TREND MICRO

Deep Security 8.0

Getting Started & Installation Guide

Document Part No.: APEM85311_120105

Release Date: January 2012

The user documentation for Trend Micro Deep Security introduces the main features of the software and installation instructions for your production environment. Read through it before installing or using the software.

Detailed information about how to use specific features within the software are available in the online help file and the online Knowledge Base at Trend Micro's Web site.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Please evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp

Contents

Preface

Welcome to the *Trend Micro™ Deep Security™ Getting Started and Installation Guide*. This guide helps you to get "up and running" by introducing Deep Security, assisting with deployment, installation, upgrade, initial configuration, and troubleshooting.

Contacting Trend Micro

For Trend Micro contact information, go to the Trend Micro Support website at:

http://esupport.trendmicro.com/enterprise/default.aspx

About Trend Micro

Trend Micro, Incorporated is a global leader in network antivirus and Internet content security software and services, focused on helping customers prevent and minimize the impact of network viruses and mixed-threat attacks through its award-winning Trend Micro Enterprise Protection Strategy. Trend Micro has worldwide operations and trades stock on the Tokyo Stock Exchange and NASDAQ.

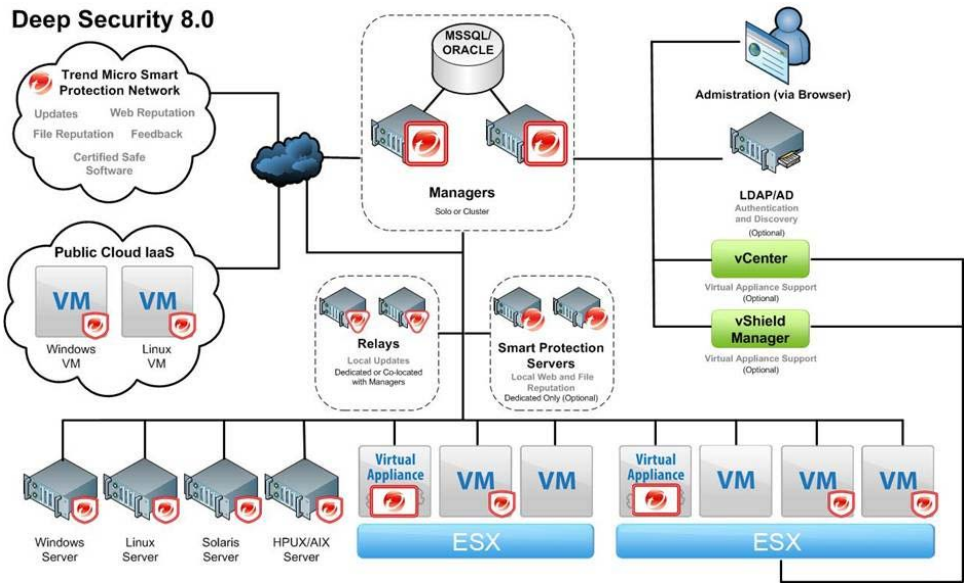
Deep Security Documentation

Documentation	Description
Getting Started and Installation Guide	A PDF document that discusses how to get started with Deep Security and the requirements and procedures for installing and upgrading Deep Security.
Administrator's Guide	A PDF document that discusses getting started information, Client installation procedures, and Server and Client management
Help	HTML files that provide "how to's", usage advice, and field-specific information. The Help is accessible from the Deep Security Server user interface.
Readme file	Contains a list of known issues and basic installation steps. It may also contain late-breaking product information not found in the Help or printed documentation.
Knowledge Base	An online database of problem-solving and troubleshooting information. It provides the latest information about known product issues. To access the Knowledge Base, go to the following Web site: http://esupport.trendmicro.com/support

Chapter 1

Getting Started

Introduction



Advanced Protection

Trend Micro™ Deep Security™ 8.0 provides advanced protection for systems in the dynamic datacenter—from virtual desktops to physical, virtual or cloud servers. Deep Security provides comprehensive protection, including:

- Anti-Malware
- Web Reputation
- Firewall
- DPI
  - Intrusion Detection and Prevention (IDS/IPS)
  - Web Application Protection
  - Application Control
- Integrity Monitoring
- Log Inspection

Deep Security integrates with the Trend Micro Smart Protection Network™ infrastructure to provide advanced protection from the cloud. The Smart Protection Network provides Deep Security with Web Reputation technology, the Certified Safe Software Service (File reputation) and collects threat information feedback from Deep Security.

Software Components

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

- **Deep Security Manager™**, the centralized management component which administrators use to configure security policy and deploy protection to enforcement components: Deep Security Virtual Appliance and Deep Security Agent.
- **Deep Security Virtual Appliance™** is a security virtual machine built for VMware™ vSphere™ environments, that provides Anti-Malware, IDS/IPS, Firewall, Web Application Protection and Application Control protection.
- **Deep Security Agent™** is a security agent deployed directly on a computer, which can provide IDS/IPS, Firewall, Web Application Protection, Application Control, Integrity Monitoring and Log Inspection protection.
- **Deep Security Relay™** relays Deep Security Updates from the Trend Micro global Update Server to Deep Security Components. At least one Deep Security Relay is always required to forward Updates to the Deep Security Manager (DPI Rules). Agents and Appliances can use Deep Security Relays to improve performance when getting Anti-Malware Component Updates (pattern and engine components). The Deep Security Relay also contains full Deep Security Agent functionality as above.

Deep Security also integrates with **Smart Protection Servers** to connect with the Trend Micro Smart Protection Network, providing Web and File Reputation services to Deep Security Agents and Appliances.

Deep Security Protection Modules

The following table identifies the protection modules provided by the Deep Security Virtual Appliance, the Deep Security Agent, or both:

	Deep Security Virtual Appliance (8.0)	Deep Security Agent (8.0)			
		Windows™	Linux	Solaris™	HP-UX™, AIX™
Anti-Malware	Yes	Yes	No	No	No
Web Reputation	Yes	Yes	No	No	No
Firewall	Yes	Yes	Yes	Yes	No
Deep Packet Inspection: **IDS/IPS** **Application Control** **Web Application Protection**	Yes	Yes	Yes	Yes	No
Integrity Monitoring	Yes	Yes	Yes	Yes	Yes
Log Inspection	No	Yes	Yes	Yes	Yes

For more details of supported features, platforms and versions, see the "**Supported Features by Platform**" table in the **Reference** section of the *Deep Security 8.0 Administrator's Guide* or the online help.

Anti-Malware

Anti-malware provides both real-time and on-demand protection against file-based threats, including threats commonly referred to as malware, viruses, Trojans, and spyware.

