-enabled Agent

Note: *Remember that before uninstalling a Relay-enabled Agent on Windows, you will need to remove the Agent Self Protection. You can do this from the Computer Editor in the Deep Security Manager. Go to* ***Settings > General****. In* ***Agent Self Protection****, either un-check the setting* ***Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent*** *or enter a password to be able to override this setting locally.*

To uninstall the Relay-enabled Agent (Windows)

From the Windows Control Panel, select Add/Remove Programs. Double-click Trend Micro Deep Security Agent from the list, and click Change/Remove.

To uninstall from the command line:

```
msiexec /x <package name including extension>
```

(For a silent uninstall, add "**/quiet**")

To uninstall the Relay-enabled Agent (Linux)

To completely remove the Relay-enabled Agent and any configuration files it created, use "rpm -e":

```
# rpm -ev ds_agent
Stopping ds_agent: [ OK ]
Unloading dsa_filter module [ OK ]
```

If iptables was enabled prior to the installation of the Relay-enabled Agent, it will be re-enabled when the Relay-enabled Agent is uninstalled.

Note: *Remember to remove the Relay-enabled Agent from Deep Security Manager's list of managed Computers, and to remove it from the Relay Group (see Basic Deep Security Configuration).*

To uninstall the Deep Security Agent

Note: *Remember that before uninstalling a Deep Security Agent on Windows, you will need to remove the Agent Self Protection. You can do this from the Computer Editor in the Deep Security Manager. Go to* ***Settings > General****. In* ***Agent Self Protection****, either un-check the setting* ***Prevent local end-users from uninstalling, stopping, or otherwise modifying the Agent*** *or select a password for local override.*

To uninstall the Deep Security Agent (Windows)

From the Windows Control Panel, select Add/Remove Programs. Double-click Trend Micro Deep Security Agent from the list, and click Change/Remove.

To uninstall from the command line:

```
msiexec /x <package name including extension>
```

(For a silent uninstall, add "**/quiet**")

To uninstall the Deep Security Agent (Linux)

To completely remove the Agent and any configuration files it created, use "rpm -e":

```
# rpm -ev ds_agent
Stopping ds_agent: [ OK ]
Unloading dsa_filter module [ OK ]
```

If iptables was enabled prior to the installation of the Deep Security Agent, it will be re-enabled when the Agent is uninstalled.

For Ubuntu:

```
$ sudo dpkg -r ds-agent
Removing ds-agent...
Stopping ds_agent: .[OK]
```

To uninstall the Deep Security Agent (Solaris 9 or 10)

Enter the following:

```
pkgrm ds-agent
```

(Note that uninstall may require a reboot.)

To uninstall the Deep Security Agent (Solaris 11)

Enter the following:

```
pkg uninstall ds-agent
```

(Note that uninstall may require a reboot.)

To uninstall the Deep Security Agent (AIX)

Enter the following:

```
installp -u ds_agent
```

To uninstall the Deep Security Agent (HP-UX)

Enter the following:

```
swremove ds_agent
```

To uninstall the Deep Security Notifier

To uninstall the Deep Security Notifier (Windows)

From the Windows Control Panel, select Add/Remove Programs. Double-click Trend Micro Deep Security Notifier from the list, and click Remove.

To uninstall from the command line:

```
msiexec /x <package name including extension>
```

(For a silent uninstall, add "**/quiet**")

To uninstall the Deep Security Manager

To uninstall the Deep Security Manager (Windows)

From the Windows Start Menu, select **Trend Micro > Trend Micro Deep Security Manager Uninstaller**, and follow the wizard steps to complete the uninstallation.

To initiate the same Windows GUI uninstall procedure from the command line, go to the installation folder and enter:

```
<installation folder>\Uninstall.exe
```

For a silent uninstall from the command line (without the Windows GUI prompts), add "**-q**":

```
<installation folder>\Uninstall.exe -q
```

Note:	*During a silent command line uninstallation, the uninstaller always saves the configuration files so that future installations can offer the repair / upgrade option.*

To uninstall the Deep Security Manager (Linux)

To uninstall from the command line, go to the installation folder and enter:

```
Uninstall
```

(For a silent uninstall, add "**-q**")

Note:	*During a command line uninstallation, the uninstaller always saves the configuration files so that future installations can offer the repair / upgrade option.*

If you selected "no" to keeping the configuration files during the uninstallation and want to reinstall the DSM, you should perform a manual clean-up before reinstalling. To remove the DSM installation directory enter the command:

```
rm -rf <installation location>
```

(The default installation location is "**/opt/dsm**").

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
Item Code: APEM97212/150921b