



9.0 Deep Security

SP1 Installation Guide

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

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

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

Document version: 1.0

Document number: APEM95862/130213

Release date: May 2013

Document generated: May 17, 2013 (8:10:22)

Table of Contents

Introduction	5
About Deep Security	6
What's New in Deep Security 9 SP1	10
Agent-Based Protection Models.....	14
Agentless Protection Models.....	16
Hybrid Protection Models	19
 Installation	 21
What you will Need.....	22
System Requirements.....	28
Preparing a VMware Environment for Agentless Protection.....	31
Install a Database for Deep Security	34
Installing a Database for Deep Security (Multi-Tenancy Requirements)	35
Install Deep Security Manager	39
Installing the Deep Security Relay	43
Preparing ESXi for Deep Security Virtual Appliance Deployment	46
Deploying the Deep Security Virtual Appliance	48
Automatically Deploying an Appliance for Stateless ESXi.....	51
Install Deep Security Agents.....	57
Installing the Deep Security Notifier.....	67
Enable Multi-Tenancy	68
Multi-Tenancy (Advanced)	78
Configure vCloud for Integration with Deep Security	81
Configure Amazon EC2 Resources for Integration with Deep Security.....	85
 Upgrading	 86
Upgrade Scenarios.....	87
Upgrading Deep Security 8.0 SP2 Software Components.....	88
Upgrading from DS 8.0 SP2 with Agentless Anti-Malware Protection (Includes upgrading ESX/ESXi 4.1 to 5.x).....	91
Upgrading from Deep Security 8.0 SP2 with Agentless FW and IPS Only (Upgrading from ESX/ESXi 4.1 to 5.x)	95
Upgrading from Deep Security 8.0 SP2 with In-guest Agent-Based Protection Only	98
Upgrade Deep Security Agents	99
Upgrade the Deep Security Notifier.....	100

Quick Start	101
Quick Start: System Configuration	102
Quick Start: Protecting a Server.....	110
Import Deep Security Software.....	119
Configuring the Deep Security Relay	121
 Appendices	 123
Supported Features by Platform.....	124
Deep Security Manager Settings Properties File.....	126
Deep Security Manager Memory Usage	133
Deep Security Virtual Appliance Memory Usage	134
Performance Features	135
Creating an SSL Authentication Certificate	137
Minimum VMware Privileges for DSVa Deployment.....	140
Uninstalling Deep Security	143
Frequently Asked Questions	148
Troubleshooting.....	150

Introduction

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 in local mode.

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 in local mode. 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

Strengthens protection against web threats for servers and virtual desktops.

Integrates with the Trend Micro™ Smart Protection Network™ web reputation capabilities to safeguard users and applications by blocking access to malicious urls. Provides same capability in virtual environments in agentless mode through the same virtual appliance that also delivers agentless security technologies for greater security without added footprint.

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. Now available in agentless form factor.

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, Web Reputation Service, Firewall, Intrusion Prevention, and Integrity Monitoring protection to virtual machines.
- **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.
- **Deep Security Relay**: The Deep Security Relay delivers Security Updates to the Agents and Virtual Appliances. (The Relay has an embedded Agent to provide local protection on its host machine.)
- **Deep Security Notifier**: The 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 Deep Security Relays, 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, and has a web services API for integration with datacenter automation environments.

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, with drill-down capabilities
- Graphs of key metrics with trends, with drill-down
- Detailed event logs, with drill-down
- 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 ESX 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.

Deep Security Relay

The Deep Security Relay is a server which relays Deep Security Updates from the Trend Micro global update server to the Deep Security system. By using Relays you can improve performance by distributing the task of delivering updates to the Manager, Appliances, and Agents of your Deep Security installation.

Deep Security Notifier

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

What's New in Deep Security 9 SP1

Deep Security 9 SP1

Trusted Common Baseline

Trusted Common Baseline is a new method of auto-tagging Integrity Monitoring Events within a group of computers. Using this method, you can identify a group of computers that are known to be malware free and implement a set of Integrity Monitoring Rules on them. When changes to files are detected on any computers in the group, Deep Security will look for the presence of files with a matching signature on the other computers in the group. If a match is found, the Event associated with the changed file will be tagged.

Ability to Update Anti-Malware Patterns Without Updating Anti-Malware Engines

There is now an option to configure a Deep Security Relay Group to distribute only Anti-Malware Pattern updates and not the Anti-Malware engine software. The option can be found on a Relay Group's Properties window by going to the **Administration > System Settings > Updates** tab and clicking on **View Relay Group...** to display the Relay Groups window, then double-clicking on a Relay Group.

Supported Platforms

Deep Security 9 SP1 supports some additional platforms including Solaris 11, HPUX, and AIX. For a list of currently supported platforms, see [System Requirements \(page 28\)](#).

Additional Language Support

The Deep Security Manager interface is now available in Japanese, Simplified Chinese, and English. As well as being able to set the default language at install time, each Deep Security User can set their user interface language individually. (To change a User's language setting, go to **Administration > User management > Users** and edit the **Properties** of the User account.)

The Deep Security Notifier is available in several additional languages, including German, French, Spanish, Italian, Russian, Japanese, Korean, Simplified Chinese, Traditional Chinese. The display language is determined by the locale settings of the computer on which the Notifier is installed.

Performance Improvements and Bug Fixes

Deep Security 9 SP1 includes a number of performance improvements and the resolution of some known issues. For a description of these, please see the accompanying release notes.

Deep Security 9

Multi-Tenancy

Multi-Tenancy lets you create independent installations of Deep Security within your enterprise. You can create Deep Security Tenancies for individual departments or lines of business within your organization. Each Tenant has access to all the functionality of Deep Security except core system settings. Tenants can be made responsible for the creation and management their own assets, Users, Policies and Rules independently of other Tenants. No Tenant's assets or security components are visible to any other Tenants. Each Tenancy is independent and isolated from every other Tenancy.

Multi-Level Policy Inheritance

Deep Security now supports multiple levels of policy inheritance. A newly created policy can be configured to inherit all or some of its settings from a parent policy. This lets you create a tree structure of security policies which get progressively more granular and detailed. For example, you can create a parent policy called "Windows Server" and two child policies, "Windows Server 2008" and "Windows Server 2003", which inherit from their parent policy. Each of those child policies can in turn have child policies of their own for different editions of Windows Server:



Child Policies can inherit all their settings from their parent Policy, or specific settings can be overridden.

Protection of Virtual Machines deployed on VMware vCloud and Amazon EC2 Infrastructure

Deep Security now provides support for virtual machines deployed in VMware vCloud and Amazon EC2 environments. This support includes:

- Discovery and synchronization of virtual datacenter organizational views or provider based virtual datacenter views.
- Identification and management of VM instances in the cloud environment.
- Activation and Policy assignment for VMs in the cloud environment and their clones to enable auto-scaling.
- Service catalog support in the vCloud Director.
- Dashboard/Alerts/reporting based on a Tenant's particular vDataCenter configuration.

Improved performance and efficiency of Malware scans in both Agent-based and Agentless environments

On Windows Agents, the Quick Scan option carries out a fast high level scan of areas that are most commonly at risk of infection. In Agentless environments, Malware scanning has been optimized to prevent multiple scans of resources shared across virtual machines.

Full IPv6 Support

IPv6 is now supported by the Deep Security Firewall and Intrusion Prevention modules. Existing Rules will be applied to both IPv4 and IPv6 traffic. New Rules can be created that apply to IPv4 or IPv6 specifically, or both.

Agentless Recommendation Scans

Recommendations Scans can now be performed on virtual machines being protected by a Deep Security Virtual Appliance. Intrusion Prevention and Integrity Monitoring Rules can be automatically assigned based on the result of a recommendation scan and Firewall Rules can be automatically assigned based on the result of a scan for open ports.

Improvements to the automation of Agent installation, activation, and Policy assignment

Scripting support has been added to Deep Security to allow the automated deployment and activation of Agents. Upon activation, Agents can automatically run a recommendation scan and assign Rules based on the results.

Improved control of Event-based Tasks for discovered assets.

Tasks such as Policy, Rule, and Group assignment can be automatically carried out on newly discovered assets based on their hostnames, IPs, Tenancy ID, Tenancy Template, Instance Type, or other cloud asset properties.

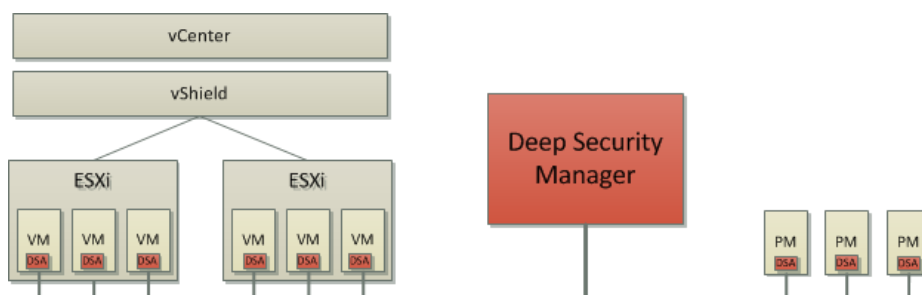
Support for VMware Trusted Platform Module (TPM) on ESXi.

VMware TPM is a hardware-based encryption module attached to an ESX/ESXi which creates a signature of data logged during the ESX boot sequence. A change to the TPM signature indicates that the ESX boot sequence has changed which could represent an attack (a change that replaces or alters a critical component in the hypervisor). The Deep Security Integrity Monitoring module is able to monitor TPM signatures and raise Alerts if changes are detected.

Agent-Based Protection Models

Single-Tenant installation

The following diagram illustrates a single Deep Security Manager managing three physical machines and six virtual machines in a VMware vCenter. The vCenter has not been imported into the Deep Security Manager. All the computers have been added to the Deep Security manager from the local network. They are all being protected by in-guest Agents.

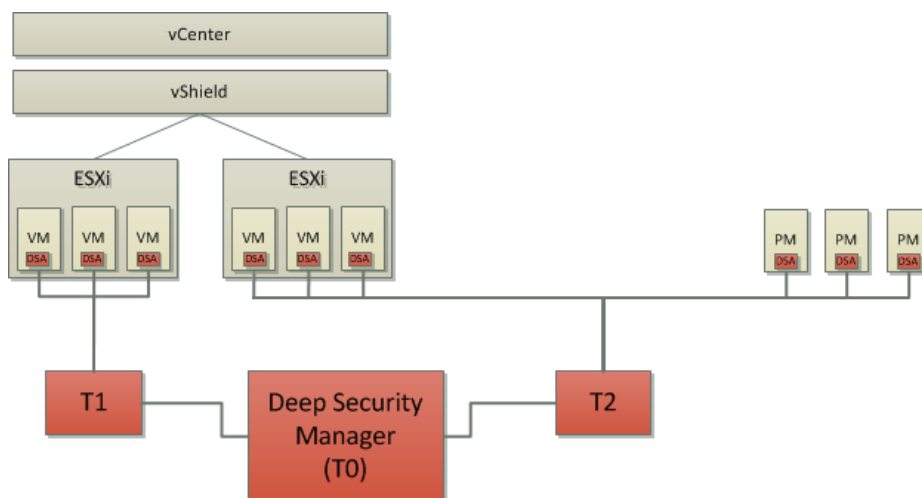


To implement this Agent-based protection model:

1. Review [What you will Need \(page 22\)](#) and [System Requirements \(page 28\)](#) information.
2. [Install a Database for Deep Security \(page 34\)](#)
3. [Install Deep Security Manager \(page 39\)](#)
4. [Install a Deep Security Relay \(page 43\)](#)
5. [Install Deep Security Agents \(page 57\)](#)
6. Enable Protection on your virtual machines. See [Quick Start: Protecting a Server \(page 110\)](#).

Multi-Tenancy installation with Agent-Based Protection

The following diagram illustrates multiple Deep Security Manager Tenants managing physical and virtual machines. The VMs have been imported into the Tenant's Deep Security Managers independently of the vCenter and all computers are being protected by in-guest Agents.



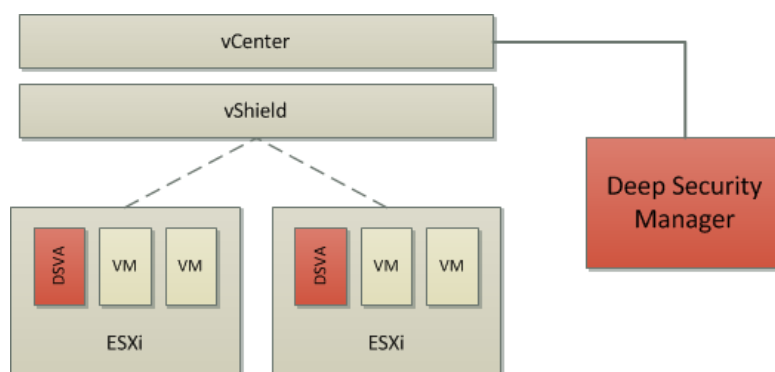
To implement this Agent-based protection model:

1. Review [What you will Need \(page 22\)](#) and [System Requirements \(page 28\)](#) information.
2. [Install a Database for Deep Security \(page 34\)](#)
3. [Install Deep Security Manager \(page 39\)](#)
4. [Enable Multi-Tenancy \(page 68\)](#)
5. [Install a Deep Security Relay \(page 43\)](#)
6. [Install Deep Security Agents \(page 57\)](#)
7. Tenants must enable protection on their managed computers. See [Quick Start: Protecting a Server \(page 110\)](#).

Agentless Protection Models

Single-Tenant installation with VMware vCenter

The following diagram illustrates a Deep Security Manager managing the virtual machines in a VMware vCenter.



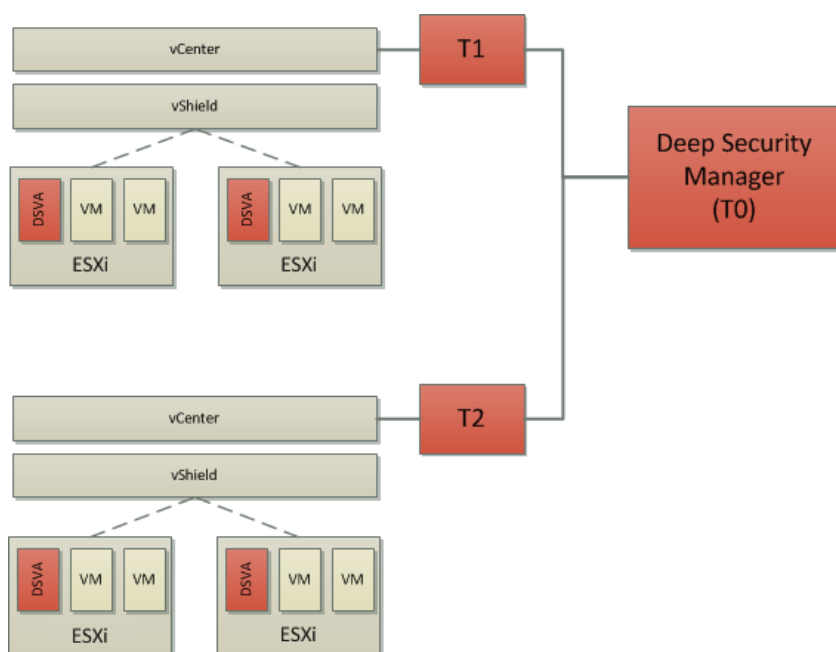
The vCenter has been imported into the Deep Security Manager and the VMs are being protected Agentlessly by the Deep Security Virtual Appliances (DSVAs) running on each ESXi. Deep Security Manager is deployed without Multi-Tenancy, and a single Deep Security Manager has been used to prepare and activate the DSVAs on the ESXi and to activate the VMs.

To implement this Agentless protection model:

1. Review [What you will Need \(page 22\)](#) and [System Requirements \(page 28\)](#) information.
2. [Prepare a VMware Environment for Agentless Protection \(page 31\)](#)
3. Deploy the Deep Security environment
 1. [Install a Database for Deep Security \(page 34\)](#)
 2. [Install Deep Security Manager \(page 39\)](#)
 3. [Install the Deep Security Relay \(page 43\)](#)
 4. [Prepare ESXi for Deep Security Virtual Appliance Deployment \(page 46\)](#)
 5. [Deploy the Deep Security Virtual Appliance \(page 48\)](#)
 6. [Installing the Deep Security Notifier \(page 67\)](#)
4. Enable Protection on your virtual machines. See [Quick Start: Protecting a Server \(page 110\)](#).

Multi-Tenancy installation with VMware vCenter

The following diagram illustrates a Multi-Tenancy Deep Security installation where Multi-Tenancy has been enabled, and each Tenant has imported a vCenter into their Deep Security Manager and are in full control of the vCenter including the management of DSVAs on the host ESXi's.



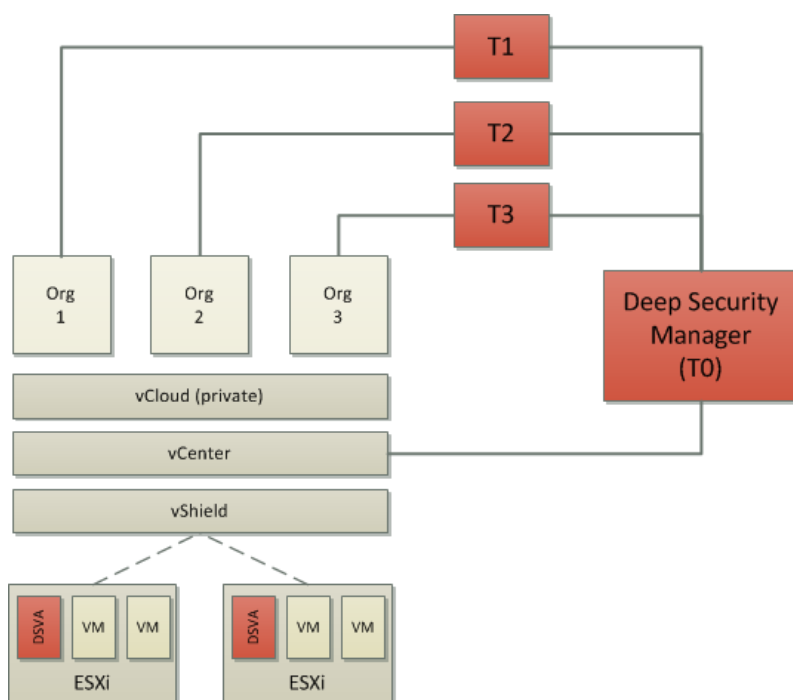
In this diagram the Deep Security Manager has Multi-Tenancy enabled but the primary Tenant T0 has not imported a vCenter. The vCenters have been imported by the T1 and T2 Deep Security Tenants.

To implement this Agentless protection model:

1. Review [What you will Need \(page 22\)](#) and [System Requirements \(page 28\)](#) information.
2. [Prepare a VMware Environment for Agentless Protection \(page 31\)](#)
3. Deploy the Deep Security environment
 1. [Install a Database for Deep Security \(page 34\)](#)
 2. [Install Deep Security Manager \(page 39\)](#)
 3. [Enable Multi-Tenancy \(page 68\)](#)
 4. [Install the Deep Security Relay \(page 43\)](#)
 5. [Prepare ESXi for Deep Security Virtual Appliance Deployment \(page 46\)](#)
 6. [Deploy the Deep Security Virtual Appliance \(page 48\)](#)
 7. [Installing the Deep Security Notifier \(page 67\)](#)
4. Enable Protection on your virtual machines. See [Quick Start: Protecting a Server \(page 110\)](#).

Multi-Tenancy installation with VMware vCenter with Private vCloud

The following diagram illustrates a Multi-Tenancy installation in which Tenants have been given access to the VMs in a vCloud Organization.



In this situation, the Primary Deep Security Tenant, T0, manages the vCenter and the deployment and management of DSVAs. The Tenants are not managing the DSVAs on the host ESXi's. In their Deep Security manager consoles, they see the VMs in the vCloud Organization which they've added as a "Cloud Account" but not the ESXi hosts or the DSVAs. The VMs to be protected in the vCloud Organization are activated and their protection is managed by the Tenants.

To implement this Agentless protection model:

1. Review [What you will Need \(page 22\)](#) and [System Requirements \(page 28\)](#) information.
2. [Prepare a VMware Environment for Agentless Protection \(page 31\)](#)
3. [Integrate Deep Security with VMware vCloud \(page 81\)](#)
4. Deploy the Deep Security environment
 1. [Install a Database for Deep Security \(page 34\)](#)
 2. [Install Deep Security Manager \(page 39\)](#)
 3. [Enable Multi-Tenancy \(page 68\)](#)
 4. [Install the Deep Security Relay \(page 43\)](#)
 5. [Prepare ESXi for Deep Security Virtual Appliance Deployment \(page 46\)](#)
 6. [Deploy the Deep Security Virtual Appliance \(page 48\)](#)
 7. [Configure vCloud for Integration with Deep Security \(page 81\)](#)
 8. [Install the Deep Security Notifier \(page 67\)](#)
5. Enable Protection on your virtual machines. See [Quick Start: Protecting a Server \(page 110\)](#).

Hybrid Protection Models

Multi-Tenancy installation in hybrid environment (VMware vCenter with vCloud private cloud, Amazon and vCloud public clouds)

The following diagram illustrates a Multi-Tenancy installation of Deep Security in a hybrid environment in which the Tenants in a single Deep Security installation are managing the security of a variety of resources.

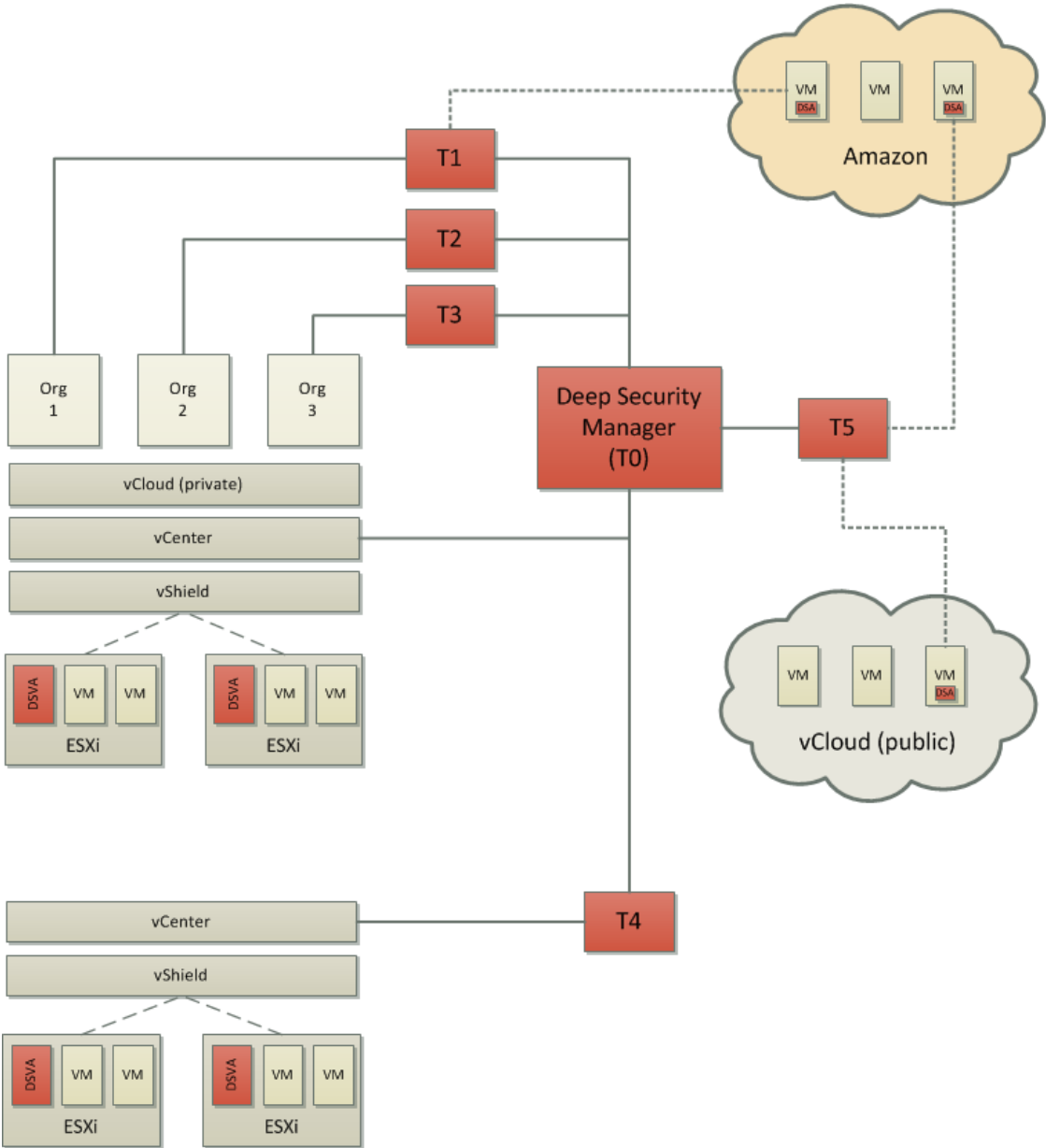
Tenant T1 is managing the security of the VMs in **Org 1** of a private vCloud (which are being protected agentlessly by the DSVA, managed by Primary user **T0**, installed on the ESXi hosting the VM in the private vCenter), and a VM from a public Amazon cloud account (which is protected by an Agent installed and managed by **Tenant T1**).

Tenants T2 and T3 are managing the security of the VMs in **Org 2** and **Org 3** of a private vCloud, which are being protected agentlessly by the DSVA, managed by Primary user **T0**, installed on the ESXi hosting the VM in the private vCenter.

Tenant T4 is managing the security the VMs from a second vCenter. T4 has imported the vCenter and is managing the deployment of the DSVA on the host ESXi's as well as the security of the VMs.

Tenant T5 is only managing the security of VM from public clouds.

To implement any of the sections of this hybrid model, see [Agentless Protection Models \(page 16\)](#) and [Agent-Based Protection Models \(page 14\)](#).



Installation

What you will Need

This section describes what you will need for a successful Deep Security Deployment

Deep Security Installer Packages

There are Deep Security Agent packages available for several types of operating systems. Download a Deep Security Agent install package for each type of computer that you need to protect.

Place the install packages for the Deep Security Manager, the Deep Security Relay, the Deep Security Virtual Appliance, and the Deep Security Filter Driver in the same folder from which you will run the Deep Security Manager installer. This way the Deep Security Manager will automatically import the Relays, Agents, Virtual Appliance, and the Filter Driver during installation. (If the Deep Security manager finds a Relay in the folder, it will offer you the option of installing a Relay along with 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.)