To identify threats, Anti-malware checks files against a comprehensive threat database, portions of which are kept locally in Deep Security as updatable patterns. Anti-malware also checks files for certain characteristics, such as compression and known exploit code.

To address threats, Anti-malware selectively performs actions that contain and remove the threats while minimizing system impact. Anti-malware can clean, delete, or quarantine malicious files. It can also terminate processes and delete other system objects that are associated with identified threats.

The Trend Micro Deep Security Virtual Appliance now supports Anti-Malware protection for virtual machines within VMware's vSphere™ 5.0 environment.

The Trend Micro Deep Security Agent now supports Anti-Malware protection for Windows computers, physical or virtual.

The Deep Security Manager's Anti-Malware module now supports:

- Agentless anti-malware protection using VMware vShield Endpoint
- Protection of active virtual machines running on vSphere 5.0
- Highly customizable Anti-Malware configurations applicable to Security Profiles and virtual machines
- Real-time, manual and scheduled scans
- Use of the Trend Micro Smart Protection Network™
- Quarantined file management, including download and delete from Deep Security Manager
- Anti-Malware support built in to Dashboard widgets and reports
- Anti-Malware Web service integration from the Deep Security Manager

Web Reputation

Web Reputation blocks web pages based on their reputation ratings. It queries Trend Micro servers for these ratings, which are collected from multiple sources, including web page links, domain and IP address relationships, spam sources, and links in spam messages. By obtaining ratings online, Web Reputation uses the latest available information to block harmful pages.

Firewall

The Firewall defines what traffic, to and from, the protected computer is allowed or denied. Firewall Rules can be applied based on a combination of protocol, port use, traffic direction, interfaces in use, and host identification triggers. Since it is a stateful firewall, rules can also be implemented to protect against various reconnaissance scans and denial of service attacks.

Firewall protection can be implemented on physical and virtual machines by installing Deep Security Agents.

You can also protect Virtual Machines in a VMware environment by installing a Deep Security Virtual Appliance on the VMware ESX/ESXi™ hypervisor hosting the VMs. The Virtual Appliance lets you provide firewall protection to the VMs without having to install Agents. You can increase the protection by also installing an Agent on the VM (the "Coordinated Approach"). The Agent will provide the primary protection with the Virtual Appliance acting as a backup.

Deep Packet Inspection (DPI)

Deep Packet Inspection analyses the actual content of the network traffic moving in and out of your computers. DPI Rules are designed to find attacks masquerading as legitimate traffic. They can stop traffic containing content designed to exploit specific application and OS vulnerabilities on a computer.

DPI Rules deliver Intrusion Detection and Prevention (IDS/IPS) protection by protecting vulnerabilities from known and unknown attacks. DPI rules also protect vulnerabilities such as Cross-Site Scripting (XSS) and SQL injection in web applications through a set of Web Application Protection rules. DPI rules are also used to provide Application Control to computers, by detecting known application traffic that may need to be restricted in corporate environments.

Ongoing Deep Security Rule updates automatically provide the most current, comprehensive protection against known and unknown attacks.

DPI protection can be implemented on both physical and virtual machines by installing Agents on the computers.

DPI can protect virtual machines using only the Virtual Appliance, or you can use the Coordinated Approach and use both the Virtual Appliance and an Agent to protect the computer.

Integrity Monitoring

The Integrity Monitoring module is used to monitor a system for changes to specified areas (certain files, registry values, etc.). This can alert you to the installation of unauthorized software or to unexpected changes to already installed software.

The Integrity Monitoring module is now supported by the Deep Security Virtual Appliance as well as by the Deep Security Agent on physical or virtual computers.

Log Inspection

The Log Inspection module is used to monitor system logs and alert when specific types of events occur. For example, there is a Log Inspection Rule which alerts when a certain number of failed authentication events occur within a certain timeframe.

The Log Inspection module requires the installation of an Agent on the computer, physical or virtual. It is not supported by the Deep Security Virtual Appliance at this time.

Smart Protection Network

Deep Security uses Trend Micro's Smart Protection Network to provide real-time security from the cloud.

Smart Protection Network provides the following services for Deep Security:

- Web Reputation Technology
- File reputation Technology
- Smart Feedback
- Global Update Server

To find out more about these services, go to
http://us.trendmicro.com/us/trendwatch/cloud/smart-protection-network/

Deep Security Relays

Deep Security Relays provide the link from your Deep Security Environment to the Global Update Server.

Smart Protection Servers

Trend Micro Smart Protection Servers can also be deployed in your Deep Security Environment to provide alternative local Smart Protection services for Deep Security.

Anti-Malware protection in a Virtual Environment

Integration with VMware vShield Endpoint

Deep Security 8.0 is designed to provide protection in a Virtual environment using a VMware ESXi 5.0 hypervisor:

VMware Software Components	Trend Micro Software Components
VMware vCenter Server 5.0	Deep Security Manager 8.0
VMware vShield Manager 5.0	Deep Security Filter Driver 8.0
VMware vShield Endpoint 5.0 (including VMware Endpoint Thin Agents for each virtual machine.)	Deep Security Virtual Appliance 8.0

The VMware vCenter manages the ESXi hypervisors which host the guest VMs that are to be protected. The VMware vShield Manager manages VMware vShield Endpoint which in turn communicates with the VMware Thin Agents. The last two components provide the API which Deep Security uses to provide Anti-Malware protection.

The Deep Security Manager coordinates the Anti-Malware protection being provided to each guest virtual machine. This is done through the Deep Security Virtual Appliance which uses the VMware Endpoint API to apply the protection to the virtual machines. The Deep Security Filter Driver controls network traffic in and out of the guest virtual machines.

For more details see Quick Start Guide to Agentless Protection in a Virtualized Environment.

What's New in Deep Security 8.0

Deep Security Manager on Linux

Deep Security Manager is available for the Linux platform (64-bit).

Agent-Less Integrity Monitoring

In Deep Security 7.5, Integrity Monitoring functionality was available only with the Deep Security Agent. In Deep Security 8.0, the DSVA now also provides Integrity Monitoring to protect Agent-less virtual machines.

Anti-Malware on Deep Security Agents for Windows

In addition to Anti-Malware protection on the Deep Security Virtual Appliance, Anti-Malware protection is now available on Deep Security Agents (Windows).

IPv6 Support

Deep Security now supports IPv6.

Note: Although IPv6 traffic is supported by Deep Security 8 Agents and Appliances, it is blocked by default. To allow IPv6 traffic on Deep Security 8 Agents and Appliances, go to the **Advanced** area of the **System > System Settings > Network Engine** tab and set the **Block IPv6 for 8.0 and Above Agents and Appliances** option to **No**.

Deep Security Relay

This new software is required by the Deep Security Manager to pull Deep Security Component Updates from the Trend Micro Smart Protection Network. Deep Security Relays also provide the capacity for Deep Security Agents and Appliances to receive Component Updates (required by all protection modules except Firewall) from Relays for improved performance.

Multiple Deep Security Relays can be installed, and they may be arranged in hierarchies to optimize bandwidth (e.g. configuring the Agents on all computers in a remote office to use a particular Relay).

Smart Protection Network

The Smart Protect Network is managed by Trend Micro, and its functionality can be made available to the Deep Security infrastructure. File Reputation is used by the Anti-Malware module when Smart Protection Mode is enabled. Web reputation requires the Smart Protection Server.

File Reputation Services:

Deep Security Agents and Appliances store the Anti-Malware Pattern which is used as the initial file threat detection and elimination tool during scans. If the risk of the file cannot be determined by Agent/Appliance, a query is sent to the Smart Protection Network or Smart Protection Server to be assessed.

Web Reputation Services:

Web Reputation services track the credibility of Web domains by assigning a reputation score based on factors such as a Web site's age, historical location changes and indications of suspicious activities discovered through malware behavior analysis. Web reputation services assign reputation scores to specific pages or links within sites instead of classifying or blocking entire sites.

Web Reputation

Deep Security's Web Reputation protection allows web pages to be blocked based on their web reputation ratings and security level required: known sources of threats, possible sources of threats or possible spam sources. Web Reputation uses Trend Micro Smart Protection Network

The configuration enables specific URLs to be blocked or allowed, and can provide a customized link to a page used to replace the blocked page.

The Web Reputation protection feature is available with a Deep Security the Anti-Malware protection license.

Smart Feedback

Trend Micro Smart Feedback provides continuous communication between Trend Micro products and the company's 24/7 threat research centers and technologies. With Smart Feedback, products become an active part of the Trend Micro Smart Protection Network™, where large amounts of threat data is shared and analyzed in real time. This interconnection enables never before possible speeds at identifying, analyzing, and stopping new threats—a level of responsiveness that addresses the thousands of new threats and threat variants released daily.

Coordinated Approach

Changes in the way the coordinated approach is implemented mean that if you have a protection feature activated and capable at both the Deep Security Virtual Appliance and a Deep Security Agent on a virtual machine protected by that Appliance, then the protection feature will be in effect at the Agent only.

Auto-Tagging and Trusted Source

As part of the Integrity Monitoring protection, the new Auto-Tagging feature allows administrators to automatically tag events from protected computers based on the similarity to selected known-good events. The source for known-good events can be a local Trusted Computer, or known-good signatures from Trend Micro's **Certified Safe Software Service**. Tags can be used to organize Events in order to simplify the task of Event monitoring and management.

Deep Security Notifier

The Deep Security Notifier is a Windows System Tray application that displays the state of the Deep Security Agent and Deep Security Relay. It also provides a pop-up user notification when the Deep Security Agent blocks malware or access to web pages.

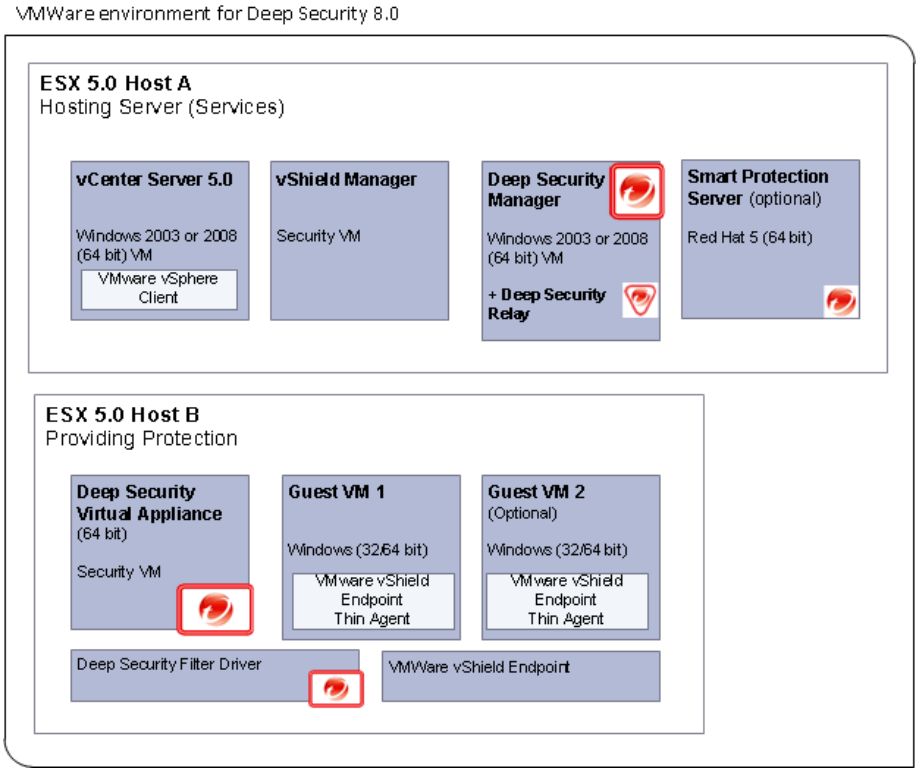
The Notifier is automatically installed by default with the Deep Security Relay and Deep Security Agent on Windows, but it can also be installed on Virtual Machines that are receiving Agentless protection from a Deep Security Virtual Appliance.

Agent Self-Protection

Administrators can use Deep Security Manager to prevent local end-users from uninstalling, stopping, or otherwise modifying the Deep Security Agents.

Quick Start Guide to Agentless Protection in a Virtualized Environment

This section describes how Deep Security is integrated into the VMware environment to provide Agentless protection using the Deep Security Virtual Appliance.



To achieve this architecture, the VMware environment must be prepared before deployment of any Deep Security components.

Note: This guide contains a detailed description of the procedures.

Prepare your VMware Environment

The VMware vShield Manager and VMware vShield Endpoint drivers are required if you want to implement Anti-Malware protection of your virtual machines.

You will need to:

1. Deploy the VMware vShield Manager. The vShield Manager is used to deploy and license vShield Endpoint Protection.
2. Install the vShield Endpoint Host Driver on the ESXi hypervisor.
3. Install vShield Endpoint Drivers on the virtual machines you want to protect.

Install a database for use by the Deep Security Manager

Deep Security requires Microsoft SQL Server, or Oracle Database. (Deep Security Manager also comes with an embedded database, which is only suitable for evaluation purposes.)