Administrator/Root Privileges

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

Available Ports

On the Deep Security Manager Host Machine

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 4119:** Used by your browser to connect to Deep Security Manager. Also used for communication from ESXi and requests for Security Updates by the DSVa (configurable).
- **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 Manager and Amazon AWS.

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

On the Deep Security Relay, Agents, and Appliances

You must make sure the following ports on the machine hosting Deep Security Relay 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 Deep Security Relays, Agents and Appliances.

Network Communication

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

The following guidelines provide a general idea of the infrastructure requirements for Deep Security deployments of different scales.

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.

Multiple Deep Security Manager Nodes

You may want to prepare more than one machine for Deep Security Manager installation. In a production environment, multiple Deep Security Manager nodes connected to a single database can be set up to provide load balancing and recovery services.

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: dedicated, co-located servers. A two millisecond latency or better is recommended for the connection from the Manager(s) to the Database.

Note: *It is a good idea to run multiple Manager Nodes for redundancy reasons, whether you have 1000 managed computers or not.*

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 host. 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 host, 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. For more information, see the **Event-Based Tasks** sections of the online help or the Administrator's Guide.*

Multi-Tenancy

Multi-Tenancy lets you create multiple distinct management environments using a single Deep Security Manager and database server installation. It fully isolates the settings, Policies, and Events for each Tenant and makes use of a number of additional infrastructure scaling options.

Multi-Tenancy was designed to provide segmentation for business units within an organization and facilitate testing in staging environments prior to full production deployments. It also allows the provision of Deep Security to customers within a service model.

When the Deep Security Manager is first installed, it is the one-and-only Tenant. After activating multi-tenancy, the initial Deep Security Manager becomes the "Primary Tenant" (T0). You can subsequently create additional Tenants but the Primary Tenant remains special. It manages and has control over the other tenants and can't be deleted. (See [Multi-Tenancy \(page 68\)](#) for more information.)

The requirements for Deep Security Multi-Tenancy are:

- Deep Security Manager 9
- Oracle Database or Microsoft SQL Server
- The necessary database account privileges for database create/delete operations. (See [Installing a Database for Deep Security \(Multi-Tenancy Requirements\) \(page 35\)](#).)
- Multi-Tenant Activation Code

Optional but recommended:

- Multi-node Manager (more than one Deep Security Manager node pointed to the same database for scalability)
- SMTP server

Architecture

***Note:** In SQL Server the data store for a Tenant is called a "database". In Oracle, the term is "User/ Tablespace". This section uses the term "database" but the information applies to both SQL Server and Oracle.*

Multi-Tenancy in Deep Security Manager operates similarly to a hypervisor. Multiple Tenants exist within the same Deep Security Manager installation but their data is highly isolated. Any Manager node can process the GUI, Heartbeat or any other job requests for any Tenant. For the background processing, each Tenant is assigned a Manager node that takes care of job-queuing, maintenance and other background tasks. The assigned Manager node is automatically rebalanced when Manager nodes are added or taken offline. The majority of each Tenant's data is stored in a separated database. This database may co-exist on the same database server as other Tenants, or can be isolated onto its own database server. In all cases, some data only exists in the primary database (the one Deep Security Manager was installed with). When multiple database servers are available, Tenants are created on the database server with the least amount of load.

The following table describes the potential capacities and ranges of requirements for Single Tenant and Multi-Tenant Deep Security deployments:

	Single Tenant	Multi-Tenant
Recommended maximum number of managed computers	100,000	1,000,000
Potential number of Deep Security Manager Nodes required	1-5	1-50
Databases/Tenants	1	1-10,000
Potential number of database servers required	1 (With or without replication)	1-100

Once Multi-Tenancy has been enabled, the Primary Tenant retains all of the capabilities of a regular installation of Deep Security Manager. However, subsequently created Tenants can have their access to Deep Security functionality restricted to varying degrees based on various configuration options set in **Administration** section of the Primary Tenant's Deep Security Manager.

The segmentation of each Tenant's data into a database provides additional benefits:

- **Data destruction:** Deleting a Tenant removes all traces of that Tenants data (Supported in the product)

- **Backup:** Each Tenant's data can be subject to different backup policies. This may be useful for something like tenancy being used for staging and production where the staging environment requires less stringent backups (Backups are the responsibility of the administrator setting up Deep Security Manager)
- **Balancing:** The potential for future re-balancing to maintain an even load on all database servers

System Requirements

Deep Security Manager

- **Memory:** 8GB, which includes:
 - 4GB heap memory
 - 1.5GB JVM overhead
 - 2GB operating system overhead
- **Disk Space:** 1.5GB (5GB recommended)
- **Operating System:** Windows Server 2012 (64-bit), Windows Server 2008 (64-bit), Windows Server 2008 R2 (64-bit), Windows 2003 Server SP2 (64-bit), Red Hat Linux 5/6 (64-bit)
- **Database:** Oracle 11g, Oracle 10g, Microsoft SQL Server 2012 (All Service Packs), Microsoft SQL Server 2008 (All Service Packs)
- **Web Browser:** Firefox 16+, Internet Explorer 8.x, Internet Explorer 9.x, Internet Explorer 10.x, Chrome 23+, Safari 6+. (Cookies enabled.)

Support for Previous versions of the Deep Security Agent

Deep Security Manager 9 SP1 supports the following previous versions of the Deep Security Agent:

- **Deep Security Agent 7.5 SP4 +**
- **Deep Security Agent 8.0 SP1 +**
- **Deep Security Agent 9.x**

(Older versions of the Agents are not supported.)

Note: *If you are running Agents older than these versions, the Deep Security Manager will display a warning during the upgrade procedure.*

Deep Security Agent

- **Memory:**
 - **with Anti-Malware protection:** 512MB
 - **without Anti-Malware protection:** 128MB
- **Disk Space:** 500MB (1GB recommended with Anti-Malware protection enabled)
- **Windows:** Windows Server 2012 (64-bit), Windows 8 (32-bit and 64-bit), Windows 7 (32-bit and 64-bit), Windows Server 2008 R2 (64-bit), Windows Server 2008 (32-bit and 64-bit), Windows Vista (32-bit and 64-bit), 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), Windows Server 2003 R2 SP2 (32-bit and 64-bit), Windows XP (32-bit and 64-bit), Windows XP Embedded

- **Linux:** Red Hat 5 (32-bit and 64-bit), Red Hat 6 (32-bit and 64-bit), Oracle Linux 5 (32-bit and 64-bit), Oracle Linux 6 (32-bit and 64-bit), SuSE 10 (32-bit and 64-bit), SuSE 11 (32-bit and 64-bit), Ubuntu 10.04 LTS (64-bit), Ubuntu 12.04 LTS (64-bit), CentOS 5 (32-bit and 64-bit), CentOS 6 (32-bit and 64-bit), Amazon Linux (32-bit and 64-bit).
(Agent-based Anti-Malware is not supported on 32-bit versions of Linux)
- **Solaris:** Solaris 9, 10, 11 (64-bit Sparc), Solaris 10 and 11, (64-bit x86)
- **AIX:** AIX 5.3, 6.1 (The AIX Agents do not support Anti-Malware or Web Reputation Service protection.)
- **HP-UX:** 11i v3 (11.31) (The HP-UX Agents only support Integrity Monitoring and Log Inspection.)

***Note:** Windows Agents running on Windows XP or Windows 2003 will not function in an IPv6 environment.*

Deep Security Relay

- **Memory:** 512MB
- **Disk Space:** 500MB (1GB recommended with Anti-Malware protection enabled)
- **Windows:** Windows Server 2012 (64-bit), Windows 8 (32-bit and 64-bit), Windows 7 (32-bit and 64-bit), Windows Server 2008 (32-bit and 64-bit), Windows Server 2008 R2 (64-bit), Windows Vista (32-bit and 64-bit), Windows Server 2003 SP2 (32-bit and 64-bit), Windows Server 2003 R2 (32-bit and 64-bit), Windows XP (32-bit and 64-bit)
- **Linux:** Red Hat 5 (64-bit), Red Hat 6 (64-bit), CentOS 5 (64-bit), CentOS 6 (64-bit)

Deep Security Virtual Appliance

- **Memory:** 2GB (Memory requirements can vary depending on the number of VMs being protected.)
- **Disk Space:** 20GB
- **Operating System:** VMware vCenter 5.x, and ESXi 5.x

***Note:** For a list of which features are supported on versions 5.0 and 5.1, see [Supported Features by Platform \(page 124\)](#).*

- **Additional VMware Utilities:** VMware Tools, VMware vShield Manager 5.x, VMware vShield Endpoint Security 5.x (ESXi5 patch ESXi500-201109001 or later for vShield Endpoint Driver).
- **VMware Endpoint Protection supported guest platforms:** Windows Server 2008 (32-bit and 64-bit), Windows Server 2008 R2 (64-bit), Windows 7 (32-bit and 64-bit), Windows Vista (32-bit and 64-bit), Windows Server 2003 SP2 R2 (32-bit and 64-bit), Windows Server 2003 SP2 (32-bit and 64-bit), Windows XP SP2 (32-bit and 64-bit).

ESXi Requirements for the Deep Security Virtual Appliance

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

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

TPM hypervisor integrity monitoring requires ESXi 5.1, and is not supported on ESXi 5.0.

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

Deep Security Notifier System Requirements

- **Windows:** Windows Server 2012 (64-bit, non-core), Windows 8 (32-bit and 64-bit), Windows 7 (32-bit and 64-bit), Windows Server 2008 R2 (64-bit), Windows Server 2008 (32-bit and 64-bit), Windows Vista (32-bit and 64-bit), Windows Server 2003 SP2 (32-bit and 64-bit), Windows Server 2003 R2 SP2 (32-bit and 64-bit), Windows XP (32-bit and 64-bit)

***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.*

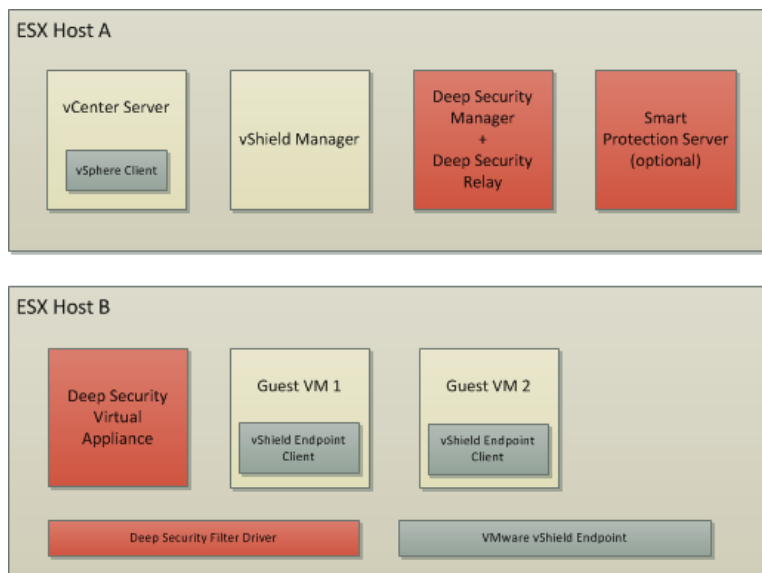
Preparing a VMware Environment for Agentless Protection

The following describes a Deep Security deployment in a typical VMware environment.

Two ESXi Hosts are required:

- **Host A:** is an ESXi hypervisor on which are running individual virtual machines (VMs) for Deep Security Manager 9.0, vShield Manager 5.x, and vCenter Server 5.x. Optionally, Trend Micro Smart Protection Server and Deep Security Relay can be installed on virtual machines on Host A. An additional virtual machine can also be provided for a second Deep Security Manager node. One VM should also be provided for installing the Deep Security Database.
- **Host B:** is an ESXi hypervisor on which are running Deep Security Virtual Appliance (DSVA) and the VMs requiring protection.

***Note:** The vCenter Server, the vShield Manager and the Deep Security Manager are installed on a separate ESXi because the protected ESXi must be restarted during the course of Deep Security deployment. Also note that the Deep Security database is not shown in this diagram. It also can be installed on a physical machine or on a VM.*



Required Resources Checklist

Check	Software Requirements	Notes
	VMware vCenter 5.x	Includes vCenter Server and vCenter Client GUI application. License is required during product installation.
	VMware vShield Manager 5.x	License is required during product installation.

Check	Software Requirements	Notes
	Trend Micro Deep Security Manager 9.0 (DSM)	License is required during product installation.
	VMware vShield Endpoint 5.x	Add the license to vCenter
	Trend Micro Deep Security Filter Driver 9.0 (FD)	
	Trend Micro Deep Security Virtual Appliance 9.0 (DSVA)	
	Supported Guest OS	vShield Endpoint drivers required on each guest VM. (Since ESXi 5 patch ESXi500-201109001, vShield Endpoint driver is included in VMware Tools).

Install vShield Endpoint on ESXi Host B

This section lists additional tasks necessary to complete the Deep Security integration with the VMware environment for Agentless protection.

At this point...

- The VMware Environment is already setup as described in Preparing a VMware Environment for Agentless Protection
- Deep Security Manager (and database) is already installed
- A Deep Security Relay has been installed and configured.

VMware vShield Endpoint Deployment on ESXi Host B

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 (Host B).
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**)

Install vShield Endpoint Drivers on the VMs to be protected on ESXi Host B

On each VM to be protected agentlessly by a Deep Security Virtual Appliance

1. Install guest OS. (If using Windows 2003 Server, make sure you install Service Pack 2)

2. Make sure the guest VM has a basic disk volume. Dynamic disks are not supported. (Note: The default installation of Windows 2003 has a basic disk volume.)
3. Install the VMware vShield Endpoint driver to this machine. The vShield Endpoint driver is contained within the vShield Drivers in VMware Tools. (Note that vShield Drivers are not installed by default during the installation of VMware Tools.)
 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.

Note: *If you plan to use manual or scheduled scans be sure to turn off sleep and standby mode on the guest virtual machines. If a guest virtual machine goes into sleep or standby mode during a scan you will see an error indicating that the scan terminated abnormally. Virtual Machines must be in the running state for scans to complete successfully.*

Note: *In a High Availability environment, you must install Deep Security Virtual Appliances on all the ESXi hypervisors in a cluster in order to provide Agentless protection for vMotioned guests.*

Install a Database for Deep Security

For Multi-Tenancy installations, see the additional requirements in [Installing a Database \(Multi-Tenancy Requirements\) \(page 35\)](#).

For enterprise deployments, Deep Security requires Microsoft SQL Server 2012 or 2008, or Oracle Database 11g or 10g. (Deep Security Manager comes with an embedded database (Apache Derby), which is only suitable for evaluation purposes.)

Note: You must install the database software, create a database, and create a user account (which Deep Security Manager will use to access the database) before you install Deep Security Manager.

Account Details

Make a note of the account details used in creation of your database instance as they will be required during the Deep Security Manager installation process.

Note: When creating a SQL Server database, the SQL Server account must be granted DB_Creator Server Roles and DB_Owner of the Deep Security Manager Database.

Note: When creating an Oracle database, the account must be assigned the roles of CONNECT and RESOURCE and the account must be granted privileges to CREATE TABLES, CREATE SEQUENCES, and CREATE TRIGGERS.

Deep Security Manager Communication with SQL Server

When using named pipes to connect to a SQL Server, a properly authenticated Microsoft Windows communication channel must be available between Deep Security Manager's 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, or
- 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.

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

Configuring Database User Accounts

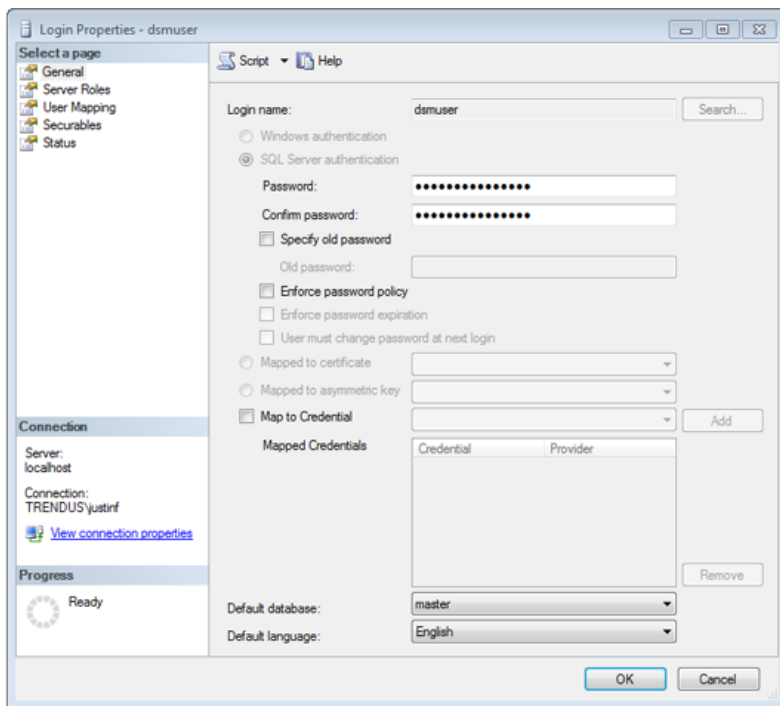
SQL Server and Oracle use different terms for database concepts described below.

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

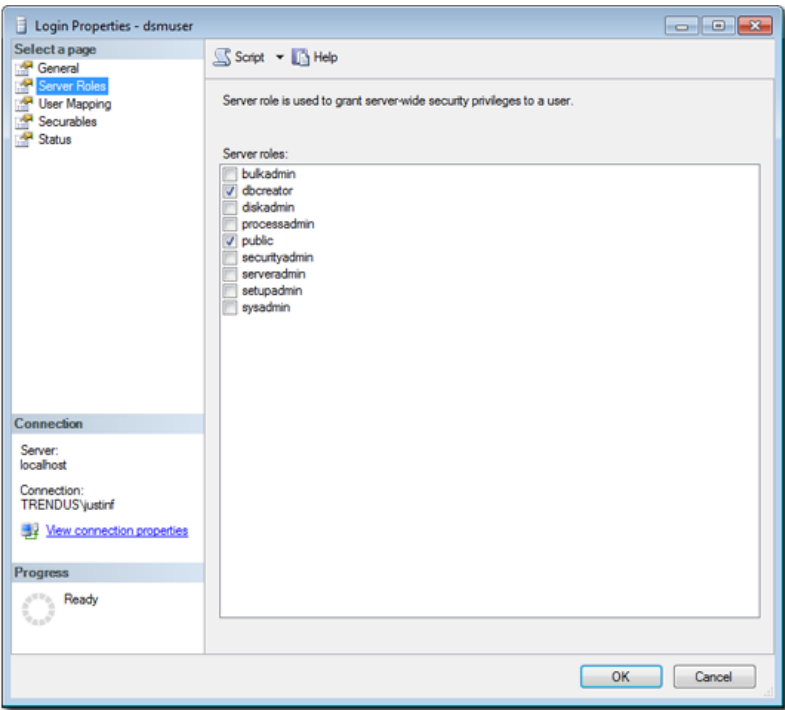
The following section uses the SQL Server terms for both SQL Server and Oracle.

SQL Server

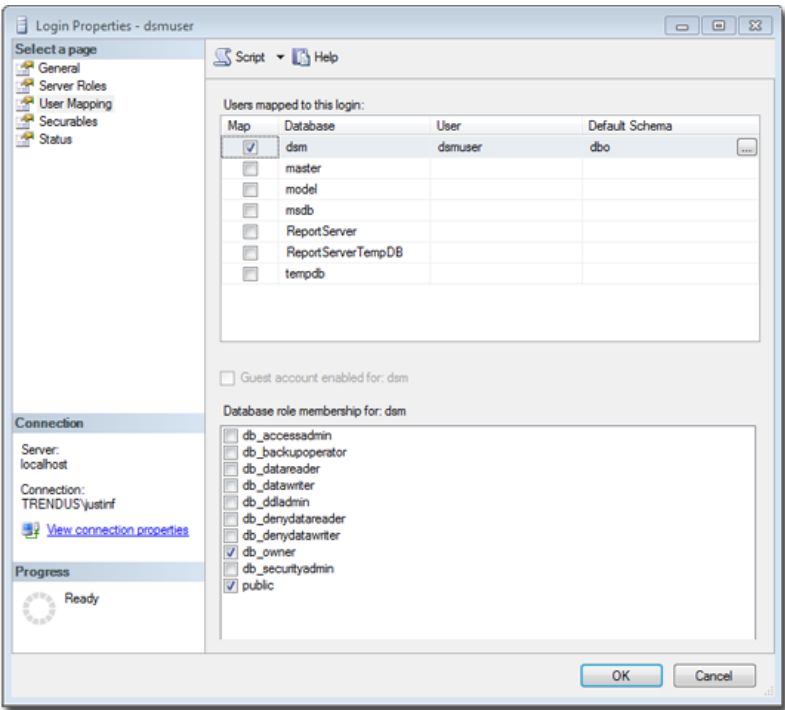
Since Multi-Tenancy requires the ability for the software to create databases, the **dbcreator** role is required on SQL Server. For example:



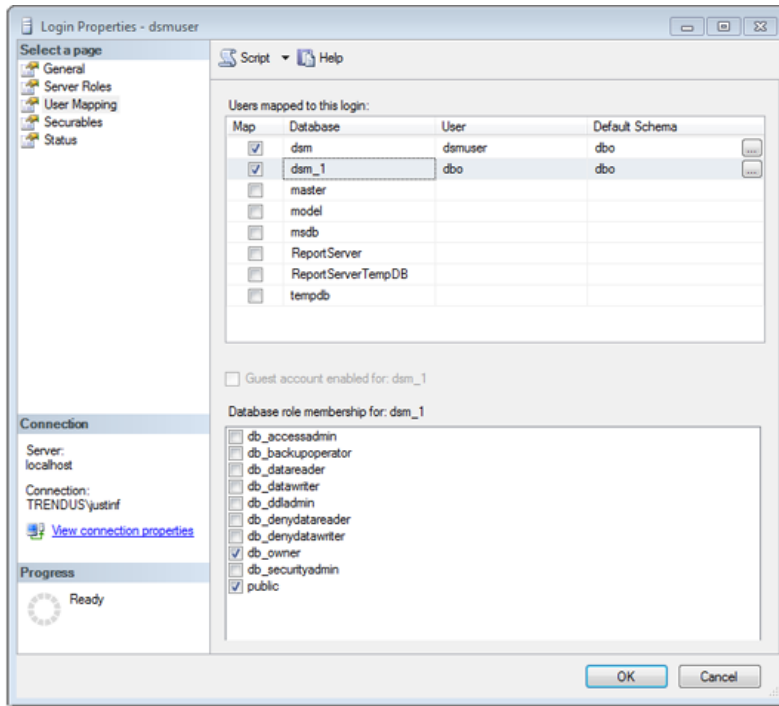
For the user role of the primary Tenant it is important to assign DB owner to the main database:



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

Multi-Tenancy in Oracle is similar to SQL Server but with a few important differences. Where SQL Server has a single user account per database server, Oracle 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/E11882_01/server.112/e10592/sql_elements008.htm

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 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 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.

Install Deep Security Manager

Copy the Installer Packages

Copy the appropriate Deep Security Manager installer and Deep Security Relay Installer to the target machine.

Note: *One or more Deep Security Relays are required for Deep Security functionality. If you intend to install a Deep Security Relay co-located on the Deep Security Manager's computer, you should copy a Deep Security Relay installer package to the same location as your Deep Security Manager installer package. During the Deep Security Manager installation, the installer checks for the Deep Security Relay package and if present and selected, will automatically continue with the Deep Security Relay installation once the Deep Security Manager has successfully installed.*

Installing the Deep Security Manager for Windows

Note: *If you are installing DSM in a vCenter where you plan to protect virtual machines, the DSM must not be installed on the same ESXi as the VMs you are planning to protect.*

Only install Deep Security Manager on the same ESXi hypervisor as one that is hosting the VMs you want to protect if that ESXi is part of an ESXi cluster. This is because installing the Deep Security Manager will force the ESXi to go into maintenance mode. If the ESXi is part of a cluster, the VMs, including the Deep Security Manager, will be vMotioned to another ESXi host during this process.

1. Start the Deep Security Manager installer by double-clicking the install package.
2. Select an installation language and click **OK** and **Next**.

Note: *After installation, Deep Security Users can set their user interface language individually. (To change a User's language setting, go to **Administration > User Management > Users** and edit the **Properties** of the User account.)*

3. If you agree to the terms of the license agreement, select **I accept the agreement** and click **Next**.
4. Specify the folder where you would like Deep Security Manager to be installed and click **Next**.

Note: *When selecting a folder, the installer may append the suggested folder name on the end of the path you have selected. Review the folder entry before proceeding if you have used the 'browse' button.*

5. Specify the type of database you wish to use. If you are using an Oracle or SQL Server database, it must be created before Deep Security Manager is installed. Enter the account details.

6. 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**.)
7. 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. Click **Next**.
8. 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. Click **Next**.
9. Select Automatic Updates (recommended). If selected, Deep Security Manager will automatically retrieve the latest Components or check for new Software. (You can configure updates later using the Deep Security Manager.) Click **Next**.
10. Select whether to install a co-located Deep Security Relay. (If you do not have the Deep Security Relay installer package in the same location as the Deep Security Manager installer this step will be bypassed.)

***Note:** If you choose not to install a co-located relay at this time, you can do so later by installing a Deep Security Relay as described in [Installing the Deep Security Relay \(page 43\)](#).*

Click **Next**.

11. 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. Click **Next**.
12. Confirm Settings. Verify the information you entered and click **Finish** to continue.
13. Click **Finish** to close the Setup wizard.

The Deep Security Manager service will start when setup is complete. If you selected to install a co-located Deep Security Relay in Step 10, the Relay installation will run silently now. 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

To install from a Linux GUI, the instructions are identical to installing the Deep Security Manager for Windows (above).

Silent Install of Deep Security Manager

To initiate a silent install on Windows, enter the command:

```
Manager-Windows-<Version>.x64.exe -q -console -varfile <PropertiesFile>
```

To initiate a silent install on Linux, enter the command:

```
Manager-Linux-<Version>.x64.sh -q -console -varfile <PropertiesFile>
```

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

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

The **<PropertiesFile>** argument is the complete/absolute path to a standard Java properties file. Each property is identified by its equivalent GUI screen and setting in the Windows Deep Security Manager installation (described above). 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. The only required values for a simple installation using an embedded database are:

```
LicenseScreen.License  
CredentialsScreen.Administrator.Username  
CredentialsScreen.Administrator.Password
```

For a complete description of available settings, see [Deep Security Manager Settings Properties File \(page 126\)](#).

Running 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 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.)

Deep Security Relay Configuration

Deep Security requires at least one Deep Security Relay to be installed and configured.

If you selected to install a co-located Deep Security Relay, use the Deep Security Manager to configure the Deep Security Relay as described in [*Configuring the Deep Security Relay \(page 121\)*](#).

Installing the Deep Security Relay

Deep Security Manager requires at least one Deep Security Relay to pull down updates from the Trend Micro Update Server. Updates are required for all protection functionality except Firewall.

Deep Security Manager gets update information only from the Deep Security Relay. A typical configuration is for the Deep Security Manager to use a Deep Security Relay co-located on the same computer. If you have chosen not to install the co-located Deep Security Relay, you should install a Deep Security Relay on another computer.

This section describes the stand-alone Deep Security Relay installation.

These steps are not required if you have already installed a co-located Deep Security Relay as part of the Deep Security Manager installation.

Preparation

Note: *When using Relay Groups, Deep Security Relays on Linux will not update correctly if they use Deep Security Relays on Windows as their update source. It is recommended that Deep Security Relays on Windows and Linux only ever be configured to update from the Trend Micro Global Update source, or from Relays of the same platform.*

The clock on a Deep Security Relay (DSR) machine must be synchronized with Deep Security Manager (DSM) to within a period of 24 hours. If the DSR clock is behind the DSM clock then an "Agent Activate" operation will fail because the certificate generated for the DSR by Deep Security Manager will not yet be valid.

Note: *If this condition is encountered an "Agent Activate Failed" event will be recorded in the System Events: "A client error occurred in the Deep Security Manager to Deep Security Agent protocol: HTTP client error received: certificate is not yet valid".*

Copy the Installer Package

Copy the installation file to the target machine.

Installing Deep Security Relay for Windows

Note: *The Deep Security Relay installer installs both Relay Server and Deep Security Agent functionality on Windows machines.*

Remember that you must have administrator privileges to install and run the Deep Security Relay on Windows machines.

1. Double-click the installation file to run the installer package. Click **Next** to begin the installation.
2. Accept the license agreement and click **Next** to continue.
3. Select the features you want to install (some features such as Anti-Malware are optional).

Click **Browse** to specify the location where you would like Deep Security Relay to be installed. (If you are upgrading, you will not be able to change the installation directory. To install to a different directory, you will have to first uninstall the previous version.)

Click **Reset** to reset the feature selection to the default settings.

***Note:** Firewall and Intrusion Prevention features may not be deselected. These features form part of the core Deep Security Agent architecture and are always installed, even if Firewall and Intrusion Prevention functions will not be used. Click Disk Usage to see the total space required for the selected features and compare with the available space on your selected destination location.*

Click **Next** to continue.

4. Click **Install** to proceed with the installation.
5. Click **Finish** to complete the installation.

The Deep Security Relay is now installed and running on this computer, and will start every time the machine boots. You will see the Deep Security Notifier icon in your Windows System Tray.

***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.*

***Note:** Installing the Deep Security Relay over Windows Remote Desktop is NOT recommended because of the temporary loss of connectivity during the install process. However, using the following command line switch when starting Remote Desktop will allow the install program to continue on the server after the connection is lost: On Windows Server 2008 or Windows Vista SP1 and later or Windows XP SP3 and later, use:*

```
mstsc.exe /admin
```

On earlier versions of Windows, use:

```
mstsc.exe /console
```

Installing the Deep Security Relay for Linux

Note: To install the Deep Security Relay on a Linux machine, you need to log on as "root".
Alternatively, you can use the "sudo" utility.

To install the Deep Security Relay for Linux:

1. Use "rpm -i" to install the ds_agent package:

```
# rpm -i Relay-RedHat_ELx_i686-9.0.0-xxx.x86_64.rpm
Preparing... ##### [100%]
1:ds_agent ##### [100%]
Loading ds_filter_im module version 2.6.x [ OK ]
Starting ds_agent: [ OK ]
```

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

2. The Deep Security Relay start automatically after installation.

To start, stop and reset the Deep Security Relay on Linux:

Command-line options:

```
/etc/init.d/ds_agent start - starts the Agent
/etc/init.d/ds_agent status - displays the status of the Agent
/etc/init.d/ds_agent stop - stops the Agent
/etc/init.d/ds_agent reset - resets the Agent
/etc/init.d/ds_agent restart - restarts the Agent
```

Preparing ESXi for Deep Security Virtual Appliance Deployment

This section describes how to prepare the VMware environment for Agentless protection using the DSVa.

At this point...

- The VMware Environment is already setup as in Preparing a VMware Environment for Agentless Protection.
- Deep Security Manager (and database) is already installed.
- A Deep Security Relay has been installed and configured.
- VMware vShield Endpoint has been deployed on the protected Host ESXi.
- The Deep Security Filter Driver and Virtual Appliance software has been downloaded from Trend Micro and imported into the Deep Security Manager.

Add vCenter to the Deep Security Manager's list of Managed Computers.

Deep Security Manager configuration must be performed by using a Deep Security Manager user account with Full Access rights.

1. From the Deep Security Manager **Computers** screen, click **New > Add VMware vCenter...**
2. Enter the vCenter Server IP Address (or hostname), Username and Password for the vCenter. Click **Next**.

Note: Make sure DNS is configured and able to resolve FQDN to IP Addresses used by all machines in this environment, otherwise enter the IP Address.

3. Enter the vShield Manager Server Address, Username and Password. (You can also configure this information later from the Deep Security Manager). Click **Next**.
4. Accept the vShield Manager SSL certificate.
5. Accept the vCenter certificate.
6. Review the vCenter information. Click **Finish**.
7. 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.

Prepare ESXi for Virtual Appliance deployment by Installing the Filter Driver

Note: *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 host (make sure a cluster server with vMotion support is set up so that this can be done automatically).*

1. From the Deep Security Manager, Select **Computers > vCenter > Hosts and Clusters**
2. Find the ESXi host in the Computers list (its **status** column should read **Unprepared**), right-click and select **Actions > Prepare ESXi** to display the Prepare ESXi Server Wizard. Click **Next**.
3. Select **Yes** to allow the Deep Security Manager automatically bring the ESXi in and out of maintenance mode. Click **Finish**.
4. The ESXi preparation process will complete all activities with no further input necessary. (The ESXi will be placed in maintenance mode, the Deep Security Filter Driver will be installed, and the ESXi will be restarted).
5. Once the process is complete, you are given the option to continue with the next step, deploying the Deep Security Virtual Appliance. Select **No thanks, I will deploy later**. Click **Close**. (The Deep Security Virtual Appliance deployment is described in [Deploying the Deep Security Virtual Appliance \(page 48\)](#)).
6. This completes the ESXi preparation.

Note: *You can monitor the preparation process in the VMware vSphere Client management console.*

Verification Steps

1. Go back to **Computers > vCenter** and make sure the **status** of the ESXi is set to **Prepared**.
2. In the VMware vSphere client, go to **ESXi Server > Configuration > Networking**. Check that the vSwitch has been created.
3. SSH into the ESXi Server ("Tech Support Mode" must be enabled on the ESXi) and run the following commands to confirm the VMware and Trend Micro drivers are installed properly:

```
vmkload_mod -l | grep dvfilter
```

Note: *dvfilter comes with the ESXi installation. dvfilter-dsa is the Trend Micro driver installed to the ESXi when the preparation process has completed .*

```
esxcli software vib list | grep Trend
```

Check that the correct version and status of dvfilter-dsa is displayed.

Deploying the Deep Security Virtual Appliance

This section describes how to Install and Activate the DSVa to provide Agentless protection.

At this point...

- The VMware Environment is already setup as in Preparing a VMware Environment for Agentless Protection.
- Deep Security Manager (and database) is already installed.
- A Deep Security Relay has been installed and configured.
- VMware vShield Endpoint has been deployed on the protected Host ESXi, and vCenter has been added to the Deep Security Manager's list of Managed Computers, see Additional Configuration for VMware Integration.
- The protected ESXi host has been prepared for Deep Security Virtual Appliance Deployment.

Note: For a detailed list of required VMware permissions, see [Minimum VMware Privileges for DSVa Deployment \(page 140\)](#).

Note: Deep Security Manager configuration must be performed by using a Deep Security Manager user account with Full Access rights.

Deploy Deep Security Virtual Appliance (DSVA) to the ESXi

To Deploy Deep Security Virtual Appliance (DSVA) to the ESXi:

1. From the Deep Security Manager, select **Computers > vCenter**.
2. Right-click on the ESXi Host being protected and select **Actions > Deploy Appliance**. Click **Next**.
3. 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**.
4. Define the Appliance Hostname. Enter the IPv4 Address and/or IPv6 Address for the Appliance. (DHCP is enabled by default). Click **Next**.
5. Select Thick Provisioned format.
6. Click **Finish** and wait for for the DSVa to be uploaded.
7. In the **Activate Deep Security Appliance** section, select **No thanks, I will activate it later**. (Activation is described later). 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.

Verification Steps:

1. On vCenter Console, go to the DSVA Console tab. Make a note of the Management Address of the DSVA, and whether it is using eth0 or eth1. Make sure the network adapters are configured correctly and that they are on the correct network pool.
2. Go to the Virtual Machine **Properties** > **Summary** tab, and click **Edit Settings**.
3. Go to the Hardware tab, there are three interfaces available.

Note: *Network Adapter 0 is always the management network. DSVA uses this interface to communicate with Deep Security Manager.*

Network Adapter 1 is used by the DSVA to communicate with the VM Kernel VNIC IP. Check the ESXi Network Configuration to make sure that the vmservice-trend-pg is on the same virtual switch as vmservice-vmknics-pg.

Activate the Deep Security Virtual Appliance

To activate the Virtual Appliance:

1. From the Deep Security Manager, select **Computers > vCenter**
2. Right Click on the DSVA machine and select **Actions > Activate Appliance**. Click **Next**.
3. For Policy, select **Deep Security Virtual Appliance**. Click **Next**. The activation process is started.
4. 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 if 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.

5. In **Activate Host Virtual Machines**, select **No thanks, I will activate them later**. (This step will be described later) Click **Close**.

The DSVA is now activated. Go back to **Computers > vCenter** and make sure the **status** of DSVA is displayed as **Managed (Online)**.

Activating Guest Virtual Machines

Assign Guest Virtual Machines to the ESXi

1. Move virtual machines to the ESXi Host.

2. Power-on the machines if they are offline.

Activating a Virtual Machine and Applying a Policy

1. From the Deep Security Manager, select **Computers > vCenter**
2. Right-click on the Virtual Machine and select **Actions > Activate**
3. Optionally, enable Anti-Malware protection by right-clicking on the Virtual Machine and selecting **Actions > Assign Policy** and selecting a suitable Policy which has Anti-Malware enabled (the **Windows Anti-Malware Protection** Policy, for example, which has only Anti-malware protection enabled).
4. Check the status of the Virtual Machine and make sure Anti-Malware status is active.

Verification steps:

If you are activating Anti-Malware protection but Anti-Malware status is displaying Anti-Malware Engine offline, there are a few things you can check:

1. Make sure the VMware tools are up-to-date on the virtual machine
2. Make sure vShield Endpoint Agent is installed and the vsepflt driver is running on the VM:

```
sc query vsepflt
```
3. Make sure Deep Security Manager is able to synchronize information with vCenter
4. In the Deep Security Manager's Computers list, make sure that the ESXi status is **vShield Endpoint: Installed**
5. In the Deep Security Manager's Computers list, make sure that the DSVA status is **vShield Endpoint: Registered**
6. Make sure the protected computer's Anti-Malware status is **On** or **Real-Time**.

Automatically Deploying an Appliance for Stateless ESXi

In addition to the ESXi 5.0 standard system requirements, the following must be installed and configured to auto-deploy an appliance for stateless ESXi:

- VMware Virtual Center (as described in [Preparing a VMware Environment for Agentless Protection \(page 31\)](#))
- TFTP server
- VMware Auto-deploy Plug-in
- If you are using DHCP, the DHCP server must be configured for PXE
- Host profile through vCenter to handle the configuration part of the ESXi once it auto-boots
- vSphere powerCLI installed on a Windows machine that it can reach the vCenter server over the network
- Deep Security Filter Driver and Virtual Appliance

Install TFTP Server

Install a TFTP server, such as WinAgents TFTP server. Create a directory on your Windows server, for example: E:\tftpboot and make this your TFTP root directory.

Install VMware Auto-deploy Plug-in

1. Install the vCenter Auto Deploy software. This can be installed on your vCenter server or can run on a separate Windows server and configured to point to your vCenter server. (You will need to provide the IP of the vCenter server and credentials.)
2. Install the Auto Deploy as a plug-in in your vSphere Infrastructure Client. (You will see the Auto Deploy icon on the Home tab.)
3. Add a boot image to your TFTP server root directory as follows:
 1. In the vSphere client, click the Auto Deploy plug-in.
 2. Choose to download the TFTP Boot Zip and extract this ZIP file into your TFTP root directory.
 3. Test your configuration by booting an ESXi host or a VM. Make sure that the ESXi host or VM is using PXE boot. You should see that it is assigned an IP address and it starts loading a TFTP image.
 4. You will see that although a TFTP image was loaded, there was no ESXi image associated with this host.

Configure DHCP Server for PXE.

If you are using DHCP, configure the DHCP server for PXE boot. The specific steps depend on the product you are using for DHCP. You need to open the scope on your DHCP server and add the following options:

```
066 - Boot server host name: <ip of your TFTP / PXE boot server>
067 - Boot file name: undionly.kpxe.vmw-hardwired
```

Add the Deep Security Filter Driver to the VIB Image

For the Trend Micro filter driver vib to be automatically deployed as part of the PXE boot image, take a default ESXi image and rebuild it with the Trend Micro filter driver vib as part of a new image and rename the file. For example, if you are using VMware-ESXi-5.0.0-441354-depot.zip, name the file VMware-ESXi-5.0.0-441354-Trend-dvfilter-depot.zip.

Adding the filter driver to the image along with a host profile allows the ESXi to appear as "prepared" to the Deep Security Manager.

The VMware vCenter Server Appliance is available from VMware, which is a preconfigured Linux-based virtual machine with PXE boot functionality already available. Using VMware vCenter Server Appliance requires less setup for auto-deploy than using Windows vCenter Virtual Center. For VMware vCenter Server Appliance installation, see the vSphere Installation and Setup publication.

Install vSphere PowerCLI

1. Download the vSphere 5 PowerCLI and install it on the server on which you will be working with your images.
2. To test if your VMware PowerCLI is working, start the VMware vSphere PowerCLI command prompt and run:

```
Get-DeployCommand
```

This will display a list of all the commands you will need to work with Auto Deploy. At this point, all requirements for vSphere Auto Deploy have been installed.

Prepare the First Image

To prepare the first image you will need to provide the following information:

- IP address of the host and the DNS hostname
- MAC address of the host
- Image name, as downloaded from VMware site)-for example, "VMware-ESXi-5.0.0-441354-Trend-dvfilter-depot.zip"
- Image name, after being added to the depot-for example, "ESXi-5.0.0-441354-standard"

- The directory for your SoftwareDepot, which will be used by the Auto Deploy software.

Preparing the Image

1. Create a directory named "Staging".
2. Create a directory called "VIB-downloads" in which you will store the VIBs and images you want to deploy.
3. Deploy the basic VMware ESXi 5.0 image to a new host without any further configuration.
4. Attach the image to the host, based on the MAC address, so that the host appears in your vCenter in a folder named in the "Staging" folder. Since it has no configuration, it will not appear in a cluster yet.
5. Create a DHCP reservation for the MAC address.
6. In your DHCP scope, create the reservation and use the proper hostname. In DNS, create an A-record for this hostname and IP address and give it a PTR/reverse lookup record.

Add a New Image to the Depot

1. Run the following command to insert the image into the "SoftwareDepot" directory:

```
Add-EsxSoftwareDepot "E:\VIB-downloads\VMware-ESXi-5.0.0-441354-depot.zip"
```

2. Run the following command to see what images are present in your depot:

```
Get-EsxImageProfile
```

The image is now ready to deploy.

Deploy the First Host

When the host reboots, it will pick up the TFTP image and will ask the vSphere Auto Deploy server for an image.

Note: When creating rules, there are two rule sets: a 'working-set' and an 'active-set'. The 'working-set' is serves as a depot of rules, the 'active-set' are the rules that are available to hosts.

Deploying the Host

1. Create a rule to connect the image to the host using the 'New-DeployRule' command:

```
New-DeployRule -Name "<rule_name" -Item "<image_name",  
"<folder_name>" -Pattern "mac=<mac_address>"
```

The new rule that has just been created is called "PreStaging". It will ensure that the image called "ESXi-5.0.0-441354-standard" (Get-EsxImageProfile) will be deployed to a host with the specified MAC address and will be placed in the "Staging" folder in vCenter.

For example, the following command creates a rule called "PreStaging" and will ensure that the image called "ESXi-5.0.0-441354-standard" (Get-EsxImageProfile) will be deployed to a host with the MAC address of 00:1a:92:b8:da:77 and will be placed in the "Staging" folder in vCenter:

```
New-DeployRule -Name "PreStaging" -Item  
"ESXi-5.0.0-441354-standard", "Staging" -Pattern  
"mac=00:1a:92:b8:da:77"
```

2. To see the rule you have created, use the command:

```
Get-DeployRule
```

This is a rule in the 'working set'.

3. To make the rule part of the 'active set' use the following command:

```
Add-DeployRule -DeployRule "PreStaging"
```

4. To check the rules in the 'active set', run the Get-DeployRuleSet command:

```
Get-DeployRuleSet
```

5. Boot your host to install. The host will appear in your vCenter.

Configure the Host Profile

After your host appears in vCenter, configure a host profile, including vSwitches, attach the datastores, and confirm the NTP settings. Because this is a diskless host, set up syslog and the core dump location. (The syslog tool and the Coredump utility can be found in the vCenter tools directory.)

Note: *If you would configure the host and reboot at this point, all changes will be lost. To preserve the configuration, you must define a host profile.*

Note: *When working with advanced host configurations, you may want to use the vSphere Enable/Disable Profile Configurations option for troubleshooting.*

Your server can now also receive core dumps in case an ESXi host receives an error.

1. Configure your ESXi host to use the Coredump server. To do this, go into the configuration screen of your host, go to the security profile and enable SSH, then logon to the ESXi console using your an SSH client and run the following commands:

```
esxcli system coredump network set --interface-name vmk0 --server-
ipv4 192.168.0.40 --server-port 6500
esxcli system coredump network set --enable true
esxcli system coredump network get
```

The last line indicates if the new settings have been enabled.

2. Log out from the ESXi host and switch back to your vSphere Client.
3. Go to the "Host and Clusters" view in your vSphere client and select the host you have just prepared.
4. Right-click the host and select Create Profile from host.
5. Give the profile a name-for example 'Profile-Cluster01'.
6. Attach the profile to this host using the Host Profiles section in the vSphere client and check that the profile is compliant.

Auto-deploy the Host with the Host Profile

The first rule created above ensures that the host with a certain MAC address will be connected to the standard image and put in the "Staging" folder:

```
New-DeployRule -Name "PreStaging" -Item "ESXi-5.0.0-441354-standard",
"Staging" -Pattern "mac=00:1a:92:b8:da:77"
```

Auto-deploying the Host

1. Create a rule to move the host into the production cluster. Use the IP range that you use in the DHCP scope for the ESXi hosts and create a reservation in the DHCP scope for each host and also create a DNS record using the following format: `New-DeployRule -Name "<rule_name>" -Item "<image_name>", "<cluster_name>", "<host_profile>" -Pattern "ipv4=<DHCP-range>"`

For example, in the following command:

```
New-DeployRule -Name "Prod-CL01" -Item "ESXi-5.0.0-441354-standard",
"CL01", "Profile-Cluster01" -Pattern
"ipv4=192.168.0.100-192.168.0.110"
```

'Prod-CL01' is the name of the rule, 'CL01' is the name of the cluster, 'Profile-Cluster01' is the name of the host profile and ipv4 is the DHCP range.

2. In the 'working-set' are now two rules ("PreStaging" and "Prod-CL01") and in the 'active-set' the "PreStaging" rule is active. Using the remove command, remove the "PreStaging" rule from the 'active-set' and next we add the "Prod-CL01" to the 'active-set' and double check what we have done:

```
Remove-DeployRule -DeployRule "PreStaging"  
Add-DeployRule -DeployRule "Prod-CL01"  
Get-DeployRuleSet
```

The configuration is now complete. When you reboot your hosts, they will come back and will be added to the CL01 cluster fully participating as a normal host.

Install Deep Security Agents

This section describes how to install and activate Deep Security Agents on each type of supported platform.

A full list of supported platforms can be found in [System Requirements \(page 28\)](#)

At this point...

- Deep Security Manager (and database) is already installed.
- A Deep Security Relay has been installed and configured.

Note: *The clock on a Deep Security Agent (DSA) machine must be synchronized with Deep Security Manager (Deep Security Manager) to within a period of 24 hours. If the DSA clock is behind the Deep Security Manager clock then an "Agent Activate" operation will fail because the certificate generated for the DSA by Deep Security Manager will not yet be valid. If this condition is encountered an "Agent Activate Failed" event will be recorded in the System Events: "A client error occurred in the Deep Security Manager to Deep Security Agent protocol: HTTP client error received: certificate is not yet valid". To avoid this problem, all clocks on Deep Security component machines should be synchronized with a internet time service if possible.*

Note: *CentOS uses the Red Hat 5 RPM and will appear as "Red Hat" in the Deep Security Manager. To use the Deep Security Agent on CentOS, follow the instructions for installing the Red Hat Agent.*

Windows

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

1. Copy the installation file to the target machine.
2. Double-click the installation file to run the installer package. Click **Next** to begin the installation
3. Read the license agreement and click **Next**.
4. Select the features you want to install and click Browse to specify the location where you would like Deep Security Agent to be installed. (If you are upgrading, you will not be able to change the installation directory. To install to a different directory, you will have to first uninstall the previous version.) Click **Reset** to reset the feature selection to the default settings.

Note: *Firewall and Intrusion Prevention features may not be deselected. These features form part of the core Deep Security Agent architecture and are always installed, even if Firewall and Intrusion Prevention functions will not be used.*

Click **Disk Usage** to see the total space required for the selected features and compare with the available space on your selected destination location.

Click **Next**.

5. Click **Install** to proceed with the installation.
6. Click **Finish** to complete the installation.

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.*

Note: *Installing the Deep Security Agent over Windows Remote Desktop is NOT recommended because of the temporary loss of connectivity during the install process. However, using the following command line switch when starting Remote Desktop will allow the install program to continue on the server after the connection is lost: On Windows Server 2008 or Windows Vista SP1 and later or Windows XP SP3 and later, use:*

```
mstsc.exe /admin
```

On earlier versions of Windows, use:

```
mstsc.exe /console
```

Linux

Note: *Starting the Deep Security Agent's `ds_filter` service will disable iptables.*

Note: *For **SuSE 11**, on the target machine before beginning the installation procedure:*

in:

```
/etc/init.d/jexec
```

after

```
# Required-Start: $local_fs
```

add the line:

```
# Required-Stop:
```

To install the Deep Security Agent on Red Hat, SuSE, or Oracle Linux

Note: The following instructions apply to Red Hat, SuSE, and Oracle Linux. To install on SuSE or Oracle Linux, substitute the SuSE or Oracle Linux RPM name in place of Red Hat.

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.

To install the Deep Security Agent on Ubuntu:

To install on Ubuntu, copy the installation file to the target machine and use the following command:

```
sudo dpkg -i <driver_deb_pkg>
```

where <driver_deb_pkg> is the Debian package with the driver that was built and placed in the <DS>/src/dsa/agent/deb/ directory.