Deploy the Deep Security Environment

After downloading the Deep Security installation packages from Trend Micro, you will need to:

1. Install the Deep Security Manager.
2. Install at least one Deep Security Relay.
3. Perform basic configuration of the Deep Security Manager and Deep Security Relay
4. Additional configuration for the VMware Environment
5. Prepare ESXi for Deep Security Virtual Appliance Deployment (by deploying the Deep Security Filter Driver)
6. Install and activate the Deep Security Virtual Appliance.
7. Install the Deep Security Notifier on Windows virtual machines to be protected (optional).

Enable protection on virtual machines

Use the Deep Security Manager to activate the virtual machines to be protected.

- Apply Protection to Virtual Machines by Assigning a Security Profile to the Appliance (Security Profiles contain rules for Deep Security Protection Modules.)

Note: Remember that newly added virtual machines must always have a vShield Endpoint Thin Agent installed before they can be provided with Anti-Malware protection.

Quick Start Guide to Protection with Agents

This section describes how to get started with Anti-Malware and/or Firewall & DPI protection with Agents installed on physical or virtual machines.

**Some features are not available on all platforms. For a complete detailed list of supported features by platform, see the online help or Administrator's Guide.

Install a database for use by the Deep Security Manager

Deep Security requires Microsoft SQL Server, or Oracle Database. (Deep Security Manager also comes with an embedded database, which is only suitable for evaluation purposes.)

Deploy the Deep Security Environment

After downloading the Deep Security installation packages from Trend Micro, you will need to:

1. Install the Deep Security Manager.
2. Install at least one Deep Security Relay.
3. Perform basic configuration of the Deep Security Manager and Deep Security Relay
4. Install Deep Security Agents on the physical or virtual machines to be protected.

Enable protection on computers

1. Use the Deep Security Manager to activate the Deep Security Agents.
2. Apply protection to Computers by Assigning a Security Profile to the Agents (Security Profiles contain rules for Deep Security Protection Modules).

Quick Start to Protection in a Mixed Environment

Deep Security can protect virtual machines using only the Virtual Appliance, or you can use the Coordinated Approach and use both the Virtual Appliance and an Agent to protect the computer.

The Virtual Appliance and the Coordinated Approach using Deep Security Agents

The Virtual Appliance

The Deep Security Virtual Appliance provides Anti-Malware, Firewall, Intrusion Detection/Prevention, Application Control, and Web Application protection services to Virtual Machines without requiring the presence of an in-guest Agent. The Virtual Appliance uses VMware's VMsafe-NET API to intercept network traffic at the hypervisor. It is supported on VMware vSphere 5 (Requires vCenter 5.0 and ESXi 5.0). Security policies are applied per virtual machine.

The Virtual Appliance provides some distinct security advantages over scenarios with an in-guest Agent:

- The Appliance is isolated from the guest. The guest can operate with only the minimum required software being installed.
- Short-lived and reverted machines for which administrator time may not have been allocated for installing security software can easily and quickly be protected.
- Virtual machines and other Appliances whose operating systems are not directly accessible can be protected, even those machines being managed by other administrators.

The Deep Security Virtual Appliance simplifies deployment. There is no need to remotely install Agent software on the virtual machine. Connectivity to the virtual machine from Deep Security is not required.

The Coordinated Approach

Using the Virtual Appliance to protect virtual machines doesn't preclude the use of Deep Security Agents for virtual machines on the same host. When virtual machines are protected by the coordinated approach, if the Agent goes offline, then protection from the Appliance is automatically activated.

This coordinated approach provides the following benefits:

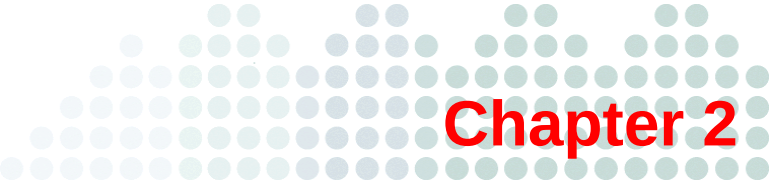
- Recommendation Scans can be run on the virtual machines.
- Provides mobility to the virtual machines. They can be moved between data centers or cloud providers and the protection moves with them.
- Performance improvement. While the Deep Security Agent is active on the virtual machine, the Virtual Appliance automatically passes traffic through to the Agent.
- Allows you to implement the additional Integrity Monitoring and Log Inspection modules on the virtual machine by using the Deep Security Agent to provide the protection.

For the Coordinated Approach to be implemented for a particular protection module, both the Agent and the Appliance have to implement that protection. The following table shows the Deep Security protection modules that can make use of the Coordinated Approach:

	Supported by Appliance	**Supported by Agent****	**Coordinated Approach Available**
Anti-Malware	Yes	Yes	No
Web Reputation	Yes	Yes	Yes
Firewall	Yes	Yes	Yes
Deep Packet Inspection	Yes	Yes	Yes
Integrity Monitoring	Yes	Yes	No
Log Inspection	No	Yes	No

**Some features are not available on all platforms. For a complete detailed list of supported features by platform, see the online help or Administrator's Guide.

.



Deep Security – Installation Guide

System Requirements

This section lists the hardware and software requirements for Deep Security software components.

Deep Security Manager System Requirements

- **Memory:** 4GB
- **Disk Space:** 1.5GB (5GB recommended)
- **Operating System:**
  - **Windows:** Microsoft Windows Server 2008 (32-bit and 64-bit), Windows Server 2008 R2 (64-bit), Windows 2003 Server SP2 (32-bit and 64-bit)
  - **Linux:** RHEL 5 (64-bit), RHEL 6 (64-bit)
- **Database (Recommended but Optional):** Oracle 11g, Oracle 10g, Microsoft SQL Server 2008 SP1, Microsoft SQL Server 2005 SP2. (20GB recommended for pre-allocation)
- **Web Browser:** Mozilla Firefox 3+ (cookies enabled) , Internet Explorer 7+ (cookies enabled) , Internet Explorer 8+ (cookies enabled)

For additional information on memory and disk space requirements see Performance Recommendations in *2: Preparation*, and Database Disk Space in *4: Installing a Database for the Deep Security Manager*.

Deep Security Relay System Requirements

- **Memory:** 512MB
- **Disk Space:** 100MB (200MB recommended, primarily for logging)
- **Windows:** Windows 7 (32-bit and 64-bit), Windows 2008 (32-bit and 64-bit), Windows 2008 R2 (64-bit), Windows Vista (32-bit and 64-bit), Windows 2003 SP2 (32-bit and 64-bit), Windows XP SP2 (32-bit and 64-bit)
- **Linux:** Red Hat 5 (64-bit), Red Hat 6 (64-bit)

ESXi 5.0 Requirements for the Deep Security Virtual Appliance

In addition to the ESXi 5.0 standard system requirements, the following specifications must be met:

- **CPU:** 64-bit, Intel-VT present and enabled in BIOS
- **Supported vSwitch:** standard vSwitch or 3rd party vSwitch – Cisco Nexus 1000v

Note: A virtualized ESXi environment (ESXi running as a VM) is not supported.