To start, stop and reset 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  
/etc/init.d/ds_filter stop
```

To reset the Agent:

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

To restart the Agent:

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

Solaris

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 Sparc/10:

- SUNWgccruntime, GCC Runtime libraries
- pfil_Solaris_10sparc.pkg (see note below)
- Agent-Solaris_5.10_U7-9.0.0-xxx.x86_64.pkg.gz
- Agent-Solaris_5.10_U5-9.0.0-xxx.x86_64.pkg.gz

For Solaris X86/11:

- SUNWgccruntime, GCC Runtime libraries
- pfil_Solaris_10x86.pkg (see note below)
- Agent-Solaris_5.11-9.0.0-xxx.i386.p5p.gz

For Solaris SPARC/11:

- SUNWgccruntime, GCC Runtime libraries
- pfil_Solaris_10x86.pkg (see note below)
- Agent-Solaris_5.11-9.0.0-xxx.sparc.p5p.gz

Note: All Solaris versions up to and including Solaris 10 Update 3 require pfil to be installed.

To install the Solaris 11 Agent:

1. Acquire all of the required packages (see above)
2. Copy the installation file to the target machine
3. 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. Acquire all of the required packages (see above)
2. Copy the installation file to the target machine
3. Install the Agent:

```
gunzip Agent-Solaris_5.10_U7-9.0.0-xxx.x86_64.pkg.gz
pkgadd -d Agent-Solaris_5.10_U7-9.0.0-xxx.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` - 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
- `/etc/init.d/ds_agent reset` - 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`*

When you have completed the installation, use the Deep Security Manager to configure protection on the computer by following the steps in [Protecting a Server \(page 110\)](#) to:

- Add Computers to the Deep Security Manager
- Enable protection on computers

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)
```

AIX

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.powerpc.bff.gz
```

5. Install the Agent:

```
/tmp> installp -a -d /tmp 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 +
```

HP-UX:

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_11.31-9.0.0-xxx.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_11.31-9.0.0-xxx.ia64.depot
ds_agent
```

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

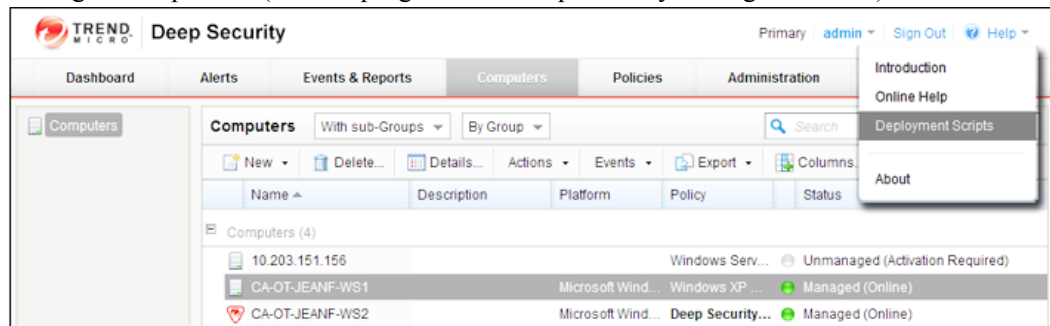
- `/sbin/init.d/ds_agent start`
- `/sbin/init.d/ds_agent stop`

Using Deployment Scripts for your Installation

Adding a computer to your list of protected resources in Deep Security and implementing protection is a multi-step process. Almost all of these steps can be performed from the command line on the computer and can therefore be scripted. The Deep Security Manager contains a deployment script writing assistant which can be accessed from the Manager's Help menu.

To generate a deployment script:

1. Start the Deployment Script generator by selecting **Deployment Scripts** from the Deep Security Manager's Help menu (at the top right of the Deep Security Manager window).



2. Select whether you are deploying and Agent or a Relay.
3. 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 from the Trend Micro Download Center. For information on importing Deep Security Software, see **Administration > System Settings > Updates** in the online help or Administrator's Guide.

4. Select **Activate the Agent Automatically**. (Agents must be activated by the Deep Security Manager before a protection Policy can be implemented.)
5. Select the Policy you wish to implement on the computer (optional)

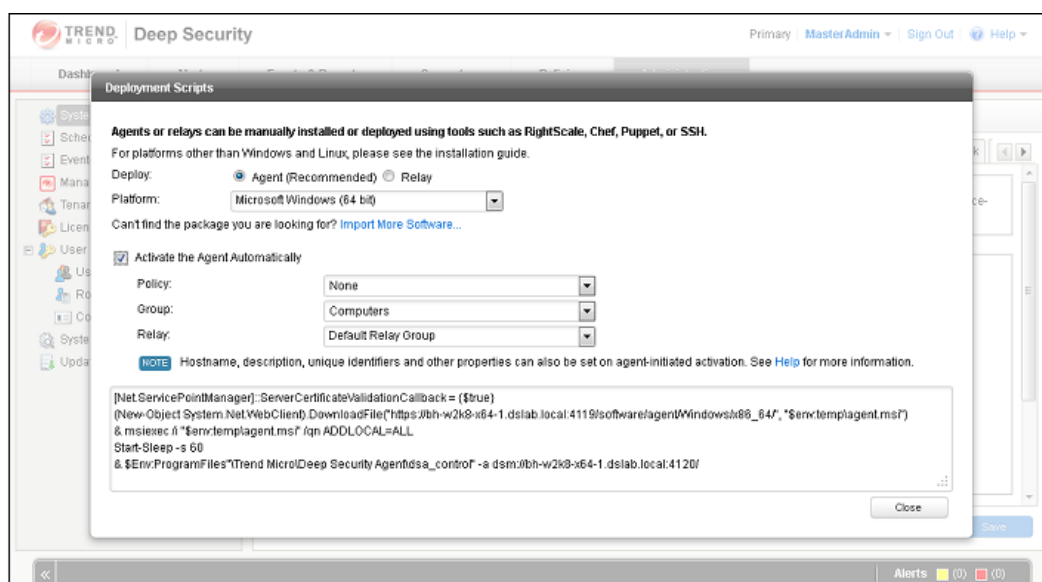
6. Select the computer Group (optional)
7. Select the Relay Group (optional)

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 toolbar on the **View Imported Software** page (**Administration > Updates > Software Updates**).

Note: The deployment scripts generated by Deep Security Manager for Windows Agent deployments require Windows Powershell version 2.0 or later.

Note: Optionally on Windows computers, if you do not intend to enable Anti-Malware protection, you may want to prevent the installation of the Anti-Malware engine entirely. To do so, delete the string "ADDLOCAL=ALL" from the Windows deployment scripts.



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 or Relay installation on Windows machines. The stand-alone installation described here is intended for use on Agentless Windows machines 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.*

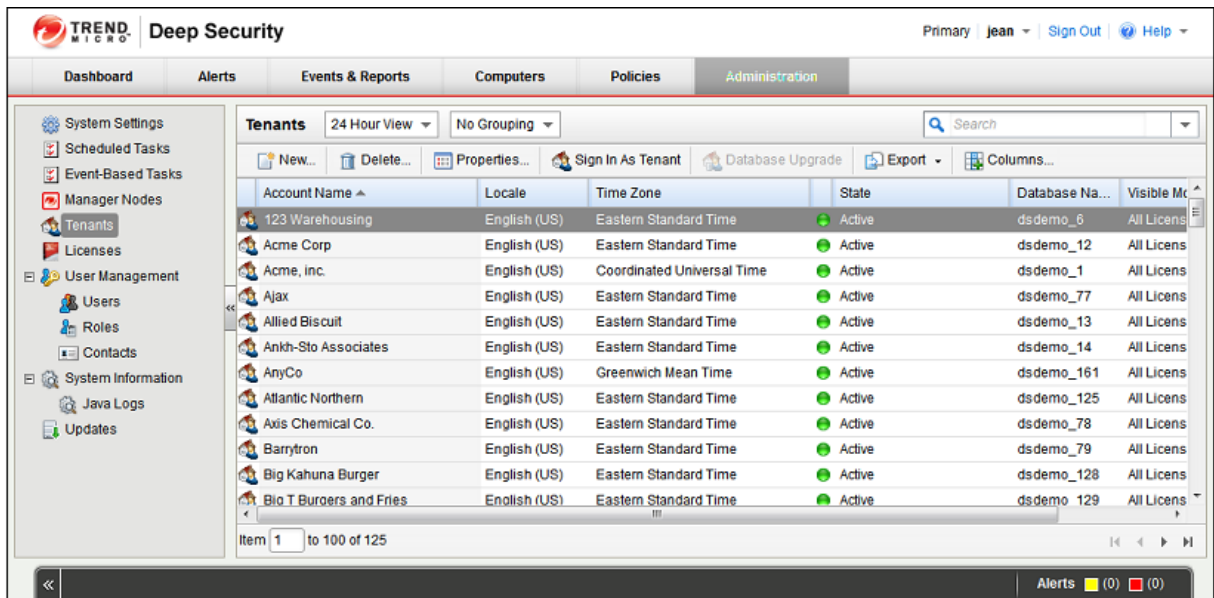
Enable Multi-Tenancy

To enable Multi-Tenancy:

1. In the Deep Security Manager, go to **Administration > System Settings > Advanced** and click **Enable Multi-Tenancy** 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. Time Zone. All Tenant-related Events will be shown to the Tenant Users in the time zone of the Tenant account. Click **Next**.
6. Enter a username for the first User of the new Tenant account.
7. 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.*

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

Examples of messages sent to Tenants

Email Confirmation Link: Account Confirmation Request

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

Account Name: AnyCo

Username: admin

Click the following URL to activate your account:

`https://managename:4119/SignIn.screen?confirmation=1A16EC7A-D84F-D451-05F6-706095B6F646&tenantAccount=AnyCo&username=admin`

Email Generated Password: Account and Username Notification

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

Account Name: AnyCo

Username: admin

You can access the Deep Security management console using the following URL:

<https://managename:4119/SignIn.screen?tenantAccount=AnyCo&username=admin>

Email Generated Password: Password Notification

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

Password: z3IgRUQ0jaFi

Managing Tenants

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

Tenants				
<div> <div>New...</div> <div>Delete...</div> <div>Properties...</div> <div>Authenticate As Tenant</div> <div>Database Upgrade</div> </div> <div>Search</div>				
Account Name ▲	Database Na...	Locale	State	Time Zone
AnyCo	dsmfuji_1	English (US)	Active	America/New_York
BetaCo	dsmfuji_2	English (US)	Pending deletion	America/New_York
CoMoTo	dsmfuji_3	Japanese	Active	Asia/Tokyo
DeltaCo	dsmfuji_4	English (US)	Confirmation Required	America/New_York
EvaMicro	dsmfuji_5	English (US)	Active	America/New_York
FireCo	dsmfuji_6	English (US)	Suspended	America/New_York

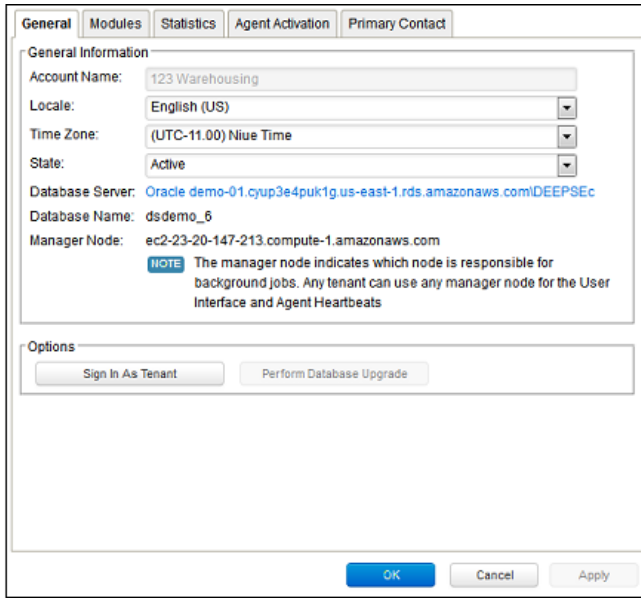
- **Created:** In the progress of being created but not yet active
- **Confirmation Required:** Created, but the activation link in the confirmation email sent to the Tenant User has not yet been clicked. (You can manually override this state.)
- **Active:** Fully online and managed
- **Suspended:**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

- **Database Upgrade Failure:** For Tenants that failed the upgrade path. The Database Upgrade button can be used to resolve this situation

Tenant Properties

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

General



The screenshot shows the 'General' tab of the 'Tenant Properties' window. The window has a title bar and a tabbed interface with tabs for 'General', 'Modules', 'Statistics', 'Agent Activation', and 'Primary Contact'. The 'General' tab is active, showing 'General Information' and 'Options' sections. The 'General Information' section contains fields for 'Account Name' (123 Warehousing), 'Locale' (English (US)), 'Time Zone' ((UTC-11:00) Niue Time), and 'State' (Active). Below these are 'Database Server' (Oracle demo-01.cyup3e4puk1g.us-east-1.rds.amazonaws.com), 'Database Name' (dsdemo_6), and 'Manager Node' (ec2-23-20-147-213.compute-1.amazonaws.com). A 'NOTE' box states: 'The manager node indicates which node is responsible for background jobs. Any tenant can use any manager node for the User Interface and Agent Heartbeats'. The 'Options' section has two buttons: 'Sign In As Tenant' and 'Perform Database Upgrade'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

General Modules Statistics Agent Activation Primary Contact

General Information

Account Name: 123 Warehousing

Locale: English (US)

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

State: Active

Database Server: [Oracle demo-01.cyup3e4puk1g.us-east-1.rds.amazonaws.com](#)DEEPSec

Database Name: dsdemo_6

Manager Node: ec2-23-20-147-213.compute-1.amazonaws.com

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

Options

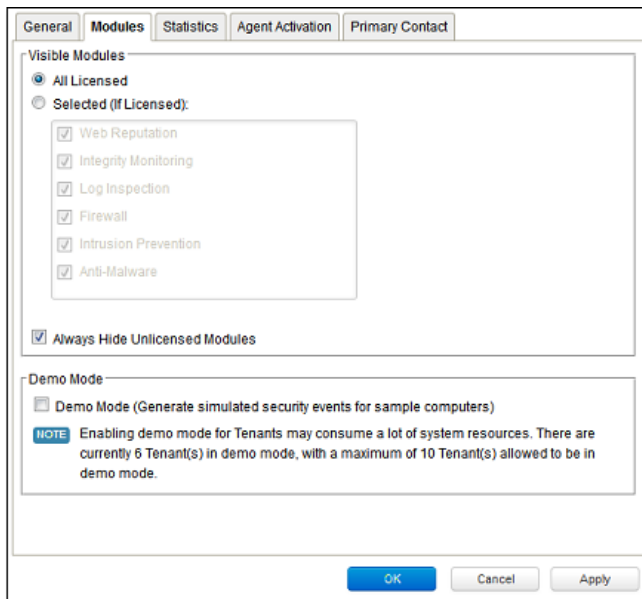
Sign In As Tenant Perform Database Upgrade

OK Cancel Apply

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

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

Modules



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

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

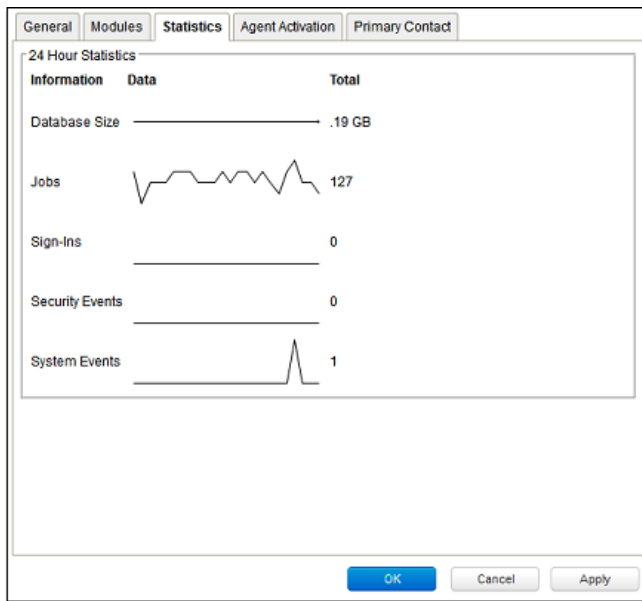
If using the "Per Tenant" licensing by default only the licensed modules for each Tenant will be visible.

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

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

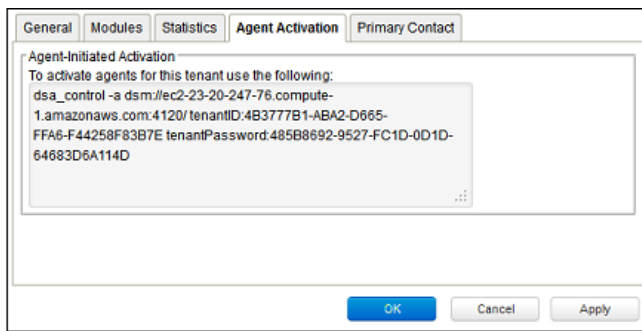
*Demo Mode is **not** intended to be used in a production environment!*

Statistics



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

Agent Activation



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

Primary Contact

Username	Role	Email Address
admin	Full Access	foster_rendr@trendmicro.com

Deep Security Relays

Each Deep Security Manager must have access to at least one Deep Security Relay, and this includes the Tenants in a Multi-Tenancy Deep Security installation. By default, the Relays 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 Deep Security Relays.

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 Relays from the Primary Tenant
 - Advanced Tab > Load Balancers
 - Advanced Tab > Pluggable Section
- Some of the help content not applicable to Tenants
- Some reports not applicable to Tenants
- Other features based on the Multi-Tenant Options (discussed later)
- 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.

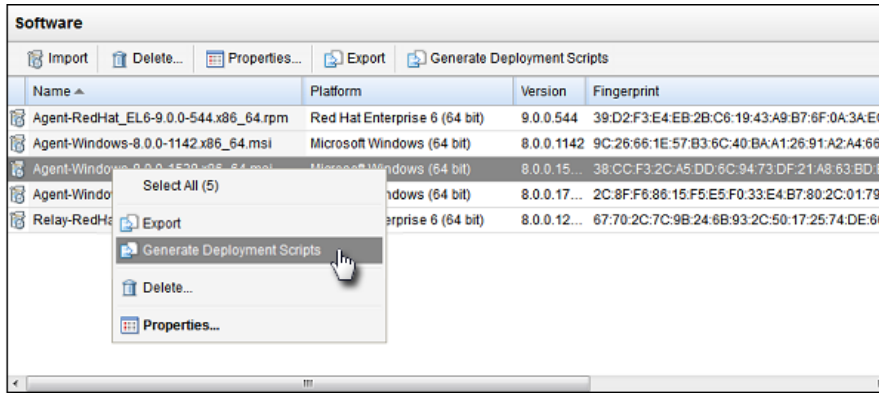
All Tenants have the ability to use Role-Based Access Control with multiple user accounts to further sub-divide access. Additionally they can use Active Directory integration for users to delegate the authentication to the domain. The Tenant Account Name is still required for any Tenant authentications.

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 clicking the **View Imported Software** button on the **Administration > Updates > Software Updates** tab, right-clicking and Agent install package, and selecting **Generate Deployment Scripts** from the context menu:



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

```
dsa_control -a dsm://manageraddress:4120/ "tenantID:7156CF5A-D130-29F4-5FE1-8AFD12E0EC02"
"tenantPassword:98785384-3966-B729-1418-3E2A7197D0D5"
```

Tenant Diagnostics

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

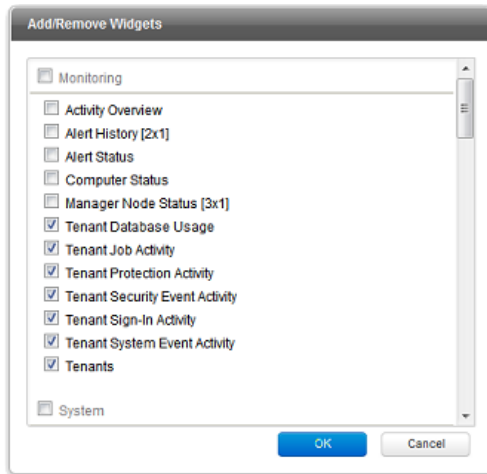
Usage Monitoring

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

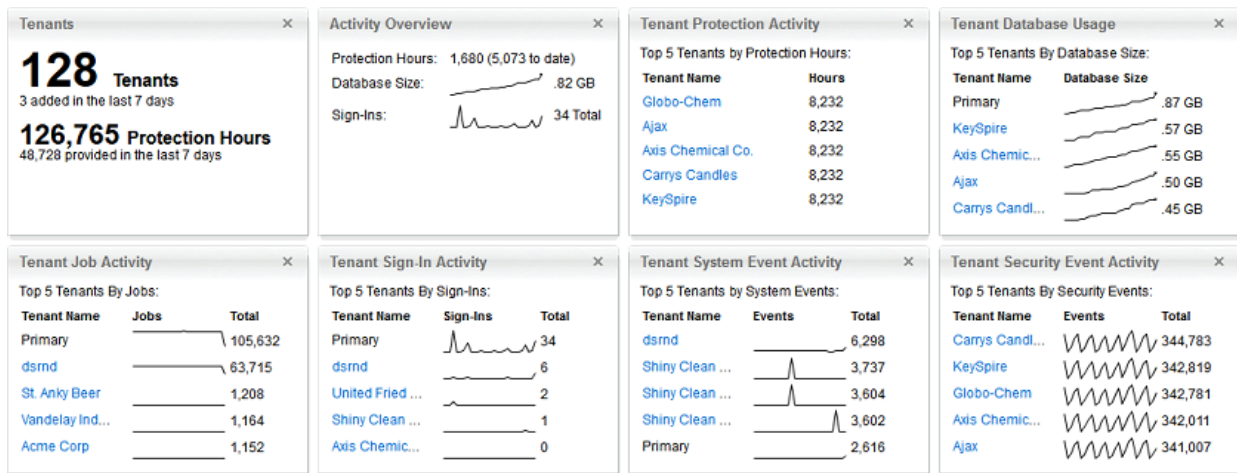
This chargeback (or viewback) information can be customized to determine what attributes are included in the record. This configuration is designed to accommodate various charging models that may be required in service provider environments. For enterprises this may be useful to determine the usage by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

Multi-Tenant Dashboard/Reporting

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



Some examples of Tenant-related widgets:



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

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

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

Multi-Tenancy (Advanced)

APIs

Deep Security Manager includes a number of REST APIs for:

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

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

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

Upgrade

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

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

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

Supporting Tenants

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

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

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

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

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

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

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

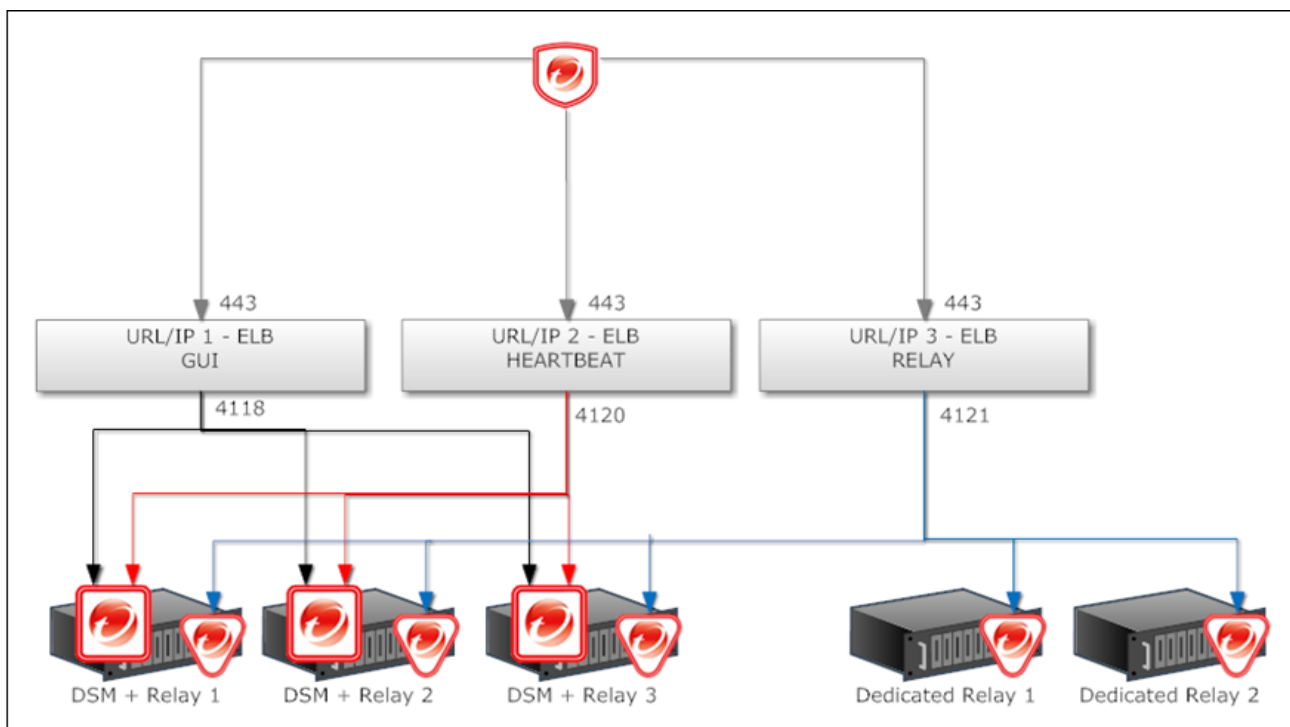
to direct the setting change or other command line action at a specific Tenant. If omitted the action is on the primary Tenant.

Load Balancers

By default, 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 balancer should be configured as TCP load balancer (not SSL Terminating) with sticky-sessions. 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.

Technical Details

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

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).

Configure vCloud for Integration with Deep Security

VMware vCloud integration allows Tenants in a Multi-Tenancy installation to import vCloud Organizations as Cloud Accounts and apply agentless Deep Security protection to them. The primary Tenant adds the vCenter hosting the VMs to their Deep Security Manager and then deploys and manages the Deep Security Virtual Appliance.

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.

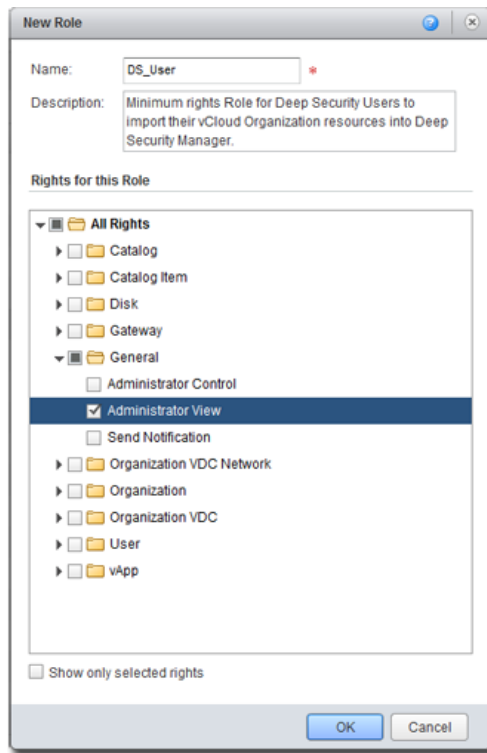
Creating a Minimum Rights Role for vCloud Account Tenant Users

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.

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 UUID duplication in virtual machines created from a vApp template breaks some third-party solutions](#)".*

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, launch Oracle Enterprise Manager and run the following commands:

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

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

```
USE vcloud
GO update CONFIG set value = '0' where
name='backend.cloneBiosUuidOnVmCopy'
commit;
select * from 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**.

Configure Amazon EC2 Resources for Integration with Deep Security

Before Amazon EC2 resources can be added to a Deep Security Manager as a "Cloud Account", you must generate an Amazon **Access Key** and a **Secret Key** for those resources that a Deep Security User will use when importing the resources to the Deep Security Manager. Then must assign minimum permissions to the User account.

To create an Access Key and Secret Key for Deep Security Manager and assign minimum permissions:

1. Go to your **Amazon Web Services** console and sign in
2. Open the **IAM** section (If you do not have privileges to use the IAM section, contact the account's administrator.)
3. Go to **Users** and click **Create New User**
4. Enter an account name, for example "deep_security"
5. Copy the generated **Access Key Id** and **Secret Key Id**
6. Select the **User** and choose **Permissions**
7. Here, you can grant the permissions either at the **Role** or at the **User** level. The minimum required permission is "**ec2:Describe***", however you can use the "**Read Only Access**" policy template for simplicity

Note: *Having a dedicated account for Deep Security ensures that you can refine the rights and permissions or revoke the account at any time. Trend Micro recommends that you give Deep Security a Access/Secret key with no more than **read-only** permissions.*

The following policy template will grant the required permissions:

```
{
  "Statement": [{
    "Sid": "Stmt1354546872297",
    "Action": [
      "ec2:Describe*"
    ],
    "Effect": "Allow",
    "Resource": [
      "*"
    ]
  }]
}
```

Upgrading

Upgrade Scenarios

To upgrade to Deep Security 9.0, you must be running Deep Security 8.0 SP2 or later. If you are running an earlier version of Deep Security, you must first upgrade to Deep Security 8.0 SP2 (or later) before upgrading to version 9.0. For instructions on how to upgrade to Deep Security 8.0 SP2, consult the **Deep Security 8.0 SP2 Installation Guide** available from the Trend Micro Download Center .

Deep Security 9.0 does not support ESX/ESXi version 4.1. To deploy Deep Security 9.0, your VMware infrastructure (vCenter, vShield Manager, vShield Endpoint, and vShield Endpoint drivers) must be upgraded to version 5.x.

Upgrading from DS 8.0 SP2 with Agentless Anti-Malware and/or Integrity Monitoring Protection (Includes upgrading ESX/ESXi 4.1 to 5.x)

Upgrading from DS 8.0 SP2 with Agentless Anti-Malware Protection (Upgrading ESX/ESXi 4.1 to 5.x) (page 91) describes the procedures for upgrading from Deep Security 8.0 SP2 to Deep Security 9.0 in a VMware 4.1 environment in which Agentless Anti-Malware protection is implemented.

Upgrading from Deep Security 8.0 SP2 with Agentless FW and IPS Only (Upgrading ESX/ESXi 4.1 to 5.x).

Upgrading from Deep Security 8.0 SP2 with Agentless FW and IPS Only (Upgrading from ESX/ESXi 4.1 to 5.0) (page 95) describes the procedures for upgrading from Deep Security 8.0 SP2 to Deep Security 9.0 in a VMware 4.1 environment in which only Agentless Firewall and IPS protection is implemented.

Upgrading from Deep Security 8.0 SP2 with In-guest Agent-Based Protection Only.

Upgrading from Deep Security 8.0 SP2 with In-guest Agent-Based Protection Only (page 98) describes the procedures for upgrading from Deep Security 8.0 SP2 to Deep Security 9.0 in any environment in which only Agent-based protection is being implemented.

Upgrading Deep Security 8.0 SP2 Software Components

Upgrading the Deep Security Manager

Download the new version of the Deep Security Manager installation package from Trend Micro Download Center and copy it to the target machine.

Run the installer package following the steps as for a new installation, described in [Installing Deep Security Manager \(page 39\)](#).

Upgrading vs. Overwriting an Existing Installation

If a previous version of Deep Security Manager is installed on your system, you are given the option to "upgrade the existing installation", or to "overwrite the existing installation". Upgrading the installation will upgrade the Deep Security Manager to the latest version but will not overwrite your Security Profiles, IPS Rules, Firewall Rules, Application Types, etc. or change any of the security settings being applied to the computers on your network. Overwriting the existing installation will erase all data associated with the previous installation and then install the latest filters, rules, profiles, etc.

***Note:** Even if you create a new installation, existing security elements currently being applied on your computers by Deep Security Agents will not be affected until you use Deep Security Manager to update them. To update Agents from a new installation of the Manager will require deactivation and reactivation of the Agents.*

Remotely Upgrading the Deep Security Components

The Deep Security Relay, the Deep Security Agent, the Deep Security Virtual Appliance, and the Deep Security Filter Driver can all be upgraded remotely using the Deep Security Manager. The software must be downloaded and imported into the Deep Security Manager first.

To download the Deep Security software packages:

1. In the Deep Security Manager, go to **Administration > Updates > Software Updates**.
2. Press **Open Download Center** This will take you to the Trend Micro Download Center Web site.
3. Download the latest software packages for the Relays, Agents, Filter Driver, and Virtual Appliance to your local machine.

To import the Deep Security software packages:

1. In the Deep Security Manager, go to **Administration > Updates > Software Updates**.

2. Press **Import Software** This will display the Import Software (From File) wizard.
3. Use the wizard to import each of the downloaded software packages into Deep Security.

Once the software packages are imported into Deep Security, you can upgrade the software components remotely from the Deep Security Manager.

To remotely upgrade a software component:

1. On the **Computers** screen of the Deep Security Manager, right-click on the computer you want to upgrade (ESXi, Deep Security Virtual Appliance, Deep Security Agent, or Deep Security Relay) and select the appropriate Upgrade option from the Actions menu.

Manually Upgrading the Deep Security Relay

To manually upgrade Deep Security Relay for Windows:

1. Copy the installation file to the target machine and run the installer package following the steps as for a new installation.

Note: *If you are upgrading, you will not be able to change the installation directory. To install to a different directory, you will have to first uninstall the previous version.*

To manually upgrade Deep Security Relay for Linux:

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

```
# rpm -U Relay-RedHat_EL5-9.0.0-xxx.x86_64.rpm
```

Manually Upgrading the Deep Security Agent

Note: *Remember that before upgrading a Deep Security Agent, you will need to make sure that Agent Self Protection is not enabled for the Deep Security Agent that you intend to upgrade. You can do this from **Policy/Computer Editor > Settings > Computer**. In the **Agent Self Protection** area, 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 manually upgrade the Deep Security Agent for Windows:

1. Copy the installation file to the target machine and run the installer package following the steps as for a new installation.

Note: *If you are upgrading, you will not be able to change the installation directory. To install to a different directory, you will have to first uninstall the previous version.*

To manually upgrade the Deep Security Agent for Linux:

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

```
# rpm -U Agent-RedHat_EL5-9.0.0-xxx.i386.rpm
```

To manually upgrade the Deep Security Agent for Solaris (all versions):

1. Use:

```
pkgadd -v -a /opt/ds_agent/ds_agent.admin -d Agent-  
Solaris_5.9_sparc-5.x.x-xxxx.sparc.pkg
```

To manually upgrade the Deep Security Agent for AIX/HPUX:

1. Use:

```
/opt/ds_agent/ds_upgrade.sh <full path to package>
```

Upgrading from DS 8.0 SP2 with Agentless Anti-Malware Protection (Includes upgrading ESX/ESXi 4.1 to 5.x)

Deep Security 9.0 does not support ESX/ESXi version 4.1. To deploy Deep Security 9.0, your VMware infrastructure (vCenter, vShield Manager, vShield Endpoint, and vShield Endpoint drivers) must be upgraded to version 5.x.

Summary of the Upgrade Procedures

Note: *The sequence of steps in this procedure is very important. Be sure to read them through at least once and follow them in the same order as they are written.*

There are two phases to this procedure: first, upgrading your VMware components, and second, upgrading your Deep Security components.

The first phase, upgrading your VMware components, will consist of the following steps:

1. Deactivate the Deep Security Virtual Appliance on the ESXi
2. Restore the ESXi (to uninstall the Deep Security Filter Driver)
3. Uninstall vShield Endpoint from the ESXi
4. Uninstall the vShield Endpoint Guest Drivers from VMs on the ESXi
5. Upgrade your vCenter
6. Upgrade the ESXi to ESXi 5.x (If you upgraded to ESXi 5.0, apply patch "ESXi 5.0 (build 474610 or later)")
7. Upgrade the vShield Manager
8. Configure the vShield Manager to integrate with the vCenter
9. Install vShield Endpoint on the ESXi
10. Install vShield Endpoint drivers (found in VMware Tools included with ESXi 5.x) on the VMs
11. Restart the ESXi

Note: *Uninstalling a vShield Endpoint module (Step 3) puts the ESXi host into maintenance mode and reboots it. Migrate your vShield Manager and any other virtual machines to another ESXi host to avoid shutting down these virtual machines during reboot.*

Note: *When upgrading the vShield Manager on a vCenter, you will have to deactivate all the Virtual Appliances running on that vCenter. This is because there is only one vShield Manager per vCenter and all the Virtual Appliances on that vCenter require an active vShield Manager. The amount of time it takes to deactivate a Virtual Appliance that is providing Agentless protection to*

VMs depends on the number of VMs that are being protected. Take this into account when estimating the amount of time the upgrade procedure will take.

Note: *Your VMs will not have Agentless protection on the ESXi while the Deep Security Virtual Appliance is deactivated.*

The second phase, upgrading your Deep Security components, will consist of these steps:

1. Upgrade the Deep Security Manager
2. Upgrade your Deep Security Relays
3. Add a security certificate to the Deep Security Manager for the vCenter and the vShield Manager
4. Import Deep Security 9.0 installation packages into the Deep Security Manager
5. Prepare the ESXi (this installs the Deep Security Filter Driver on the ESXi)
6. Reactivate your Deep Security Virtual Appliance in preparation for upgrade
7. Upgrade the Deep Security Virtual Appliance on your ESXi
8. Activate the guest VMs on the ESXi
9. Upgrade Deep Security Notifier (if required)
10. Deploy Deep Security Agents (if required)

Phase One: Upgrading Your VMware Components

Note: *These instructions provide the sequence in which you should carry out your VMware and Deep Security upgrade. For detailed instructions on upgrading the components of your VMware environment, consult your VMware documentation. Refer to VMware's Web site where you can find the latest information and knowledge base articles.*

To upgrade your VMware components:

1. In the Deep Security Manager, go to the **Computers** screen, right-click on the Virtual Appliance and select **Actions > Deactivate Appliance**.
2. On the **Computers** screen of the Deep Security Manager, right-click the ESXi and select **Actions > Restore ESX...** and follow the steps in the wizard. (This procedure will uninstall the 8.0 SP2+ Deep Security Filter Driver from the ESXi.)

Note: *Uninstalling a vShield Endpoint module puts the ESXi host into maintenance mode and reboots it.*

Migrate your vShield Manager and any other virtual machines to another ESXi host to avoid shutting down these virtual machines during reboot. Using vShield Manager 4.1, uninstall vShield Endpoint from the ESXi.

3. Using Add/Remove Programs on each VM, uninstall vShield Endpoint guest drivers from the VMs on the ESXi.

4. Run the VIM installer following the directions provided by VMware.
5. Upgrade the ESXi to ESXi 5.x (If upgrading to ESXi 5.0, apply patch "ESXi 5.0 (build 474610 or later)".)
6. Follow the directions in VMware's vShield_Quick_Start_Guide.pdf to upgrade the vShield Manager.
7. When the upgrade of the vShield Manager is complete and the vShield Manager has been restarted, log in to the vShield Manager console and add the configuration information required to re-integrate it with the vCenter.
8. Use the vShield Manager to install vShield Endpoint on the ESXi.
9. Use VMware Tools to install the vShield Endpoint guest drivers on the VMs.
10. Restart the ESXi to complete the VMware phase of the upgrade process.

When the ESXi has restarted, verify that all components of your vCenter are working correctly before continuing with phase two of the upgrade procedure, upgrading your Deep Security components.

Phase Two: Upgrading your Deep Security Components

The Deep Security software must be downloaded from the Trend Micro Download Center to a location from which it can be imported into the Deep Security Manager.

Note: You must have successfully completed phase one of this upgrade procedure, **Upgrading Your VMware Components**, before upgrading your Deep Security components.

Note: The Deep Security Filter Driver and the Deep Security Virtual Appliance must always be upgraded to the same version. Upgrading one without the other will leave both in a non-functional state.

To upgrade your Deep Security Components:

1. Upgrade the Deep Security Manager to version 9.0. Follow the same procedures as described in [Installing Deep Security Manager \(page 39\)](#).
2. Follow the instructions described in [Deploying the Deep Security Relay \(page 43\)](#).
3. On the **Computers** screen in the Deep Security Manager, right-click on the vCenter and select **Properties**. On the vCenter **Properties** screen, click **Add/Update Certificate...** on the **General** tab to add a certificate for the vCenter, and click **Add/Update Certificate...** on the **vShield Manager** tab to add a certificate for the vShield Manager.
4. In the Deep Security Manager, go to **Administration > Updates > Software Updates** and import the Deep Security Agent 9, Deep Security Relay 9, Deep Security Filter Driver 9, and Deep Security Virtual Appliance 9 installation packages.
5. The ESXi will be "unprepared". Follow the instructions in [Preparing ESXi for Deep Security Virtual Appliance Deployment \(page 46\)](#) to prepare the ESXi.
6. On the **Computers** screen in the Deep Security Manager, right-click on the Deep Security Virtual Appliance and select **Actions > Activate Appliance**. Do not activate the VMs at this time.

7. On the Computers screen in the Deep Security Manager, right-click on the Deep Security Virtual Appliance and select **Actions > Upgrade Appliance...**
8. Activate the guest VMs on the ESXi. Follow the instructions described in the section "Activating Guest Virtual Machines" in *Deploying the Deep Security Virtual Appliance (page 48)*.
9. Upgrade Deep Security Notifier (if required) as described in *Upgrade the Deep Security Notifier (page 100)*.
10. Deploy Deep Security Agents (if required). Follow the instructions described in *Deploying Deep Security Agents (page 57)*.

Upgrading VMware and Deep Security is now complete.

Upgrading from Deep Security 8.0 SP2 with Agentless FW and IPS Only (Upgrading from ESX/ESXi 4.1 to 5.x)

Deep Security 9.0 does not support ESX/ESXi version 4.1. To deploy Deep Security 9.0, your VMware infrastructure (vCenter, vShield Manager, vShield Endpoint, and vShield Endpoint drivers) must be upgraded to version 5.x.

The following upgrade procedures apply to VMware environments where Deep Security is providing Agentless Firewall and IPS protection only.

Summary of the Upgrade Procedures

Note: *The sequence of steps in this procedure is very important. Be sure to read them through at least once and follow them in the same order as they are written.*

There are two phases to this procedure: first, upgrading your VMware components, and second, upgrading your Deep Security components.

The first phase, upgrading your VMware components, will consist of the following steps:

1. Deactivate the Deep Security Virtual Appliance on the ESXi
2. Restore the ESXi (to uninstall the Deep Security Filter Driver)
3. Upgrade your vCenter
4. Upgrade the ESXi to 5.x. (If upgrading to 5.0, apply patch "ESXi 5.0 (build 474610)" or later.)

The second phase, upgrading your Deep Security components, will consist of these steps:

1. Upgrade the Deep Security Manager
2. Add a security certificate to the Deep Security Manager for the vCenter and the vShield Manager
3. Import Deep Security 9 installation packages into the Deep Security Manager
4. Prepare the ESXi (this installs the Deep Security Filter Driver on the ESXi)
5. Reactivate your Deep Security Virtual Appliance in preparation for upgrade
6. Upgrade the Deep Security Virtual Appliance on your ESXi
7. Deploy and configure a Deep Security Relay
8. Activate the guest VMs on the ESXi
9. Deploy Deep Security Agents (if required)

Phase One: Upgrading Your VMware Components

1. In the Deep Security Manager, go to the **Computers** screen, right-click on the Virtual Appliance and select **Actions > Deactivate Appliance**.
2. On the **Computers** screen of the Deep Security Manager, right-click the ESXi and select **Actions > Restore ESX...** and follow the steps in the wizard.
3. Run the VIM installer following the directions provided by VMware.
4. Upgrade the ESXi to 5.x. (If upgrading to 5.0, apply patch "ESXi 5.0 (build 474610)" or later.)

Verify that all components of your vCenter are working correctly before continuing with phase two of the upgrade procedure, upgrading your Deep Security components. Make sure the version numbers of the upgraded components match those in the Post-Upgrade Version column in the table at the beginning of these steps.

Phase Two: Upgrading your Deep Security Components

The Deep Security software must be downloaded from the Trend Micro Download Center to a location from which it can be imported into the Deep Security Manager.

Note: *You must have successfully completed phase one of this upgrade procedure, **Upgrading Your VMware Components**, before upgrading your Deep Security components.*

Note: *The Deep Security Filter Driver and the Deep Security Virtual Appliance must always be upgraded to the same version. Upgrading one without the other will leave both in a non-functional state.*

1. Upgrade the Deep Security Manager to version 9.0. Follow the same procedures as described in [Installing Deep Security Manager \(page 39\)](#).
2. On the **Computers** screen in the Deep Security Manager, right-click on the vCenter and select **Properties**. On the vCenter **Properties** screen, click **Add/Update Certificate...** on the **General** tab to add a certificate for the vCenter, and click **Add/Update Certificate...** on the **vShield Manager** tab to add a certificate for the vShield Manager.
3. In the Deep Security Manager, go to **Administration > Updates > Software Updates** and import the Deep Security Agent 9, Deep Security Relay 9, Deep Security Filter Driver 9, and Deep Security Virtual Appliance 9 installation packages.
4. After upgrading the ESXi in phase one, the ESXi will be "unprepared". Follow the instructions in [Preparing ESXi for Deep Security Virtual Appliance Deployment \(page 46\)](#) to prepare the ESXi.
5. On the **Computers** screen in the Deep Security Manager, right-click on the Deep Security Virtual Appliance and select **Actions > Activate Appliance**. Do not activate the VMs at this time.
6. On the **Computers** screen in the Deep Security Manager, right-click on the Deep Security Virtual Appliance and select **Actions > Upgrade Appliance...**
7. Follow the instructions described in [Deploying the Deep Security Relay \(page 43\)](#).

8. Follow the instructions described in the section "Activating Guest Virtual Machines" in *Deploying the Deep Security Virtual Appliance (page 48)*.
9. Follow the instructions described in *Deploying Deep Security Agents (page 57)*.

Upgrading to Deep Security 9 with Agentless Firewall and IPS protection only is now complete.

Upgrading from Deep Security 8.0 SP2 with In-guest Agent-Based Protection Only

The following upgrade procedures apply to environments (physical or virtual) where Deep Security is providing in-guest Agent-based protection only.

Note: *If you are running Deep Security 8.0 SP2 in a VMware vSphere 4 Environment and you are implementing in-guest Agent-based protection only, only your Deep Security components need to be upgraded to 9.0.*

The Upgrade Procedure

The software installation packages must be downloaded from the Trend Micro Download Center to a location from which they can be imported into the Deep Security Manager.

The procedures for upgrading from Deep Security 8.0 SP2 to Deep Security 9.0 in a physical or virtual environment when providing in-guest Agent-based protection only are as follows:

1. Upgrade the Deep Security Manager from 8.0 SP2 to 9. Follow the same procedures described in [Installing Deep Security Manager \(page 39\)](#).
2. Import the remaining Deep Security 9 installation packages. Download the Deep Security Agent 9.0, Relay 9.0, Filter Driver 9.0, and Virtual Appliance 9.0 installation packages from the Trend Micro Download Center to a locally accessible computer. Then, in the Deep Security Manager, go to **Administration > Updates > Software Updates** and import the packages.
3. Upgrade your Deep Security Relays. Follow the instructions as described in [Deploying the Deep Security Relay \(page 43\)](#).
4. Upgrade your Deep Security Agents. Follow the instructions described in [Deploying Deep Security Agents \(page 57\)](#).

Upgrading to Deep Security 9.0 with in-guest Agent-based protection only is now complete.

Upgrade Deep Security Agents

Note: *Deep Security Agents 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.*

Deep Security Agents can be upgraded using the Deep Security Manager interface, but the Agent software must first be imported into the Deep Security Manager.

To import Agent software into the Deep Security Manager:

1. In the Deep Security Manager, go to the **Administration > Updates > Software Updates** tab.
2. At the bottom of the page, click on **Open Download Center...** to open a browser window to the Trend Micro Download Center web site.
3. Download the Agent software for platforms you require to a location accessible from the server hosting the Deep Security Manager.
4. Close the Download Center browser window.
5. Back in the Deep Security Manager on the **Software Updates** tab, click **Import Software...** to start the **Import Software** wizard.
6. Use the wizard to navigate to the location where you downloaded the Agents and import them into the Deep Security Manager.

The Agent software is now imported into the Deep Security Manager.

Note: *Once the new software is imported into the Deep Security Manager, depending on how your Alerts are configured, you may get a **Agent Upgrade Recommended** alert for each computer on which the Agent is determined to be out of date.*

To Upgrade Deep Security Agents using the Deep Security Manager:

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

Agent software upgrade is now complete.

Note: *You can manually upgrade the Agents locally on the computer. To do this, follow the instructions in [Install Deep Security Agents \(page 57\)](#).*

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 Deep Security Notifier 8.0 SP2
2. Install Deep Security Notifier 9.0 according to the procedures described in [Installing the Deep Security Notifier \(page 67\)](#).

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

Quick Start

Quick Start: System Configuration

This Quickstart Guide describes the initial basic Deep Security system configuration that is required before you can start protecting your computer resources.

To complete basic Deep Security system configuration, you will need to:

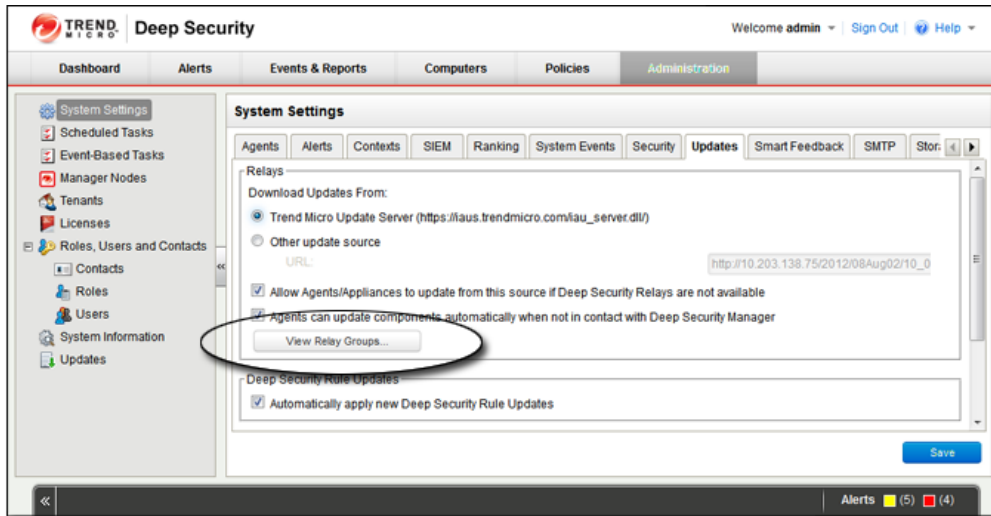
1. Make sure you have at least one Deep Security Relay
2. Configure Deep Security's ability to retrieve Updates from Trend Micro
3. Check that you have a Scheduled Task to perform regular Updates
4. Set up email notification of important events

Make sure you have at least one Deep Security Relay

The Deep Security Relay is responsible for retrieving Security Updates from Trend Micro and distributing them to your protected computers, therefore you must have at least one Deep Security Relay installed. See [Installing the Deep Security Relay \(page 43\)](#) if you do not.

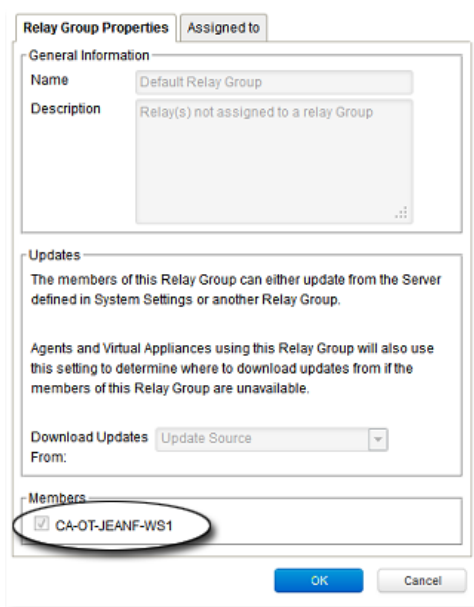
Note: *Relays are always organized into Relay Groups, even if it's a only a group of one. Deep Security has a default Relay Group (named "Default Relay Group") to which all new Relays are assigned. You can create multiple Relay Groups if you have a large number of computers and want to create a hierarchical Relay structure or if your computers are spread out over large geographical areas. For more information on Relay Groups, see [Configuring the Deep Security Relay \(page 121\)](#) and **Relay Groups** in the online help or the Administrator's Guide.*

To view your Deep Security Relays, go to the **Administration > System Settings > Updates** tab and click **View Relay Groups...** in the **Relays** area: (Make sure you are on the **Updates** tab on the **System Settings** page and not the **Updates** page located parallel to the **System Settings** page.)



This will display your current Relay Groups in the **Relay Groups** window. Usually you will only have the single **Default Relay Group**.

Double-click the Default Relay Group to display its **Relay Group Properties** window:



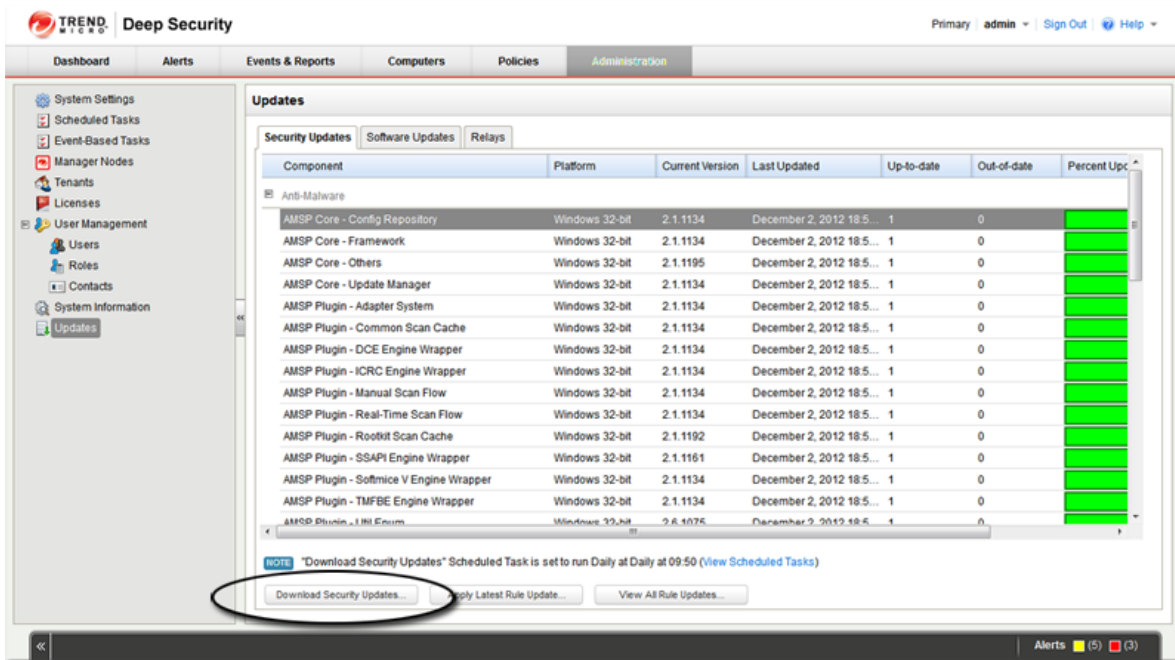
In the Members area of the **Relay Group Properties** window you'll see the Relays that are members of the group.