Deep Security Virtual Appliance System Requirements

- **Memory:** 1GB (Memory requirements can vary depending on the number of VMs being protected. See Appendix C: Deep Security Virtual Appliance Memory Usage for details.)
- **Disk Space:** 20GB
  - **Operating System:** VMware vCenter 5.0.0 and ESXi 5.0.0
  - **Additional VMware Utilities:** VMware Tools, VMware vShield Manager, VMware vShield Endpoint Security 5.0 (ESXI5 patch ESXi500-201109001 for vShield Endpoint Driver).
  - **VMware Endpoint Protection supported guest platforms**: Windows Vista (32-bit), Windows 7 (32-bit), Windows XP SP2 (32-bit), Windows 2003 SP2 (32-bit, 64-bit), Windows 2008 (32-bit, 64-bit). (For the latest list of supported guest platforms, see your VMware documentation.)

Deep Security Agent System Requirements

- **Memory**:
  - **with Anti-Malware:** 512MB
  - **without Anti-Malware:** 128MB
- **Disk Space:** 100MB (200MB recommended, primarily for logging) (1GM recommended with Anti-Malware protection enabled)
- **Windows:** Windows 7 (32-bit and 64-bit), Windows 2008 (32-bit and 64-bit), Windows 2008 R2 (64-bit), Windows Vista (32-bit and 64-bit), Windows 2003 SP2 (32-bit and 64-bit), Windows XP SP2 (32-bit and 64-bit)
- **Solaris:** Solaris 9 and 10, (64-bit Sparc), Solaris 10 (64-bit x86)
- **Linux:** Red Hat 4 (32-bit and 64-bit), Red Hat 5 (32-bit and 64-bit), Red Hat 6 (32-bit and 64-bit), SuSE 10 (32-bit and 64-bit), SuSE 11 (32-bit and 64-bit), SuSE 11 SP1 (32-bit and 64-bit)
- **AIX:** AIX 5.3, 6.1 (The AIX Agents only support Integrity Monitoring and Log Inspection.)
- **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 Notifier System Requirements

- **Windows:** Windows 7 (32-bit and 64-bit), Windows 2008 (32-bit and 64-bit), Windows 2008 R2 (64-bit), Windows Vista (32-bit and 64-bit), Windows 2003 SP2 (32-bit and 64-bit), Windows XP SP2 (32-bit and 64-bit)

Preparation

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

What you will need

Deep Security Installer Packages

All Deep Security Installer packages are available from the Trend Micro Download Center, http://downloadcenter.trendmicro.com.

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

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. (This way the Deep Security Manager will automatically import the Relay, Virtual Appliance and the Filter Driver when it is installed.)

Note: Updates to security Components, Deep Security Agents, and Deep Security Virtual Appliances can all be deployed using the Deep Security Manager. New versions of the Deep Security Manager, however, must be installed independently of your current Deep Security Manager. That is, you must download the new version from the Trend Micro Download Center, run the installer, and follow the instructions to perform a software upgrade.

License (Activation Code)

A license (Activation Code) is required for each Deep Security protection module that you want to use.

Licenses will also be required for VMware components.

Administrator/Root Privileges

You need to have Administrator/Root privileges to install Deep Security software components.

Free 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.
- **Port 1433 and 1434:** bi-directional Microsoft SQL Server Database ports.
- **Port 389:** connection to an LDAP Server for Active Directory integration (configurable).
- **Port 80, 433:** connection to Trend Micro 7.5 Legacy ActiveUpdate Server (configurable).
- **Port 25:** communication to a SMTP Server to send email alerts (configurable).
- **Random Port:** for DNS Lookup.

Note: For a detailed list of ports 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 80, 433:** connection to Trend Micro Update Server and Smart Protection Server.
- **Port 514 (optional):** bi-directional communication with a Syslog server.

Depending on the configuration of communication direction, the Deep Security Manager automatically implements a firewall rule to open the required communication ports on machines hosting Deep Security Relays, Agents and Appliances.

Note: See "**Communication Direction**" in the **Computers** section of the online help or the Administrator's Guide.

Network Communication

Communication between Deep Security Manager and Deep Security Relays/Agents/Appliances and ESXi uses DNS hostnames.

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 requires that the Deep Security Manager computer have a DNS entry or an entry in the Relay/Agent/Appliance computer's hosts file.

Note: Note you will specify this hostname as part of the Deep Security Manager installation procedure. If you do not have DNS, you will have to specify 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 Network Time Protocol (NTP) server.

The clock on a Deep Security Relay (DSR) machine must be synchronized with Deep Security Manager (DSM) to within a period of 24 hours.

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 of Deep Security Manager operations require high CPU and Memory resources (such as Updates and Recommendation Scans). Trend Micro recommends that each Manager node have 4 cores and sufficient RAM in high scale environments. Where possible the 64-bit version of the Manager should be used as it can address 4GB of RAM (compared to the 1GB the 32-bit version uses).

The Database should be installed on hardware that is equal to or better than the specifications of the best 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 plans should be put in effect.

Deep Security Multiple 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 may be configured for load balancing and recovery purposes. For evaluation purposes, only one Deep Security Manager is required

For more information on running multiple Manager nodes, see **Multi-Node Manager** in the **Reference** section of the online help or the Administrator's Guide.

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 2ms latency or better is recommended between the Manager and 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 intend to take advantage of VMware High Availability (HA) capabilities, make sure that the HA environment is established before you begin installing Deep Security. All ESXi hypervisors used for recovery operations must be imported into the Deep Security Manager with their vCenter, they must be "prepared", and a Deep Security Virtual Appliance must be installed on each one. Setting up the environment in this way will ensure that Deep Security protection will remain 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 a local store as opposed to a shared store. When the Virtual Appliance is deployed onto a local store it cannot be vMotioned by DRS.) For further information on DRS and pinning virtual machines to a specific ESXi host, please consult your VMware documentation.

Note: If a virtual machine is vMotioned by HA 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 **Tasks** section of the online help or the Administrator's Guide.

Required Resources Check List

Check	Hardware Requirements (preferred)	
	Database: SQL Server or Oracle	Memory: 4GB Disk Space: >20GB Operating System: Windows Server 2008 (64 bit)
	Deep Security Manager	Memory: 4GB Disk Space: 5GB Operating System: Windows Server 2008 (64 bit) or Linux (64 bit)
	Deep Security Relay(s)	One Relay may be co-located on Deep Security Manager host machine.