Note: If there are no computers in the Members area see [Installing the Deep Security Relay \(page 43\)](#) and [Configuring the Deep Security Relay \(page 121\)](#).

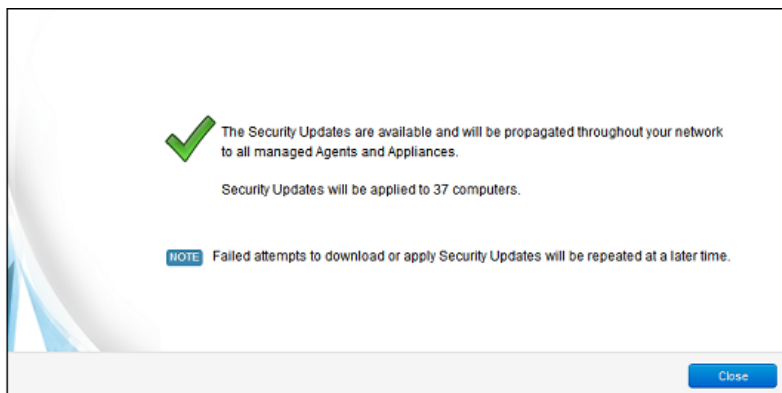
Configure Deep Security's ability to retrieve Updates from Trend Micro

Now that you've confirmed that you have a Relay, you can find the Relay in your Computers list and check that it can retrieve updates from Trend Micro.

Go to the **Administration > Updates > Security Updates** tab and click the **Download Security Updates ...** button.



This will display the **Security Update Wizard** which contacts the Trend Micro Update Servers and downloads the latest Security Updates and distributes them to your computers. If upon completion the wizard displays the success message it means your Relay can communicate with the Update servers:

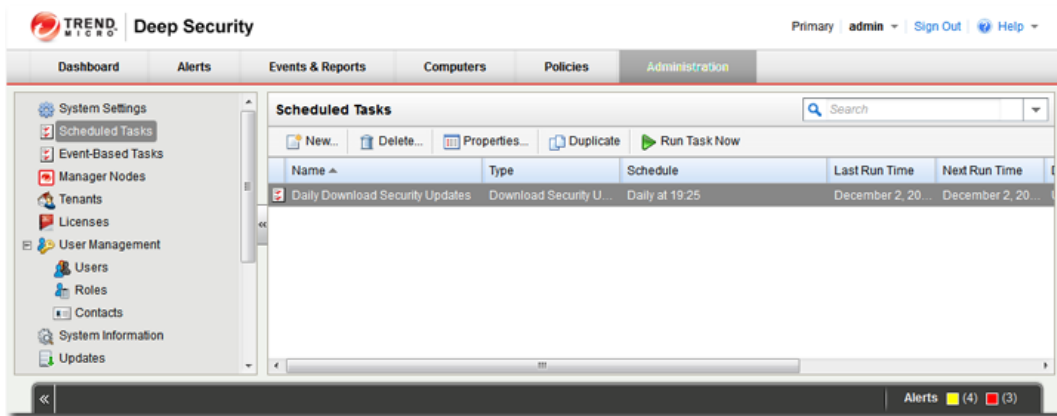


Note: If your Relays are unable to update their Components, see [Installing the Deep Security Relay \(page 43\)](#) and [Configuring the Deep Security Relay \(page 121\)](#).

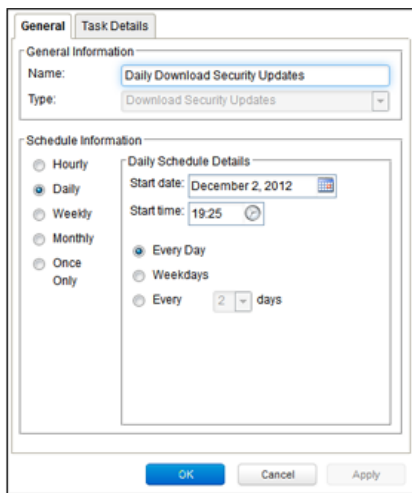
Check that you have a Scheduled Task to perform regular Updates

Now that you know your Relay can communicate with the Update servers, you should create a Scheduled Task which will regularly retrieve and distribute security Updates.

Go to **Administration > Scheduled Tasks**. There you should see at least one Scheduled Task called **Daily Download Security Updates**:



Double-click the Scheduled Task to view its **Properties** window:



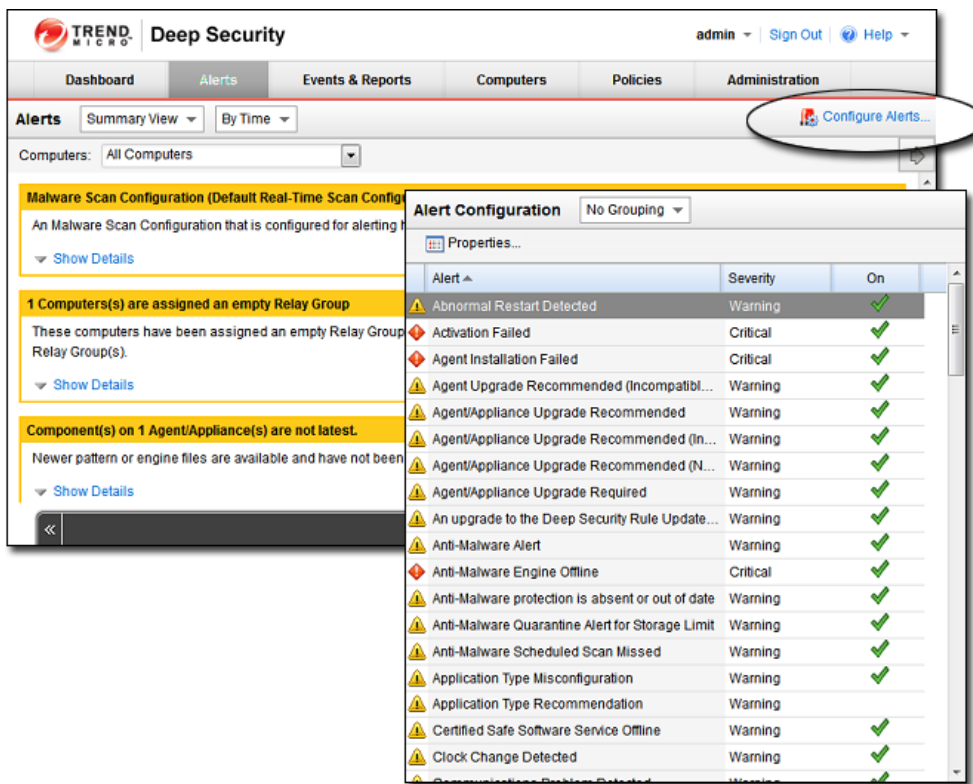
Notice that (in this case) the **Download Security Updates** Scheduled Task is set to perform a Security Update everyday at 19:25.

Note: If you don't have a **Download Security Updates** Scheduled Task in your list, you can create one by clicking on **New** on the Scheduled Task page menu bar and following the instructions in the **New Scheduled Task** wizard.

Set up email notification of important events

Deep Security Alerts are raised when situations occur that require special attention. Alerts can be raised due to security Events such as the detection of malware or an abnormal restart on a protected computer, or they can be system events like the Deep Security Manager running low on disk space. Deep Security can be configured to send email notifications when specific Alerts are raised.

To configure which Alerts will generate an email notification, go to the **Alerts** page and click **Configure Alerts...** to display the list of Deep Security Alerts:



Double-click on an Alert see its **Properties** window where you can set the Alert options for email notification:

General

Alert Information

Alert: Anti-Malware Alert

Description: An Malware Scan Configuration that is configured for alerting has raised an event on one or more computers.

Dismissible: Yes

☒ On

When on, the alert will be raised when the conditions are met.

Options

Severity: Warning

☐ Alert for all rules (Regardless of rule settings)

☒ Send Email to notify when this alert is raised.

☒ Send Email to notify when conditions for this alert change (such as the # of items).

☒ Send Email to notify when this alert no longer exists.

☐ Off

When off, the alert will not be raised. Use this setting if you do not wish this condition to raise an alert.

OK Cancel Apply

Now you need to configure your User account to receive the email notifications Deep Security will send out. Go to **Administration > User management > Users** and double-click on your User account to display its **Properties** window. Go to the **Contact Information** tab and enter an email address and select the **Receive Alert Emails** option:

TREND MICRO Deep Security

Primary | admin | Sign Out | Help

Dashboard Alerts Events & Reports Computers Policies Administration

System Settings
Scheduled Tasks
Event-Based Tasks
Manager Nodes
Tenants
Licenses
User Management
Users
Roles
Contacts
System Information
Updates

Users By Role Search

New... Delete... Properties... Set Password... Synchronize with Directory

Username	Name	Locked Out	Signed In	Last Sign In
admin				April 27, 2013 14:13
marion				April 17, 2013 15:51

Full Access (2)

marion

Contact Information

Phone Number:

Mobile Number:

Pager Number:

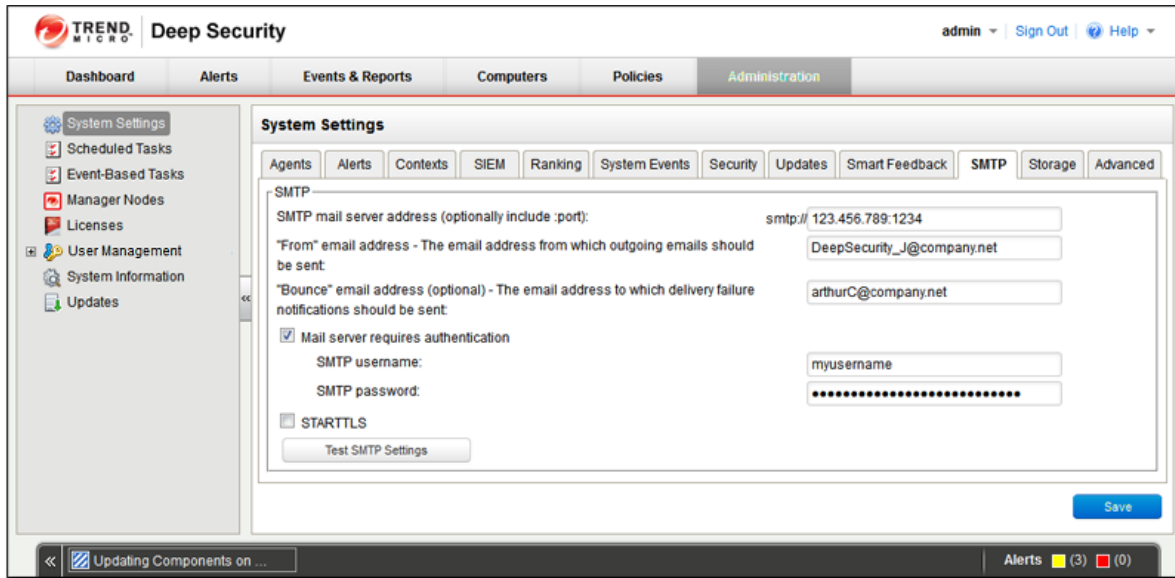
Email Address: jean_francœur@trendmicro.com

☒ Primary Contact

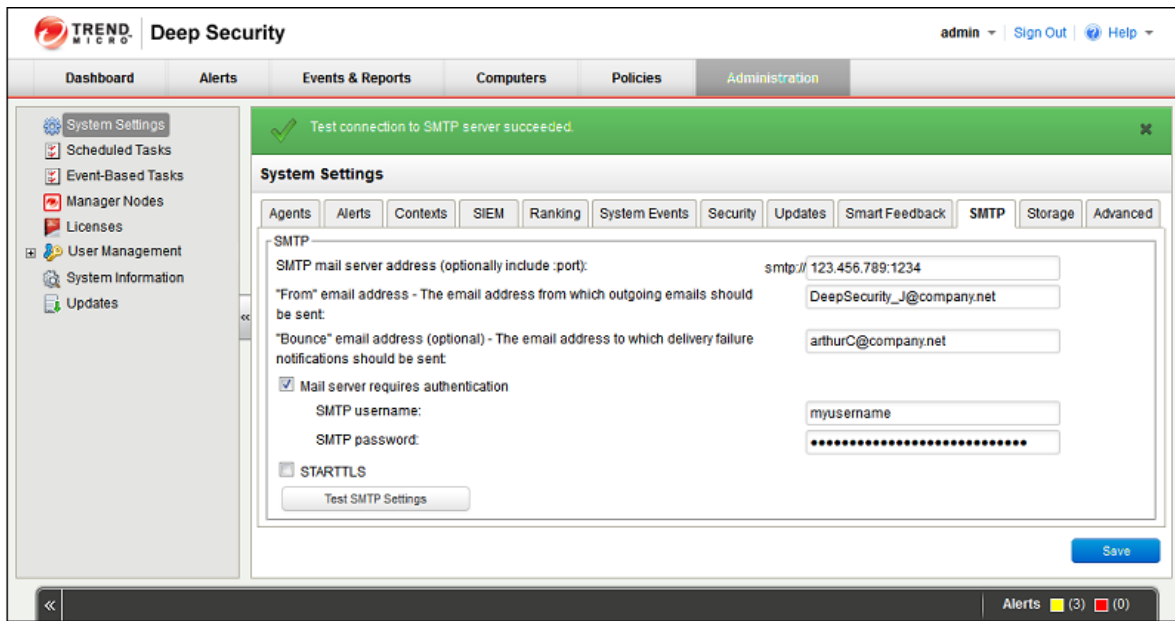
☒ Receive Alert Emails

OK Cancel Apply

In order for Deep Security to send email notification it has to be able to communicate with an SMTP server (access to an SMTP server is a requirement for email notifications). To connect the Deep Security Manager to your SMTP server, go to the **Administration > System Settings > SMTP** tab:



Complete the required fields in the **SMTP** area press test SMTP Settings at the bottom of the page when you're done. you should see a **Test connection to SMTP server succeeded** message:



Note: If you unable to connect with your SMTP server, make sure the the Manager can connect with the SMTP server on port 25.

Basic Configuration is complete

This completes the basic Deep Security system configuration. Deep Security is now configured to regularly contact Trend Micro for security Updates and distribute those Updates on regular basis, and it will send you email notifications when Alerts are raised. Now you need to apply Deep Security protection to your computers.

See [*QuickStart: Protecting a Server \(page 110\)*](#) or **QuickStart: Protecting a Mobile Laptop** in the online help or the Administrator's Guide for a quick guide to protecting those two kinds of computer resources.

Quick Start: Protecting a Server

The following describes the steps involved in using Deep Security to protect a Windows Server 2008 computer.

It will involve the following steps:

1. Adding the computer to the Deep Security Manager.
2. Configuring and running a Recommendation Scan
3. Automatically implement scan recommendations
4. Create a Scheduled task to perform regular Recommendation Scans
5. Monitor Activity Using the Deep Security Manager

Note: *We will assume that you have already installed the Deep Security Manager on the computer from which you intend to manage the Deep Security Agents/Appliances throughout your network. We will also assume that **you have installed (but not activated) Deep Security Agent on the computer you wish to protect** or that you have deployed and activated Deep Security Appliances on the ESXi hosts on which are running the VMs you intend to protect. And finally, we will assume that you have a Deep Security Relay installed from which Deep Security can download the latest Security Updates. If any of these requirements are not in place, consult the Installation Guide for instructions to get to this stage.*

Adding the computer to the Deep Security Manager

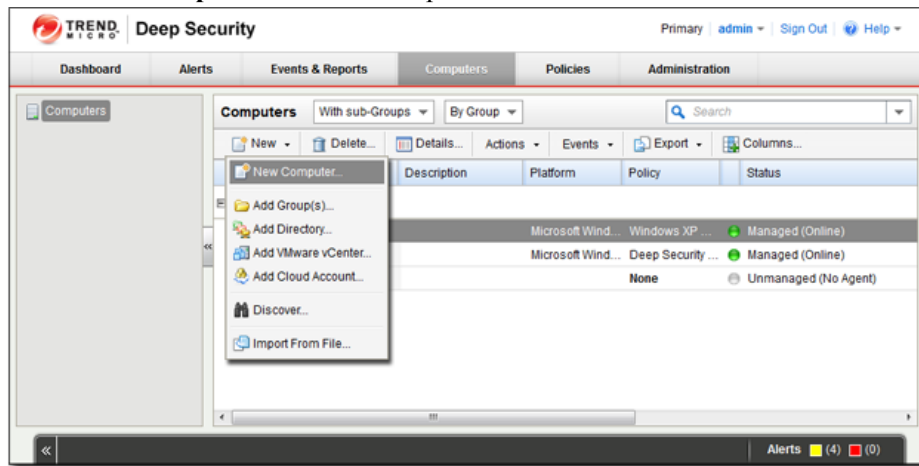
There are several ways of adding computers to the Deep Security Manager's **Computers** page. You can add computers by:

- Adding computers individually from a local network by specifying their IP addresses or hostnames
- Discovering computers on a local network by scanning the network
- Connecting to a Microsoft Active Directory and importing a list of computers
- Connecting to a VMware vCenter and importing a list of computers
- Connecting to computing resources from the following Cloud Provider services:
 - Amazon EC2
 - VMware vCloud

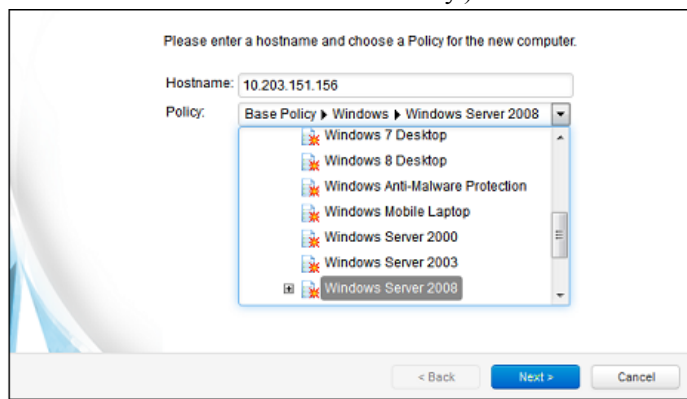
For the purposes of this exercise, we will add a computer from a local network but once a computer is added to the Manager, the protection procedures are the same regardless of where the computer is located.

To add a computer from a local network:

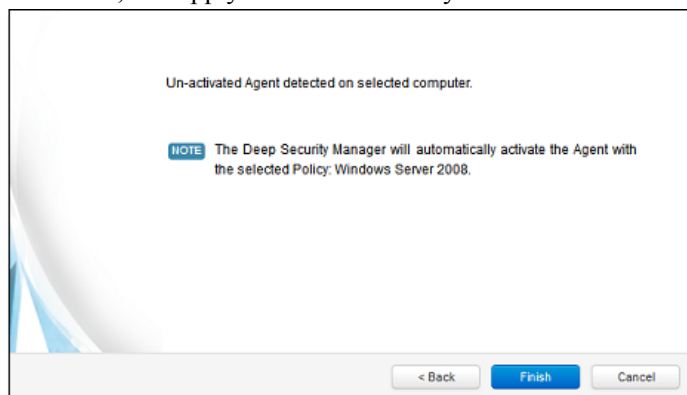
1. In the Deep Security Manager console, go to the **Computers** page and click **New** in the toolbar and select **New Computer...** from the drop-down menu.



2. In the **New Computer** wizard, enter the hostname or IP address of the computer and select an appropriate security Policy to apply from the Policy tree in the drop-down menu. (In this case we will select the **Windows Server 2008** Policy.) Click **Next**.

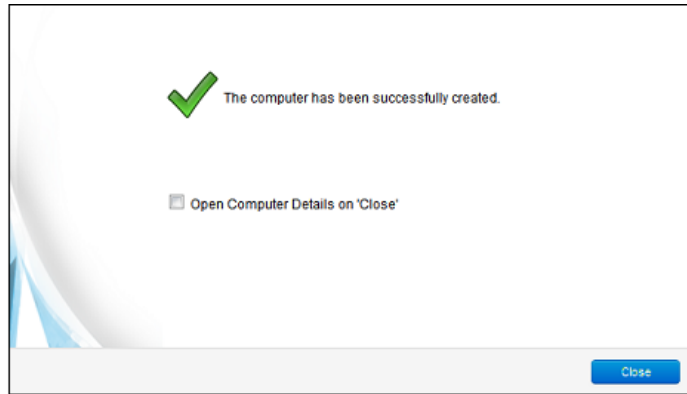


3. The wizard will contact the computer, add it to the Computers page, detect the unactivated Agent, activate it, and apply the selected Policy. Click **Finish**.



Note: An Agent can be configured to automatically initiate its own activation upon installation. For details, see **Command-Line Instructions** in the online help of the Administrator's Guide.

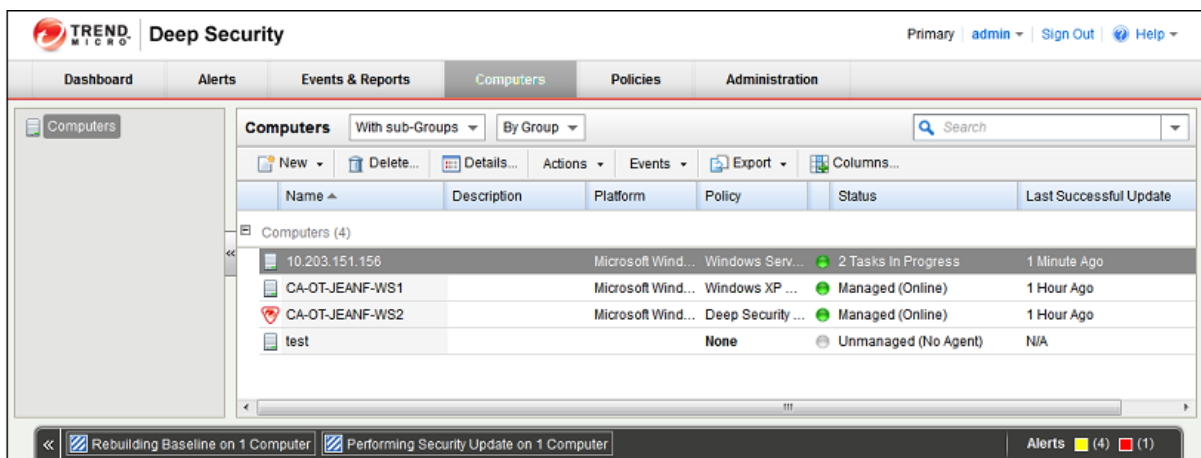
4. When the computer has been added the wizard will display a confirmation message:



5. Leave the **Open Computer Details on 'Close'** option unselected and click **Close**.

The computer now appears in the Deep Security Manager's list of managed computers on the **Computers** page.

Deep Security will automatically download the latest Security Updates to the computer after activation. As well, The **Windows Server 2008** Policy that was assigned to the computer had the we assigned to the computer has Integrity Monitoring enabled and so it will start to Build an Integrity Monitoring baseline for the computer. You can see activities currently being carried out in the status bar of the manager window:



Once Deep Security Manager has completed its initial post-activation tasks the computer's **Status** should display as managed (Online):

Note: More information is available for each page in the Deep Security Manager by clicking the **Help** button in the menu bar.

Configuring and Running a Recommendation Scan

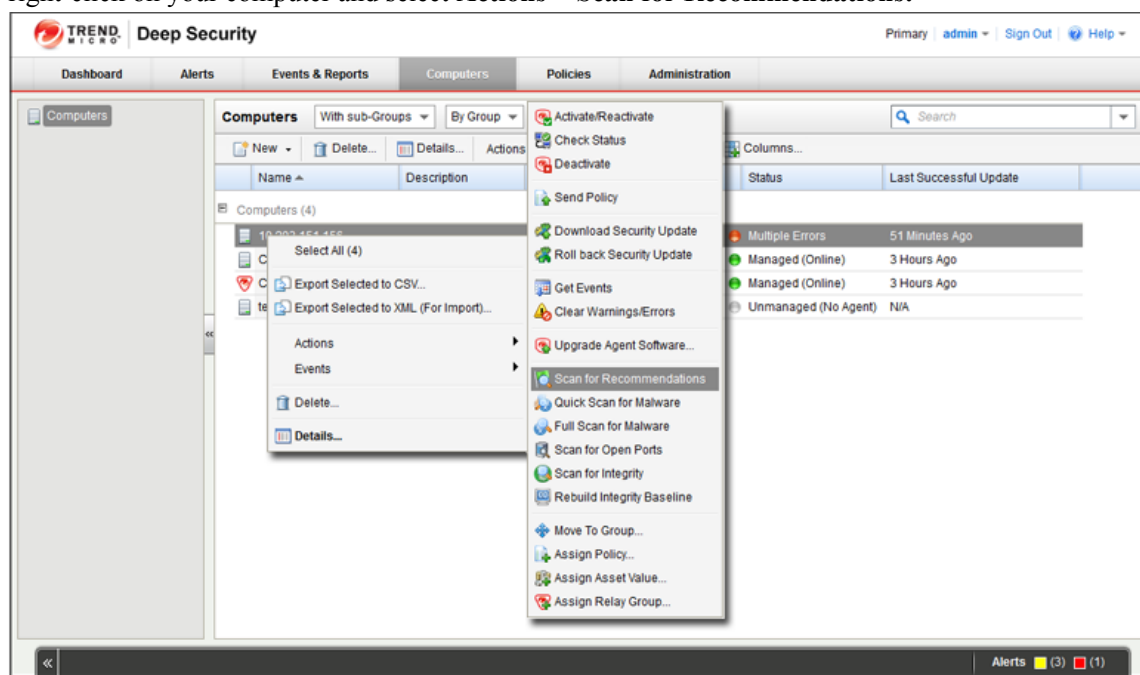
The security Policy that we assigned to the computer is made up of a collection of Rules and settings designed for a computer running the Windows Server 2008 operating system. However, a static Policy can soon fall out of date. This can be because of new software being installed on the computer, new operating system vulnerabilities being discovered for which Trend Micro has created new protection Rules, or even because a previous vulnerability was corrected by an operating system or software service pack. Because of the dynamic nature of the security requirements on a computer, you should regularly run Recommendation Scans which will assess the current state of the computer and compare it against the latest Deep Security protection module updates to see if the current security Policy needs to be updated.