Check	Hardware Requirements (preferred)	
		Disk Space: 200MB Operating System: Windows Server 2008 (64 bit) or Linux (64 bit)

Check	License Requirements	
	Deep Security Manager	License is required for protection modules.

Preparing a VMware Environment for Agentless Protection

Recommended Environment - Overview

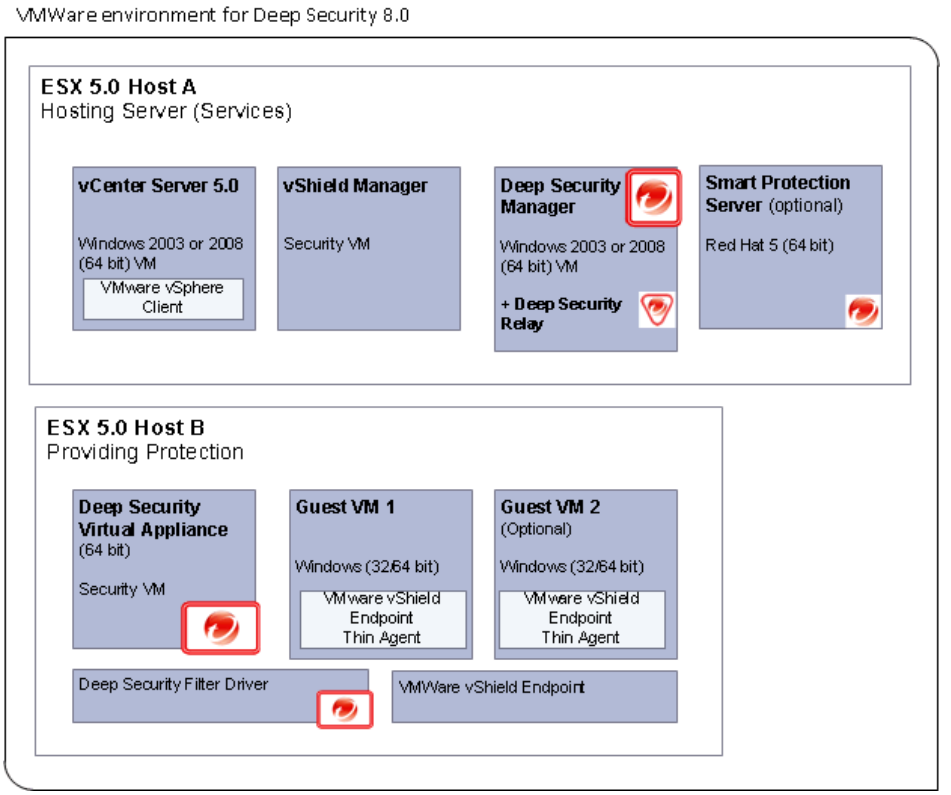
The following describes a Deep Security deployment in a typical VMware environment.

There are two types of ESXi Hosts:

Host A is an ESXi hypervisor on which are running individual virtual machines (VMs) for Deep Security Manager 8.0, vShield Manager 5.0, and vCenter Server 5.0 (can be installed on a physical machine). 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 ESX hypervisor on which are running Deep Security Virtual Appliance (DSVA) and the VMs requiring Anti-Malware protection.

Note: Although the vCenter Server, the vShield Manager and the Deep Security Manager can be installed on physical machines, most enterprises install them on VMs because the virtualized environment is available. They 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 (but, again, not on a protected ESXi).



Minimum Requirements

Host A: ESXi 5.0

(Each of the following components on one guest VM):

Check	Hardware Requirements	
	vCenter Server 5.0 on Windows Server 2008 or 2003 (64-bit)	Intel (64 bit processor) • 6 GB RAM: • 1 GB for vCenter • 2 GB for vShield Manager 2 GB for DSM 160 GB HDD
	vShield Manager 5.0 (deployed in a security VM)	
	Database (Oracle or SQL) for Deep Security	
	Deep Security Manager 8.0 on Windows	

Check	Hardware Requirements	
	Server 2008 R2 or Windows 2003 (64 bit)	CD/DVD Drive
	Deep Security Relay 8.0 (optional on the Deep Security Manager VM)	

Host B: ESXi 5.0

Check	Hardware Requirements	
	Deep Security Virtual Appliance 8.0 (deployed in a security VM)	Intel (64 bit processor) 4 GB RAM: • 1 GB for Deep Security Virtual Appliance • Other depends on how many guest OSs you want to install on this Host 80 GB HDD CD/DVD Drive
	Guest VMs to be protected.	

Deep Security is compatible with specific versions of VMware software. For a detailed list of the VMware software versions required, and how to check for the correct versions, see Upgrading from Deep Security 7.5

Check	Software Requirements	Notes
	VMware vCenter 5.0	Includes vCenter Server and vCenter Client GUI application. License is required during product installation.
	VMware vShield Manager 5.0	License is required during product installation.
	Trend Micro Deep Security Manager 8.0 (DSM)	License is required during product installation.
	VMware vShield Endpoint 5.0 (ESXI5 patch ESXi500-201109001.)	Add the license to vCenter
	Trend Micro Deep Security Filter Driver 8.0 (FD)	

Check	Software Requirements	Notes
	Trend Micro Deep Security Virtual Appliance 8.0 (DSVA)	
	Supported Guest OS (for Anti-Malware protection)	For Anti-Malware protection, VMware Endpoint will be required on each guest VM. (Since ESXI5 patch ESXi500-201109001, vShield Endpoint driver is included in VMware Tools). For Anti-Malware protection, supported VMware guest platforms are Windows only Note: If using Windows XP or Windows 2003, make sure SP2 is installed.
	Trend Micro Deep Security Agent 8.0 (optional)	For coordinated protection.

("VMware vSphere" is the suite of VMware services associated with vCenter.)

Server Preparation

Preparation of Servers (On Host A)

Follow the tasks in the recommended order.

Task1: ESXi 5.0 Setup

Step 1. Install ESXi 5.0 on Host A

Step 2 Configure ESXi (e.g. Network static IP)

Task 2: vCenter Server 5.0 Setup

Step 1. Prepare Guest OS Windows Server 2008 or 2003 (64 bit)

Step 2. Browse to your ESXi welcome page and download vCenter Server and vSphere Client

Step 3. Install vCenter Server 5.0

Step 4. Install the vSphere Client on the same Guest VM or on any other computer (except on ESXi Host B)

Step 5. On vCenter console, add Host A via "Add Host"

Note: vCenter Console refers to the vSphere Client GUI

Task 3: vShield Manager (vSM) 5.0 Setup

Step 1. On vCenter Console, select **File>Deploy OVF Template**

Step 2. Browse and select the vShield Manager OVA file

Make sure you deploy vSM on any ESXi host except Host B

Step 3. Once vSM is deployed, power on vSM and login as admin:default from console

Type "enable" to turn on privileged mode command with "default" as password

Type “setup” and follow step to finish vSM network configuration

Step 4. Login to vSM by using an internet browser to go to https://<vSM-ip>

Make sure vSM web console is displayed

Task 4: Prepare a Guest OS for Database Installation

This Guest will host your Oracle or SLQ database for use by the Deep Security Manager.

Step 1. Prepare a guest OS Windows 2008 R2 or 2003 (64 bit)

(Make sure the latest patches are applied).

Task 5: Prepare a Guest OS for Deep Security Manager Installation

Step 1. Prepare a guest OS Windows 2008 R2 or 2003 (64 bit)

Step 2. Optionally prepare an additional guest OS for other Deep Security Manager nodes

Important: 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 ESX cluster. This is because 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.

Guest OS Preparation

Guest OS Preparation (On Host B) – Virtual Machines to be protected by Deep Security

Task 6: ESXi 5.0 Setup

Step 1. Install ESXi 5.0 on Host B

Step 2. Configure ESXi network settings (e.g. Network Static IP)

Step 3. On vCenter Console, add Host B via "Add Host"

Task 7: Guest OS Preparation

Guest VM #1 to be protected by Deep Security Anti-Malware

Step 1. Install guest OS.

(If using Windows 2003 Server, make sure you install Service Pack 2)

Step 2. Make sure the guest VM has a basic disk volume. Dynamic disks are not supported. (Note: The default installation of Windows 2003 has basic disk)

Step 3. Install the VMware vShield Endpoint driver to this machine.

As of ESXI5 patch ESXi500-201109001, 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.)

To install the Endpoint vShield drivers:

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.

Guest VM #2 to be protected by Deep Security Anti-Malware

Step 1. You may install more than one supported guest VM on Host B. Please follow the same steps as above and install the vShield Endpoint Thin Agent package.

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 Anti-Malware Scan Terminated Abnormally. Virtual Machines must be in the running state for scans to complete successfully.

Note: In a High Availability environment, Trend Micro strongly recommends that you implement Agent-less Anti-Malware protection on all the ESXi hypervisors in a cluster.

After completing the tasks above, continue to follow the instructions in the next section s to:

- Install a database
- Install the Deep Security Manager and Deep Security Relay
- Configure the DSM for integration with VMware
- Prepare for and deploy the DSVA

Installing a Database for the Deep Security Manager

Deep Security Manager comes with an embedded database (Apache Derby), which is only suitable for evaluation purposes. For enterprise deployments, Deep Security requires Microsoft SQL Server 2008 or 2005, or Oracle Database 11g or 10g.

During the installation of Deep Security Manager, the installer asks whether you are using the embedded database engine, or one of the two supported enterprise database engines. If you choose the latter, the installer will prompt you for configuration information.

Note: If you intend to use Microsoft SQL Server or Oracle Database, you must install it and create a database ***before*** you install Deep Security Manager.

Database Disk Space

Database disk space should be pre-allocated. When logging is left at default levels, an average Deep Security Agent protecting a computer will require approximately 50 MB of database disk space for data and an additional 5MB of space for transaction logs. So one thousand computers will require 50 GB for data and 5 GB for transaction logs, two thousand computers will require 100 GB for data and 10 GB for transaction logs, etc.

The amount of space required per computer is a function of the number of logs (events) recorded and how long they are retained. The **Firewall and DPI** tab of the **System > System Settings** screen allows you to control settings such as the maximum size of the event log files, the number of these log files to retain at any given time ("pruning controls"). Similarly, the **TCP**, **UDP**, and **ICMP** tabs on a Stateful Configuration's **Properties** window lets you configure how Stateful Configuration Event logging is performed. Similar settings are available for other Deep Security modules in the **System > System Settings** screens. (For more information on logging, see "Advanced Logging Policy Modes" and "Configure Logging" in the **Reference** and the **How To…** sections of the online help or the *Deep Security Administrator's Guide*.)

These Event collection settings can be fine-tuned at the Global, Security Profile, and individual computer level. (See **Inheritance and Overrides** in the **Reference** section of the online help or the Administrator's Guide.)

Note: At their default settings, the following three modules generally consume the most disk space, in descending order: Firewall, Integrity Monitoring, and Log Inspection.

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 an SQL database, the SQL account must be granted **DB_Creator** Server Roles and **DB_Owner** of the DSM Database.

DSM 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 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

You must log in as an Administrator to install Deep Security Manager.

Step 1. Start the Deep Security Manager by double-clicking the installation file

When the Installation Wizard appears, click **Next** to continue

Step 2. Accept the license agreement, and click **Next**

Step 3. Specify the folder where you would like Deep Security Manager to be installed and click **Next**.

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

Step 4. 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.

Step 5. 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 **System > Licenses**.)

Step 6. Enter the hostname, URL, or IP address of this computer.

Note: 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**.

Step 7. 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**.

Step 8. 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**.

Step 9. 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 Deploying the Deep Security Relay.

Click **Next**.

Step 10. 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**.

Step 11. Confirm Settings. Verify the information you entered and click **Finish** to continue.

Step 12. Click **Finish** to close the **Setup** wizard.

The Deep Security Manager service starts when setup is complete.

If you selected to install a co-located Deep Security Relay in Step 11, the Relay installation will run silently now.

To start the Deep Security Manager Web-based management console, select the **Run Trend Micro Deep Security Manager** option before clicking **Finish**.

Note: The installer places a shortcut to Deep Security Manager in the program menu. You need to note this URL if you want to access the Manager remotely.

Make sure you can login to Deep Security Manager web-based management console.

Installing the Deep Security Manager for Linux

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

To install from the Linux command-line, see Deep Security Manager Silent Install (below).

Running Deep Security Manager

The Deep Security Manager service starts automatically at boot up. 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.

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 Basic Deep Security Configuration.

If you have not already installed a co-located Deep Security Relay, then you should install one as described in Deploying the Deep Security Relay, before configuring it.

Deep Security Manager Silent Install

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

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

Or on Linux:

```
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
```

A complete description of all possible settings is included in Appendix A: Deep Security Manager Settings Properties File.

Deploying 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.

When you have completed the Relay installation, use the Deep Security Manager to Configure Deep Security Relay as described in Basic Deep Security Configuration.

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.