Recommendation Scans make recommendations for the following protection modules:

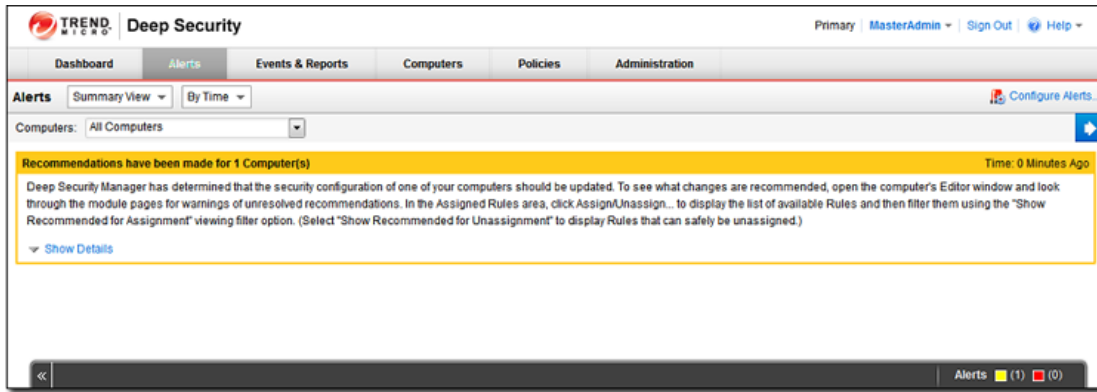
- **Intrusion Prevention**
- **Integrity Monitoring**
- **Log Inspection**

To run a Recommendation Scan on your computer:

1. Go to the Computers page in the main Deep Security manager console window.
2. right-click on your computer and select **Actions > Scan for Recommendations**:



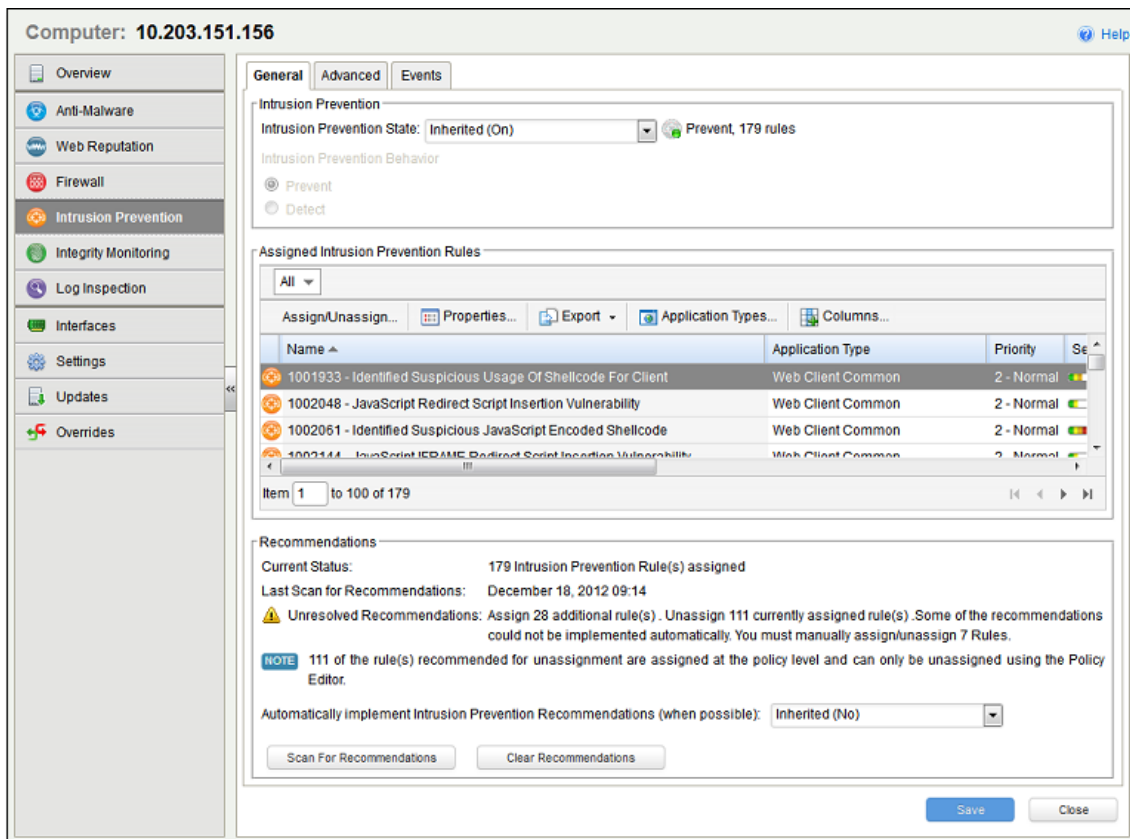
During the Recommendation Scan, your computer's Status will display **Scanning for Recommendations**. When the scan is finished, if deep Security has any recommendations to make, you will see an Alert on the Alerts screen:



To see the results of the Recommendation Scan:

1. Open the computer editor for your computer (**Details...** in the **Computers** page menu bar or from the right-click menu.)
2. In the computer editor window, go to the **Intrusion Prevention** module page.

In the **Recommendations** area of the **General** tab, you'll see the results of the scan:



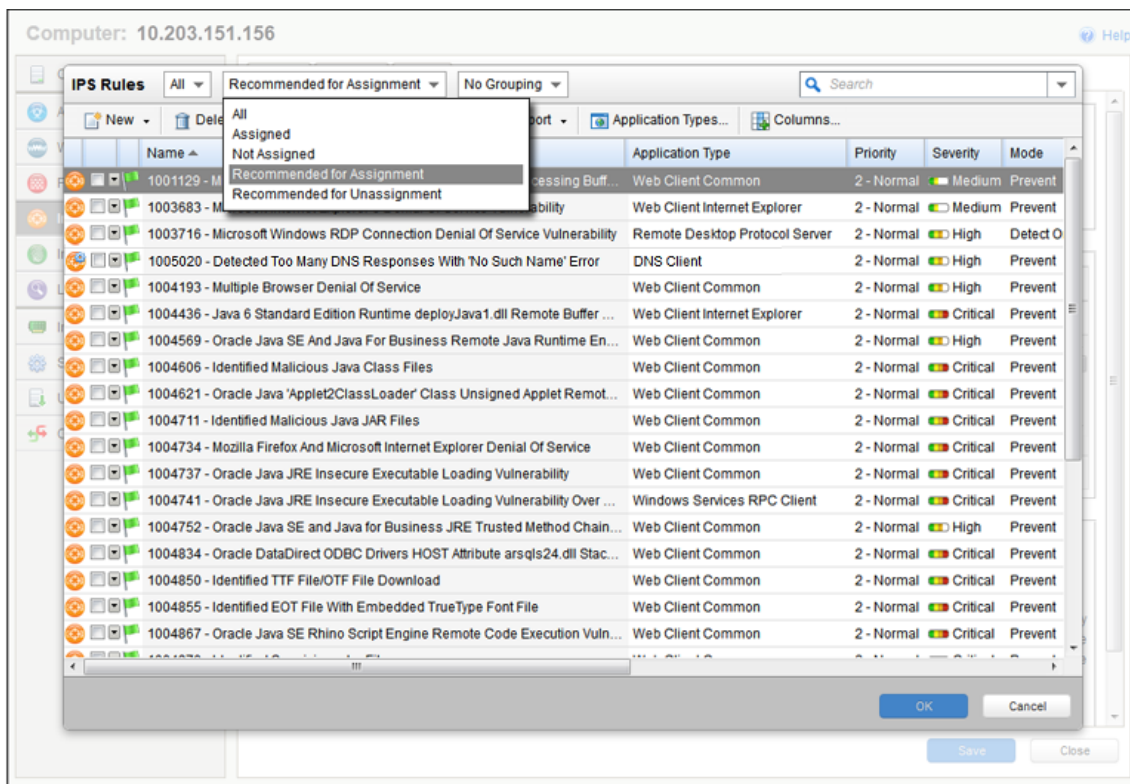
The **Current Status** tells us that there are currently 179 Intrusion Prevention Rules assigned to this computer.

Last Scan for Recommendations tells us that the last scan took place on December 18th, 2012, at 09:14.

Unresolved Recommendations tells us that as a result of the scan, Deep Security recommends assigning an additional 28 Intrusion Prevention Rules and unassigning 111 currently assigned Rules.

The **Note** informs us that 111 of the Rules recommended for unassignment (all of them as it turns out) have been assigned at the Policy level (rather than directly here on the computer level). Rules that have been assigned at a level higher up the Policy tree can only be unassigned in the Policy where they were assigned -- in this case, the **Windows Server 2008** Policy. (If we had opened the **Windows Server 2008** Policy editor, we would have seen the same recommendations and we could have unassigned them from there.)

We are also told that 7 of the Rules that are recommended for assignment can't be automatically assigned. Usually these are either Rules that require configuration or Rules that are prone to false positives and whose behavior should be observed in detect-only mode being enforced in prevent mode. To see which Rules have been recommended for assignment, click **Assign/Unassign...** to display the **IPS Rules** rule assignment modal window. Then select Recommended for Assignment from the second drop-down filter list:



Rules that require configuration are identified by an icon with a small configuration badge (🔧). To see the configurable options for a Rule, double-click the Rule to open its **Properties** window (in local editing mode) and go to the **Configuration** tab. To Assign a Rule, select the checkbox next to its name.

To view Rules that are recommended for *unassignment*, filter the list of Rules by selecting **Recommended for Unassignment** from the same drop-down list. To unassign a Rule, deselect the checkbox next to its name.

Note: Rules that are in effect on a computer because they have been assigned in a Policy higher up the policy tree can't be unassigned locally. The only way to unassign such Rules is to edit the Policy where they were originally assigned and unassign them from there. For more information on this kind of Rule inheritance, see **Policies, Inheritance and Overrides** in the online help or the *Administrator's Guide*.

Automatically implement scan recommendations

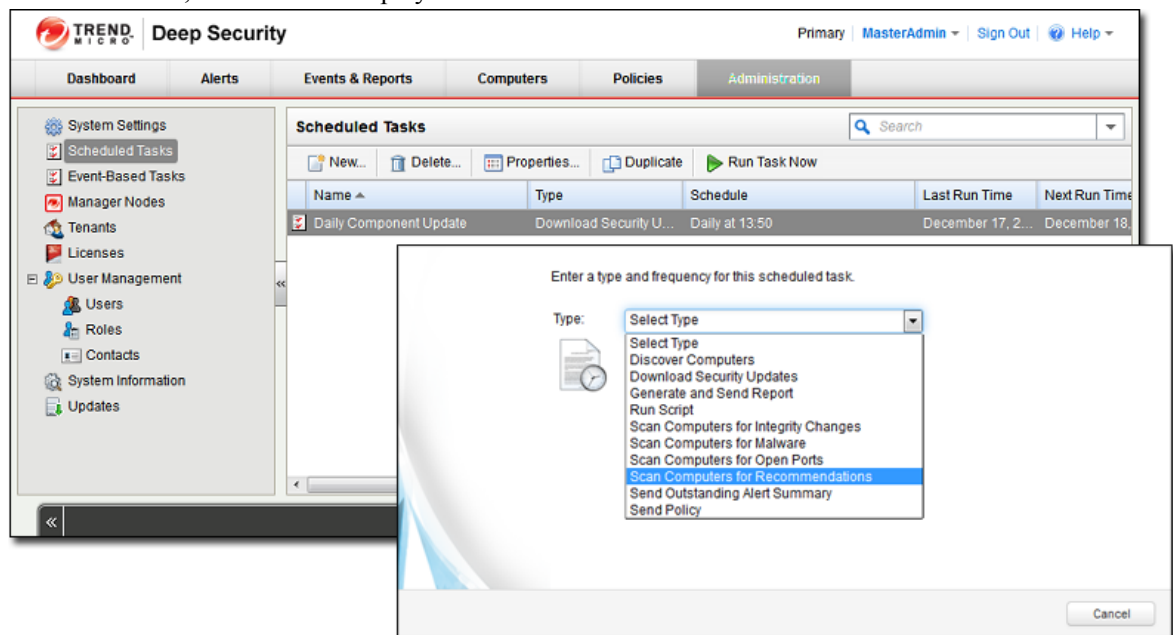
You can configure Deep Security to automatically assign and unassign Rules after a Recommendation Scan. To do so, open the computer or Policy editor and go to the individual protection module pages that support Recommendation Scans (Intrusion, Prevention, Integrity Monitoring, and Log Inspection). In the Recommendation area on the General tab, set **Automatically implement Intrusion Prevention Rule Recommendations:** to Yes.

Create a Scheduled task to perform regular Recommendation Scans

Performing regular Recommendation Scans ensures that your computers are protected by the latest relevant Rule sets and that those that are no longer required are removed. You can create a Scheduled Task to carry out this task automatically.

To create a Scheduled Task:

1. In the main Deep Security Manager window, go to **Administration > Scheduled Tasks**
2. In the menu bar, click **New** to display the **New Scheduled Task** wizard.



3. Select **Scan Computers for Recommendations** as the scan type and select **Weekly** recurrence. Click **Next**.

4. Select a start time, select every 1 week, and select a day of the week. Click **Next**.
5. When specifying which computers to Scan, select the last option (**Computer**) and select the Windows Server 2008 computer we are protecting. Click **Next**.
6. Type a name for the new Scheduled Task. Leave the **Run task on 'Finish'** unchecked (because we just ran a Recommendation Scan). Click **Finish**.

The new Scheduled task now appears in the list of Scheduled Tasks. It will run once a week to scan your computer and make recommendations for you computer. If you have set **Automatically implement Recommendations** for each of the three protection modules that support it, Deep Security will assign and unassign Rules are required. If Rules are identified that require special attention, an Alert will be raised to notify you.

Schedule Regular Security Updates

If you follow the steps described in [Quick Start: System Configuration \(page 102\)](#), your computer will now be regularly updated with the latest protection from Trend Micro.

Monitor Activity Using the Deep Security Manager

The Dashboard

After the computer has been assigned a Policy and has been running for a while, you will want to review the activity on that computer. The first place to go to review activity is the Dashboard. The Dashboard has many information panels ("widgets") that display different types of information pertaining to the state of the Deep Security Manager and the computers that it is managing.

At the top right of the Dashboard page, click **Add/Remove Widgets** to view the list of widgets available for display.

For now, we will add the following widgets from the **Firewall** section:

- Firewall Activity (Prevented)
- Firewall IP Activity (Prevented)
- Firewall Event History (2x1)

Select the checkbox beside each of the three widgets, and click **OK**. The widgets will appear on the dashboard. (It may take a bit of time to generate the data.)

- The **Firewall Activity (Prevented)** widget displays a list of the most common reasons for packets to be denied (that is, blocked from reaching a computer by the Agent on that computer) along with the number of packets that were denied. Items in this list will be either types of Packet Rejections or Firewall Rules. Each "reason" is a link to the corresponding logs for that denied packet.

- The **Firewall IP Activity (Prevented)** widget displays a list of the most common source IPs of denied packets. Similar to the **Firewall Activity (Prevented)** widget, each source IP is a link to the corresponding logs.
- The **Firewall Event History (2x1)** widget displays a bar graph indicating how many packets were blocked in the last 24 hour period or seven day period (depending on the view selected). Clicking a bar will display the corresponding logs for the period represented by the bar.

Note: Note the trend indicators next to the numeric values in the **Firewall Activity (Prevented)** and **Firewall IP Activity (Prevented)** widgets. An upward or downward pointing triangle indicates an overall increase or decrease over the specified time period, and a flat line indicates no significant change.

Logs of Firewall and Intrusion Prevention Events

Now drill-down to the logs corresponding to the top reason for Denied Packets: in the **Firewall Activity (Prevented)** widget, click the first reason for denied packets (in the picture above, the top reason is "Out of Allowed Policy"). This will take you to the **Firewall Events** page.

The **Firewall Events** page will display all Firewall Events where the **Reason** column entry corresponds to the first reason from the **Firewall Activity (Prevented)** widget ("Out of Allowed Policy"). The logs are filtered to display only those events that occurred during the view period of the Dashboard (Last 24 hours or last seven days). Further information about the **Firewall Events** and **Intrusion Prevention Events** page can be found in the help pages for those pages.

Note: For the meaning of the different packet rejection reasons, see **Firewall Events and Intrusion Prevention Events** in the online help or the Administrator's Guide .

Reports

Often, a higher-level view of the log data is desired, where the information is summarized, and presented in a more easily understood format. The **Reports** fill this Role, allowing you to display detailed summaries on computers, Firewall and Intrusion Prevention Event Logs, Events, Alerts, etc. In the **Reports** page, you can select various options for the report to be generated.

We will generate a **Firewall Report**, which displays a record of Firewall Rule and Firewall Stateful Configuration activity over a configurable date range. Select **Firewall Report** from the Report drop-down. Click **Generate** to launch the report in a new window.

By reviewing scheduled reports that have been emailed by the Deep Security Manager to Users, by logging into the system and consulting the dashboard, by performing detailed investigations by drilling-down to specific logs, and by configuring Alerts to notify Users of critical events, you can remain apprised of the health and status of your network.

Import Deep Security Software

Note: *Deep Security Manager configuration must be performed by using a Deep Security Manager user account with Full Access rights.*

Import Deep Security Agents

To import Agent software into the Deep Security Manager:

1. In the Deep Security Manager, go to the **Administration > Updates > Software Updates** tab.
2. At the bottom of the page, click on **Open Download Center...** to open a browser window to the Trend Micro Download Center web site.
3. Download the Agent software for platforms you require to a location accessible from the server hosting the Deep Security Manager.
4. Close the Download Center browser window.
5. Back in the Deep Security Manager on the **Software Updates** tab, click **Import Software...** to start the **Import Software** wizard.
6. Use the wizard to navigate to the location where you downloaded the Agents and import them into the Deep Security Manager.

The Agent software is now imported into the Deep Security Manager.

Import Deep Security Filter Driver (DSFD) and Deep Security Virtual Appliance (DSVA) into Deep Security Manager

To import Filter Driver and Virtual Appliance software into Deep Security Manager:

1. In the Deep Security Manager, go to the **Administration > Updates > Software Updates** tab.
2. At the bottom of the page, click on **Open Download Center...** to open a browser window to the Trend Micro Download Center web site.
3. Download the Filter Driver and Virtual Appliance software to a location accessible from the server hosting the Deep Security Manager.
4. Close the Download Center browser window.
5. Back in the Deep Security Manager on the **Software Updates** tab, click **Import Software...** to start the **Import Software** wizard.
6. Browse and Select FilterDriver-ESX_5.0-9.0.0-xxxx.x86_64.zip. Click Next and Finish on the next screen.
7. Click **Import Software...** from Software Updates tab again. Browse and Select Appliance-ESX-9.0.0-xxxx.x86_64.zip Click Next and wait for Software Properties window and select Finish.

***Note:** The package upload may take 5-10 minutes depending on network bandwidth.*

8. Click the View Imported Software and make sure both the Filter Driver and DSVA are imported.

Configuring the Deep Security Relay

Note: *The Deep Security Relay contains a Deep Security Agent which must be activated by the Deep Security Manager before it can be configured.*

Activate the Deep Security Relay

In the Deep Security Manager:

1. From the **Computers** screen, use the New option to add the computer on which the Deep Security Relay is installed, and Activate it.
2. Check that the Relay Agent status is **Managed (Online)**.
3. On the Deep Security Relay computer, open the Deep Security Notifier and check the status is OK.

Configure Updates via the Relay

In the Deep Security Manager:

1. Go to **Administration > System Settings > Updates**.
2. Click the **View Relay Groups** button.
3. On the Relay Groups window, click **New**, and create a new relay group, checking the newly added Relay Agent computer in the Members section. Click **OK**.
4. Go to **Administration > System Settings > Updates**. You should see the newly added Relay as a member of the Relay Group in the Relays section.
5. In the **Administration > Updates > Security Updates** section, the list of Components will all show **Not updated yet**. Click **Download Security Updates...**, and then in the **Security Update** wizard, click Finish.
6. Downloading the Updates to the Deep Security Relay may take a few minutes.
7. When the **Security Update** wizard shows that the update has completed, click Finish.
8. Return to **Administration > System Settings > Updates**. In the Security Updates section, the list of Components will all show **100% Updated**.
9. On the Deep Security Relay computer, open the Deep Security Notifier and you will see that the Components list has been updated.

Deep Security Agents and Appliances can be configured to either pull the updates from Deep Security Relays or directly from the Trend Micro Update Server.

Use the **Administration > System Settings > Updates** screen to configure Deep Security Relays.

To assign a Relay to an Agent/Appliance, go to the **Computers** screen, right-click the Computer and from the Actions menu, select **Assign Relay Group**.
















































Appendices

























Supported Features by Platform

The following tables list which Deep Security 9 features are supported on which platforms.

Note: The features listed in the Virtual Appliance column represent those functions that the Virtual Appliance can perform on agentless virtual machines.

Deep Security Manager 9.0 SP1

Modules	Features	DS Agents 9.0 SP1					DS Virtual Appliance 9.0 SP1	
		Windows	Linux	Solaris	AIX	HP-UX	ESXi 5.x, Windows guest	ESXi 5.x, Linux guest
Anti-Malware	File Scan							
	Registry Scan							
	Memory Scan							
	Smart Scan							
	Real Time							
		Windows	Linux	Solaris	AIX	HP-UX	ESXi 5.x, Windows guest	ESXi 5.x, Linux guest
Web Reputation Service	All Functions							
		Windows	Linux	Solaris	AIX	HP-UX	ESXi 5.x, Windows guest	ESXi 5.x, Linux guest
Firewall	All Functions							
		Windows	Linux	Solaris	AIX	HP-UX	ESXi 5.x, Windows guest	ESXi 5.x, Linux guest
Intrusion Prevention	Intrusion Prevention							
	Application Control							
	Web Application Protection							
	SSL							
		Windows	Linux	Solaris	AIX	HP-UX	ESXi 5.x, Windows guest	ESXi 5.x, Linux guest
Integrity Monitoring	Files							
	Registry							

Modules	Features	DS Agents 9.0 SP1					DS Virtual Appliance 9.0 SP1	
		Windows	Linux	Solaris	AIX	HP-UX	ESXi 5.x, Windows guest	ESXi 5.x, Linux guest
	Others							
	Real Time Files							
	Real Time Other							
		Windows	Linux	Solaris	AIX	HP-UX	ESXi 5.x, Windows guest	ESXi 5.x, Linux guest
Log Inspection	All Functions							
		Windows	Linux	Solaris	AIX	HP-UX	ESXi 5.x, Windows guest	ESXi 5.x, Linux guest
Recommendation Scan	All Functions							
		Windows	Linux	Solaris	AIX	HP-UX	ESXi 5.x, Windows guest	ESXi 5.x, Linux guest
User Notification	All Functions						 (with Notifier)	

Notes:

- The Linux Agents support Anti-Malware on 64-bit, non-Ubuntu, versions only.

Deep Security Manager Settings Properties File

This section contains information about the contents of the Property file that can be used in a command-line installation of the Deep Security Manager, such as a Windows silent install.

Settings Properties File

The format of each entry in the settings property 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	Notes
LicenseScreen.License.-1=<value>	<AC for all modules>	blank	

OR

Property	Possible Values	Default Value	Notes
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	Notes
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
Dinstall4j.language=<value>	en jp zh_CN	en	"en" = English, "jp" = Japanese, "zh_CN" = Simplified Chinese

UpgradeVerificationScreen

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

Property	Possible Values	Default Value	Notes
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	Microsoft SQL Server	
DatabaseScreen.Hostname=<value>	The name or IP address of the database host Current host name	Current host name	
DatabaseScreen.DatabaseName=<value>	Any string	dsm	Not required for embedded
DatabaseScreen.Transport=<value>	Named Pipes TCP	Named Pipes	Required for SQL Server only

Property	Possible Values	Default Value	Notes
DatabaseScreen.Username=<value>			Not required for Embedded
DatabaseScreen.Password=<value>		blank	Not required for Embedded
DatabaseScreen.SQLServer.Instance=<value>			Blank implies default instance. Optional, required for SQL Server only
DatabaseScreen.SQLServer.Domain=<value>			Optional, required for SQL Server only
DatabaseScreen.SQLServer.UseDefaultCollation=<value>	True False	False	Optional, required for SQL Server only

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>	
AddressAndPortsScreen.ManagerPort=<value>	<valid port number>	4119	
AddressAndPortsScreen.HeartbeatPort=<value>	<valid port number>	4120	
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 indicates that you want Deep Security Manager to automatically retrieve the latest Components
SecurityUpdateScreen.UpdateSoftware=<value>	True False	True	True indicates that you want to setup a task to automatically check for new software.

RelayScreen

This value controls the installation of a co-located Deep Security Relay Server.

Property	Possible Values	Default Value	Notes
RelayScreen.Install=<value>	True False	False	If an appropriate Deep Security Relay install package is found (in the same location as the DSM installer) and this flag is set True then the Relay Server will be installed automatically.
RelayScreen.AntiMalware=<value>	True False	False	Enable anti-malware on the co-located relay
RelayScreen.Proxy=<value>	True False	False	Define a proxy for use by the co-located relay (to access the iAU server)
RelayScreen.ProxyType=<value>	SOCKS4 SOCKS5 HTTP	HTTP	Define the protocol used by the relay proxy
RelayScreen.ProxyAddress=<value>	<String>		The host name or IP address of the relay proxy
RelayScreen.ProxyPort=<value>	<Number>		The port number of the relay proxy
RelayScreen.ProxyAuthentication=<value>	True False	False	The relay proxy requires authentication
RelayScreen.ProxyUsername=<value>	<String>		The user name sent as part of the relay proxy authentication handshake
RelayScreen.ProxyPassword=<value>	<String>		The password sent as part of the relay proxy authentication handshake

Some parameters are dependent on others. For example:

- If **RelayScreen.Install** is false then none of the other values are required.
- If **RelayScreen.Proxy** is false then none of the other proxy values are required.
- If **RelayScreen.ProxyAuthentication** is false then the username and password are not required.

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

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...
```

```
Detecting previous versions of Trend Micro Deep Security Manager...
```

```
Upgrade Verification Screen settings accepted...
```

```
Database Screen settings accepted...
```

```
License Screen settings accepted...
```

```
Address And Ports Screen settings accepted...
```

```
Credentials Screen settings accepted...
```

```
All settings accepted, ready to execute...
```

```
Uninstalling previous version
```

```
Stopping Services
```

```
Extracting files...
```

```
Setting Up...
```

```
Connecting to the Database...
```

```
Creating the Database Schema...
```

```
Updating the Database Data...
```

```
Creating MasterAdmin Account...
```

```
Recording Settings...
```

```
Creating Temporary Directory...
```

```
Installing Reports...
```

```
Creating Help System...
```

```
Setting Default Password Policy...
```

```
Importing Example Security Profiles...
```

```
Applying Security Update...
```

```
Assigning IPS Filters to Example Security Profiles...
```

```
Correcting the Port for the Manager Security Profile...
```

```
Correcting the Port List for the Manager...
```

```
Creating IP List to Ignore...
```

```
Creating Scheduled Tasks...
```

```
Creating Asset Importance Entries...
```

```
Creating Auditor Role...
```

```
Auditing...
```

```
Optimizing...
```

```
Recording Installation...
```

```
Creating Properties File...
```

```
Creating Shortcut...
Configuring SSL...
Configuring Service...
Configuring Java Security...
Configuring Java Logging...
Cleaning Up...
Starting Deep Security Manager...
Finishing installation...
```

Failed Install

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

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

Deep Security Manager Memory Usage

Configuring the Installer's Maximum Memory Usage

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

To configure the amount of RAM available to the installer:

1. Go to the directory where the installer is located.
2. Create a new text file called "Manager-Windows-9.0.xxxx.x64.vmoptions" or "Manager-Linux-9.0.xxxx.x64.vmoptions", depending on your installation platform (where "xxxx.xxx" is the build number of the installer and platform).
3. Edit the file by adding the line: "-Xmx800m" (in this example, 800MB of memory will be made available to the installer.)
4. Save the file and launch the installer.

Configuring the Deep Security Manager's Maximum Memory Usage

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

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

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

Deep Security Virtual Appliance Memory Usage

The following table lists minimum recommended Deep Security Virtual Appliance memory allocation based on the number of VMs being protected:

Number of virtual machines being protected by the Deep Security Virtual Appliance	Recommended memory allocation
1 - 32 VMs	2GB
33 - 64 VMs	4GB
65+ VMs	8GB

Configuring the Deep Security Virtual Appliance's Memory Allocation

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

To configure the Deep Security Virtual Appliance's memory allocation:

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

Performance Features

Performance Profiles

As of Deep Security Manager 7.5 SP1, a new system for optimizing the performance of Manager-initiated and Agent/Appliance-initiated operations is available. Previously the Manager processed all operations in a fixed amount of concurrent jobs using a first-in first-out system. This has been replaced with an optimized concurrent 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 DSM 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 > System Information** and clicking the **Managers...** button in the toolbar. From this screen select the desired 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 amount 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 will not restart until the available disk space is greater than 5MB.

You must restart the Manager manually.

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

Creating an SSL Authentication Certificate

The Deep Security Manager creates a 10-year self-signed certificate for the Web browser-to-Manager connections. If required, this certificate can be replaced with a certificate from a trusted certificate authority. (The certificate is maintained after a Deep Security Manager upgrade.)

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

To create your SSL authentication certificate:

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

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

5. Choose password: **changeit**

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.*

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" and the second is the CA certificate itself.

10. 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"
```

11. 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)

12. 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
```

13. 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
```

14. Copy the .keystore file from your user home directory **C:\Documents and Settings\Administrator** to **C:\Program Files\Trend Micro\Deep Security Manager**
15. 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$85ef650a5c40bb0f914993ac1ad855f48216fd0664ed2544bbec6de80160b2
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 SSL certificate is signed by your CA.

Minimum VMware Privileges for DSVA Deployment

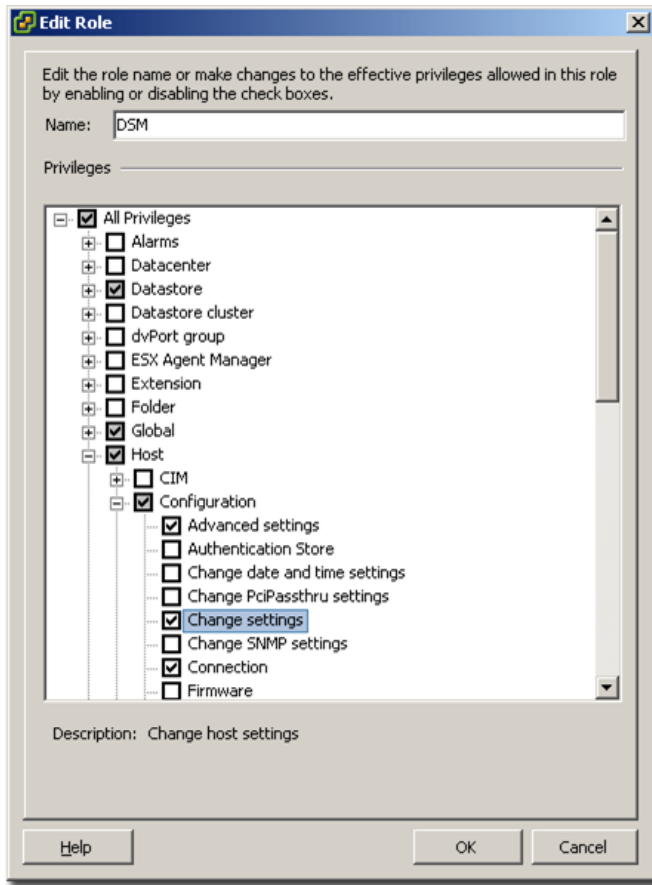
The following tables list the VMware environment privileges required by the VMware role assigned to the account used by the Deep Security Manager to deploy the Deep Security Virtual Appliance. (The account used to connect to the vCenter when importing the vCenter into the Deep Security Manager.)

These privileges must be applied at the data center level in the Hosts and Clusters view. Installation requires the ability to fetch the parent IDs of various entities. Applying the privileges at the cluster level only will generate errors.

The tables are divided into the following four stages:

1. **Preparing the ESXi host.** A kernel driver is loaded on the ESXi host, and a separate vSwitch is configured to facilitate internal connectivity for the DSVA.
2. **Deploying the Virtual Appliance.** The virtual appliance itself is deployed from an OVF file.
3. **Using the Deep Security Manager to activate the Virtual Machine.** The computer being protected by the Virtual Appliance is registered with the Deep Security Manager and secure communications are established.
4. **Ongoing operations.** Day to day Deep Security operations.

The tables list the required privilege and the function for which the privilege is required. To set the privilege, use the vSphere Client to edit the properties of the role used by the Deep Security Manager to access the vCenter. The required privileges can be found in the Privileges tree of the VMware Role Editor. For example, the following screen shot shows the location of the **Host > Configuration > Change Settings** privilege:



Preparing the ESXi Host

Privilege	Function
Host > Configuration > Change Settings	Query Modules on ESXi
Host > Configuration > Maintenance	Enter and Exit Maintenance Mode
Host > Configuration > Network Configuration	Add new virtual switch, port group, virtual NIC etc.
Host > Configuration > Advanced Settings	Setup networking for dvfilter communication on ESXi
Host > Configuration > Query Patch	Install Filter Driver
Host > Configuration > Connection	Disconnect/reconnect a host
Host > Configuration > Security profile and firewall	Reconfiguration outgoing FW connections to allow retrieval of Filter Driver package from DSM
Global > Cancel Task	Required to cancel a task if required

Deploying the Virtual Appliance

Privilege	Function
vApp > Import	Deploy DSVa from OVF file
vApp > vApp application configuration	Upgrade the DSVa
Datastore > Allocate Space	Allocate space for DSVa on datastore.
Host > Configuration > Virtual machine autostart configuration	Set DSVa to autostart on ESXi
Network > Assign Network	Assign DSVa to networks
Virtual Machine > Configuration > Add new disk	Add disks to DSVa
Virtual Machine > Interaction > Power On	Power on DSVa
Virtual Machine > Interaction > Power Off	Power off DSVa

Deploying into a DRS-enabled Cluster

Privilege	Function
Host > Inventory > Modify Cluster	Deploy DSVa to DRS-enabled cluster.

Activating the Virtual Machine (the protected computer)

Privilege	Function
Virtual Machine > Configuration > Advanced	Reconfigure virtual machine for dvfilter

Ongoing Operations

Privilege	Function
Host > Configuration > Change Settings	Query Modules on ESXi
Virtual Machine > Configuration > Advanced	Reconfigure virtual machine for dvfilter

Uninstalling Deep Security

Note: When you uninstall an activated Agent or a Relay 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 from the Manager before uninstallation, or simply delete the computer from the list.

To remove the Deep Security Virtual Appliance

To remove the Virtual Appliance:

1. Use the Deep Security Manager to "deactivate" the Virtual Appliance.
2. Log in to vCenter.
3. Stop the Appliance.
4. Delete from disk.

To remove the Deep Security Filter Driver from a prepared ESXi

To restore the ESXi to its "un-prepared" state:

1. From the Deep Security Manager Computers list, select the Virtual Center. Choose the Prepared Computer for un-deployment, right-click the Computer and select Restore ESX.
2. Follow the wizard steps, accepting the defaults.
3. Choose **"Yes"** to have the DSM handle the ESXi driver un-installation automatically.

Note: The Deep Security Manager will attempt to bring the ESXi into and out of maintenance mode automatically. Any running virtual machines will need to be manually shutdown. At the end of the uninstallation process, the ESXi will be automatically rebooted and brought out of maintenance mode.

Or

4. Choose **"No"** to manually put the ESXi into /out of maintenance mode.

Note: The Deep Security Manager wizard will start the uninstallation of the Filter Driver automatically once the ESXi has been put into maintenance mode. At the end of the uninstallation process, the ESXi will be automatically re-booted but remain in maintenance mode.

To uninstall the Deep Security Relay

Note: Remember that before uninstalling a Deep Security Relay, 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 > Computer**. 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 Relay (Windows)

From the Windows Control Panel, select Add/Remove Programs. Double-click Trend Micro Deep Security Relay 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 Relay (Linux)

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

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

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

Note: Remember to remove the Relay 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, 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 > Computer**. 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)

Enter the following:

```
pkgrm 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"**).

Frequently Asked Questions

***Note:** Please consult the Deep Security Deep Security Manager, Deep Security Virtual Appliance, or Deep Security Agent readme files for any issues not addressed in the Troubleshooting or FAQs sections.*

Where can I download the installer packages for Deep Security 9.0?

The Trend Micro Download Center: <http://downloadcenter.trendmicro.com>

Where can I download the technical documents for Deep Security 9.0?

The Trend Micro Download Center: <http://downloadcenter.trendmicro.com>. On the Download Center page, click on the name of the Deep Security software you are interested in and then click the "+**More Details**" link to see the documentation available.

What is the default username and password to log into the Deep Security Manager console?

You are prompted for a username and password during installation. The default username to log in to the Manager Console is "MasterAdmin" (no quotes). There is no default password. Both this and the password are set during the installation. The username IS NOT case-sensitive. However, the password IS case-sensitive.

Can I reset the Manager console login password?

Yes. You can reset or change the Manager console login password. Go to **Administration > User Management > Users**, right-click on the User and select **Set Password...**

How can I unlock a locked out User?

In the Manager, go to **Administration > User Management > Users**, right-click on the User and select **Unlock User(s)**.

To unlock a User from the Manager host command line, enter the following from the Deep Security Manager's install directory:

```
dsm_c -action unlockout -username USERNAME [-newpassword NEWPASSWORD]
```

where **USERNAME** is the User's username. Optionally, use "-newpassword" to set a new password for the User.

Can I use my domain account credentials when logging on to the Manager console?

Yes. Go to **Administration > User Management > Users** and select **Synchronize with Directory**.

How can I mass-deploy the Agents to the computers being protected?

Organizations typically use existing enterprise software distribution systems such as Microsoft System Center or Novell ZENworks to install Agents.

Can I still use my existing license or activation code when upgrading to version 9.0?

Yes, your existing protection modules will be still be activated.

Can I uninstall the DS Agents from the Manager console?

No. You can de-activate an Agent/Appliance from the DSM, but you must uninstall locally.

What is the end of life or support policy for Deep Security?

- Product support is provided 2 years after a release, or
- Product support is provided for 18 months after a subsequent release, whichever time period is longer

How do I deactivate the DS Agent from the command line?

See the Administrator's Guide or online help section **Manually Deactivate/Stop/Start the Agent/Appliance**. It is platform dependent.

How can I manually update the DS Agent that has no connection with the DS Manager?

Updating the Agent is not possible without connection to the Manager, since the Manager must send the security configuration details to the Agent.

Troubleshooting

Note: Please consult the *Deep Security Manager*, *Deep Security Agent* and *Deep Security Virtual Appliance "readme"* files for any issues not addressed in the *Troubleshooting* or *FAQs* sections.

Deep Security Manager

Installation

Problem

Experiencing problems installing two Deep Security Managers on the same machine.

Solution

Only one instance of the Deep Security Manager can be installed on any given machine.

Problem

Unable to install or upgrade the Deep Security Manager.

Solution

During installation or upgrade of the Deep Security Manager the service may fail to install properly if the Services screen is open on some platforms. Close the services screen prior to installation or upgrade of Deep Security Manager.

If the problem persists, reboot the computer.

Communications

Problem

The Agent protecting the Deep Security Manager is generating "Renewal" errors, and/or you cannot connect remotely to the Deep Security Manager.

Solution

After applying the "Deep Security Manager" Security Profile, you may notice that the Deep Security Agent will return numerous "Renewal Error" IPS Events. This is because the Agent cannot inspect the SSL Traffic that existed before the "Deep Security Manager" Security Profile and its SSL Host Configuration was applied. It is recommended that all browser sessions to the Deep Security Manager be restarted after applying the "Deep Security Manager" Security Profile.

Problem

"Communications Problem Detected" Alert on a computer managed by the Deep Security Manager.

or

Offline Bundle.zip error when preparing the ESXi.

or

Offline Bundle.zip error when deploying the Deep Security Virtual Appliance.

or

Protocol Error when activating the Deep Security Appliance.

Solution

If you encounter any of the above situations it may be that a computer being managed by the Deep Security Manager is unable to resolve the hostname of the computer hosting the Deep Security Manager.

To ensure the Deep Security Manager is able to resolve the hostname of the computer hosting the Deep Security Manager:

1. Log in to the Deep Security Manager that is managing the Agent
2. Go to **Administration > System Information** and in the **System Details**, view the Manager Node entry and note the hostname
3. Log in to the computer that is having communication problems
4. Perform an nslookup using the name from step 2
5. If the nslookup fails you must modify the hosts file on the computer to use the DSM hostname with the correct IP address or update the DNS entry for the Deep Security Manager machine on the specified DNS server

Configuration

Note: *To change the hosts file on the Virtual Appliance you must log in via vCenter. Once in the console press ALT+F2 to get to the console login screen. Then type: `sudo vi /etc/hosts`*

Problem

Traffic Analysis is not working.

Solution

Stateful Configuration must be on, with TCP and UDP logging enabled.

Problem

Many IPS rules are being triggered on the Agent protecting the database used by Deep Security Manager.

Solution

When using Deep Security Manager with a database on a remote computer that is running a Deep Security Agent (DSA) there is a possibility of IPS false positives. The false positives are caused by the contents of the IPS Rules (when saving to the database) triggering the IPS Rules running on the DSA. The workaround is to either create a bypass Firewall Rule to apply to the database server with the source IP being the static IP of Deep Security Manager or to enable encryption on the database channel. SQL Server can be encrypted by adding:

```
database.SqlServer.ssl=require
```

to **\webclient\webapps\ROOT\WEB-INF\dsm.properties** and restart the Deep Security Manager service.

Problem

Port scans show ports 25 and 110 are open regardless of which Firewall Rules I implement to close them.

Solution

The presence of Norton Antivirus may interfere with scan results. Norton AV filters ports 25 and 110 to check incoming and outgoing email for viruses. This can cause erroneous scan results if the Manager is installed on a machine with email scanning enabled since ports 25 and 110 will always appear to be open regardless of any filters placed on the host.

Problem

Port scans show ports 21, 389, 1002, and 1720 are open regardless of which Firewall Rules I implement to close them.

Solution

If Windows Firewall is enabled on the Deep Security Manager it may interfere with port scans causing false port scan results. Windows Firewall may proxy ports 21, 389, 1002, and 1720 resulting in these ports always appearing open regardless of any filters placed on the host.

Deep Security Virtual Appliance

Deployment

Problem

Timeout when preparing the ESXi.

Solution

In order for the Filter Driver to be successfully installed, the ESXi it is being deployed to must be rebooted. The Deep Security Manager offers the option to automatically reboot the server. If this selection is chosen all virtual machines on the ESXi host must be paused/stopped or vMotioned off of the box. If this is not done the ESXi cannot be put in to maintenance mode and cannot be rebooted. The Deep Security Manager will report a timeout issue if the ESXi cannot be put in to maintenance mode.

Problem

Cannot contact the Deep Security Virtual Appliance.

Solution

By default the Deep Security Virtual Appliance uses DHCP to acquire an IP address when it is deployed. If you are deploying in an environment that does not have a DHCP server then you must assign a static IP address to the Appliance.

To assign a static IP address to the Virtual Appliance:

1. Log in to the Virtual Center hosting the Deep Security Virtual Appliance using vSphere Client
2. Select the Appliance and click the console tab

3. Log in to the Appliance by pressing F2 and using the default username and password (dsva:dsva)
4. Select Configure Management Network from the menu and press Enter
5. Change the Hostname, IP Address, Netmask, Gateway and DNS entries to match that of your network
6. Press Enter to save the changes
7. Reboot the Appliance by selecting Reboot System from the main menu Configuration

Problem

Anti-Malware scan terminated abnormally.

Solution

Virtual machines must be in the running state for scans to complete successfully. This termination may be due to the Virtual Machine being shutdown or suspended during the scan. Check on the status of the Virtual Machine, and try again.

This happens when the guest VM was rebooted, or enters into a sleep or standby mode.

Deep Security Agent

Installation

Problem

The following error is seen during a Solaris Agent installation:

```
## Executing postinstall script.  
devfsadm: driver failed to attach: dsa_filter  
Warning: Driver (dsa_filter) successfully added to system but failed to  
attach  
Starting Trend Micro Deep Security Drivers  
can't load module: Invalid argument
```

Solution

Some Solaris patches change the version of netinfo running on a system. It is the version of netinfo that determines which Agent install package is required for a particular system.

To identify the netinfo version on a system, run the following command:

```
modinfo | grep neti
```

The filesize determines which install package to use:

Filesize	Install Package
74c	u5sparc
1abc	u7sparc
ec8	u5x86
2600	u7x86

For more detail you can view `/var/adm/messages`

The following entries indicate that you are attempting to install a U7 Agent on a machine that requires the U5 Agent:

```
Feb 19 11:14:58 Sparc-v210-2 unix: [ID 819705 kern.notice] /usr/kernel/
drv/sparcv9/dsa_filter: undefined symbol
Feb 19 11:14:58 Sparc-v210-2 unix: [ID 826211 kern.notice]
'net_protocol_release'
Feb 19 11:14:58 Sparc-v210-2 unix: [ID 819705 kern.notice] /usr/kernel/
drv/sparcv9/dsa_filter: undefined symbol
Feb 19 11:14:58 Sparc-v210-2 unix: [ID 826211 kern.notice] 'hook_alloc'
Feb 19 11:14:58 Sparc-v210-2 unix: [ID 819705 kern.notice] /usr/kernel/
drv/sparcv9/dsa_filter: undefined symbol
Feb 19 11:14:58 Sparc-v210-2 unix: [ID 826211 kern.notice]
'net_hook_register'
Feb 19 11:14:58 Sparc-v210-2 unix: [ID 819705 kern.notice] /usr/kernel/
drv/sparcv9/dsa_filter: undefined symbol
Feb 19 11:14:58 Sparc-v210-2 unix: [ID 826211 kern.notice] 'hook_free'
Feb 19 11:14:58 Sparc-v210-2 unix: [ID 819705 kern.notice] /usr/kernel/
drv/sparcv9/dsa_filter: undefined symbol
Feb 19 11:14:58 Sparc-v210-2 unix: [ID 826211 kern.notice]
'net_protocol_lookup'
Feb 19 11:14:58 Sparc-v210-2 unix: [ID 819705 kern.notice] /usr/kernel/
drv/sparcv9/dsa_filter: undefined symbol
Feb 19 11:14:58 Sparc-v210-2 unix: [ID 826211 kern.notice]
'net_hook_unregister'
Feb 19 11:14:58 Sparc-v210-2 unix: [ID 472681 kern.notice] WARNING:
mod_load: cannot load module 'dsa_filter'
```

The following entries indicate that you are attempting to install a U5 Agent on a machine that requires the U7 Agent:

```
Feb 19 11:19:36 Sparc-v210-1 unix: [ID 819705 kern.notice] /usr/kernel/  
drv/sparcv9/dsa_filter: undefined symbol  
Feb 19 11:19:36 Sparc-v210-1 unix: [ID 826211 kern.notice]  
'net_unregister_hook'  
Feb 19 11:19:36 Sparc-v210-1 unix: [ID 819705 kern.notice] /usr/kernel/  
drv/sparcv9/dsa_filter: undefined symbol  
Feb 19 11:19:36 Sparc-v210-1 unix: [ID 826211 kern.notice]  
'net_register_hook'  
Feb 19 11:19:36 Sparc-v210-1 unix: [ID 819705 kern.notice] /usr/kernel/  
drv/sparcv9/dsa_filter: undefined symbol  
Feb 19 11:19:36 Sparc-v210-1 unix: [ID 826211 kern.notice] 'net_lookup'  
Feb 19 11:19:36 Sparc-v210-1 unix: [ID 819705 kern.notice] /usr/kernel/  
drv/sparcv9/dsa_filter: undefined symbol  
Feb 19 11:19:36 Sparc-v210-1 unix: [ID 826211 kern.notice] 'net_release'  
Feb 19 11:19:36 Sparc-v210-1 unix: [ID 472681 kern.notice] WARNING:  
mod_load: cannot load module 'dsa_filter'
```

Problem

Deep Security Agent is unable to start.

Solution

There are several conditions that can prevent the `ds_agent` service from being able to start. Reasons include: Invalid credentials (not valid yet, corrupt, expired, bad digital signature), unable to read the private key (corrupt, hardware changed radically), listen port already in use.

In cases where the DSA is unable to start, it is not able to report to the DSM, so it writes to the Windows Event Log. You should check the Windows Event log to diagnose the problem.

Activation

Problem

Deep Security Agent is installed, but the Agent UI displays blank fields.

Solution

If the "Manager URL", "Manager certificate name", and "Manager certificate fingerprint" fields are blank, the Agent has not been activated. These fields are blank until the Agent has been activated by Deep Security

Manager. Find the Computer in the DSM's Computers list, right-click on it and select Actions > Activate/Reactivate.

Problem

Getting the following error message in an "Agent Activate Failed" system event: "A client error occurred in the DSM to DSA protocol: HTTP client error received: certificate is not yet valid".

Solution

The clock on a Deep Security Agent machine must be synchronized with the Deep Security Manager to within 24 hours. If the DSA clock is behind the DSM clock then an Agent Activate operation will fail because the certificate generated for the Agent by the Deep Security Manager will not yet be valid.

Configuration

Problem

You see a **DSA_IOCTL_SET_FILTER_CONFIG** error on a computer with the description:

```
Engine command code DSA_IOCTL_SET_FILTER_CONFIG failed with error:  
0x0005aa  
(insufficient system resources exist to complete the requested service.).
```

Solution

This may be caused by one of two reasons:

The system is running with the /3GB boot option.

The /3GB flag reduces the amount of memory available to the kernel, which in turn reduces the amount of non-pageable memory in the kernel. The exact amount can be influenced by many factors such as TCP chimney offloading, use of large amounts memory over the 4GB addressing space, external device drivers such as audio, video, etc.

Too many rules are applied on the computer for the amount of kernel memory available to the driver.

In these situations it will be necessary to reduce the number of Firewall and IPS rules applied to your Computer in order to reduce the memory footprint, as well as improve performance. The Recommendation Scan feature of Deep Security can help with this. By Scanning your computers for Recommendations you can

use the "Show Recommended for Unassignment" view of the "IPS Rules" page for computer and unassign IPS Rules that do not need to be applied to maintain appropriate security. If you manage your computers via Security Profiles you can use the same "Show Recommended for Unassignment" IPS Rules view but note that it will only show IPS Rules that are not recommended on any of the Computers to which the Security Profile is assigned, and may still leave you with a set of IPS Rules that has a footprint that is too large for some Computers. If the Security Profile itself still has too many IPS Rules assigned it may be necessary to make additional Security Profiles and divide the Computers amongst them such that the Security Profiles are better representations of what IPS Rules are actually recommended to be applied to the various Computers. This should allow you to reduce the number of IPS Rules assigned to all your Computers.

Diagnostics Collection

Problem

Your support provider has asked for a diagnostics package.

Solution

In Deep Security Manager, go to **Administration > System Information** and click **Create Diagnostics Package...** in the toolbar. This displays the **Diagnostic Package** Wizard which will create a zip file containing Install/Uninstall and Debug Logs, System Information, Database Contents (last hour only for time-sensitive items), and a File Listing. This information can be given to your support provider to help troubleshoot any problems.

Problem

Your support provider has asked you to increase the size of the diagnostics package.

Solution

The default maximum size of a diagnostic package is approximately 200MB. A command line instruction is available to increase the size of the diagnostic package: `dsm_c -action changesetting -name configuration.diagnosticMaximumFileSize -value #####` The following example increases the size of the package to 1GB (1000MB): `dsm_c -action changesetting -name configuration.diagnosticMaximumFileSize -value 1000` Do not change the size of the diagnostic package unless instructed to do so by your support provider.

Problem

Cannot create a diagnostics package with Internet Explorer 7.

Solution

When exporting files (CVS, XML, software, or updates) or creating a diagnostic package, Internet Explorer's "Information Bar" may inform you that file downloads are being blocked and Deep Security Manager will instruct you to "check the server0.log". To permit file downloads, click on "More information" in the Information Bar and follow the instructions to allow file and software downloads.



TREND MICRO INCORPORATED

10101 North De Anza Blvd. Cupertino, CA., 95014, USA

Tel: +1(408)257-1500 / 1-800 228-5651 Fax: +1(408)257-2003 info@trendmicro.com

www.trendmicro.com

Item Code: APEM95862/130213