Step 1. Double-click the installation file to run the installer package.

Click **Next** to begin the installation.

Step 2. Accept the license agreement and click **Next** to continue.

Step 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 DPI features may not be deselected. These features form part of the core Deep Security Agent architecture and are always installed, even if Firewall and DPI 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.

Step 4. Click **Install** to proceed with the installation.

Step 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.

When you have completed the installation, use the Deep Security Manager to Configure Deep Security Relay as described in Basic Deep Security Configuration.

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
```

When you have completed the installation, use the Deep Security Manager to Configure Deep Security Relay as described in Basic Deep Security Configuration.

Installing the Deep Security Relay for Linux

To install the Deep Security Relay for Linux:

Step 1. 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 Relay.

```
$ su
Password:
```

Step 2. Use "rpm -i" to install the ds_agent package:

```
# rpm -i Relay-RedHat_2.6.18_8.EL5_i686-8.0.0-xxxx.i386.rpm

Preparing...          ########################################
[100%]
      1:ds_agent      ########################################
[100%]
Loading ds_filter_im module version 2.4.21-20.EL-i686 [ OK ]
Starting ds_agent: [ OK ]
```

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

Step 3. The Deep Security Relay will be started automatically upon 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
```

When you have completed the installation, use the Deep Security Manager to Configure Deep Security Relay as described in Basic Deep Security Configuration**.**

Deep Security Relay and Component Updates in an Air-Gapped Environment

In the default architecture, at least one Deep Security Relay is configured to download Updates from the Trend Micro Global Update source.

However, if your environment requires that the Deep Security Relay is not allowed to connect to an Update Server via the internet, then an alternative method is available to import a package of Updates to a Relay for distribution to other Deep Security Software Components.

Using a Deep Security Relay to generate an Updates package

You will need a second Deep Security Manager and a Deep Security Relay installed in a location that has access to the internet and the Trend Micro Update Servers. Use that Deep Security Manager to activate the Relay and configure it to regularly download Component Updates from Trend Micro Update Servers. (See Basic Deep Security Configuration.)

Once the Relay has downloaded a Component Update, use the following procedures to create a zipped update bundle that you can transfer to the air-gapped Relays that need to be updated:

Step 1. To create a Relay Updates bundle from the command line, enter the following:

```
dsa_control /b
```

The command line output will show the name and location of the.zip file that was generated.

Step 2. Copy the Relay Updates bundle .zip file to the installed location of the Deep Security Relay that you want to import the Updates.

Note: You should always generate a Deep Security updates package from the a Deep Security Relay running on the same platform as the one that will be importing the bundle.

An updates package generated from a Deep Security Relay on Windows cannot be successfully imported by a Deep Security Relay running on Linux. If you have a mixed (Windows and Linux) environment, then you should always generate the updates bundle on a Linux Deep Security Relay to ensure that is can be imported by all other Relays.

Importing Updates to the air-gapped Deep Security Relay

If a Component Update is initiated from the Deep Security Manager (either scheduled or manual) and the Deep Security Relay is unable to get the update from the configured Update Server location then it will automatically check for the presence of a Relay Updates bundle .zip file in its installation directory location.

If the Relay Updates bundle file is found, then the Deep Security Relay extracts and imports the Updates from the file.

Note: Remember to remove the Relay Updates bundle .zip file after the Updates have been successfully imported to the Relay.

Configuring an Update Source for an Air-Gapped Relay

Air-gapped Relays will still try to contact an Update server to check for Updates. To avoid Update failure Alerts, set the Relay to use itself as an Update source:

1. In the Relay's **Details** window, go to System > System Settings > Updates
2. In the **Relays** area, select "Other Update Source:" and enter https://localhost:4122
3. Click **Save**.

Additional Configuration for VMware Integration

Additional Configuration to prepare the Deep Security/VMware Environment

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 on the DSM.

VMware vShield Endpoint (EPSec) Deployment on Host ESXi

Step 1. Install VMware vShield Endpoint (EPSec) on ESXi host for protected machines (Host B)

(Please refer to the diagram in Preparing a VMware Environment for Agentless Protection.)

Step 2. Login to vShield Manager by browsing to https://<vSM-ip>

Input admin:default as the login account

Step 3. On the right side **Configuration** tab, enter your vCenter Server Information

Step 4. Select **Host & Cluster** in the left navigation pane

Step 5. Select the ESXi hypervisor to be protected by Deep Security (Host B).

On the right pane, click **Install** link with the Service item **vShield Endpoint**

Step 6. In **Select services to install/upgrade**, check **vShield Endpoint** and click the **Install** button at the top right of the screen

Step 7. After installing, make sure the Service **vShield Endpoint** correctly displays the installed version (The **Install** link has changed to **Uninstall**)

Step 8. On vCenter Console, go to the vShield Manager Console tab

Login as admin:default

Step 9. Type **enable** command to turn on privileged mode, with default as password

Step 10. Type **reboot** to reboot vShield Manager

Step 11. Login to vShield Manager by browsing to https://<vSM-ip>

Make sure vShield Manager web console is displayed.

Verify the status of the ESXi and make sure that the correct version information is displayed for vShield Endpoint

Add vCenter to the DSM's list of Managed Computers.

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

Step 1. From the DSM's left navigation panel select **Computers->New->Add VMware vCenter…**

Step 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.

Step 3. Enter the vShield Manager Server Address, Username and Password.

(You can also configure this information later from the DSM).

Click **Next.**

Step 4. Accept the vShield Manager SSL certificate.

Step 5. Accept the VMware default certificate.

Step 6. Review the vCenter information. Click **Finish**

"The VMware vCenter has been successfully added" message will be displayed, Click **Close**.

Step 7. Click **Computers->vCenter** to make sure the vCenter is listed.

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

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 on the DSM.
- VMware vShield Endpoint (EPSec) has been deployed on the protected Host ESXi, and vCenter has been added to the DSM's list of Managed Computers, see Additional Configuration for VMware Integration

Import Deep Security Software packages into the DSM

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

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

Step 1. From the DSM select **System->Updates**

Step 2. Scroll down and select **Import Software…** from **Software Updates** area.

Browse and Select FilterDriver-ESX-8.0.0-xxxx.x86_64.zip

Click **Next** and **Finish** on the next screen.

Step 3. Select **Import Software** from Software Package section.

Browse and Select Appliance-ESX-8.0.0-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)

Step 4. Click the **View Imported Software** and make sure both the Filter Driver and DSVA are imported.

Prepare ESXi for Virtual Appliance deployment by Installing the Filter Driver

Important: 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)

Step 1. From the DSM, Select Computers->vCenter->Hosts and Clusters

Step 2. Find the ESXi host in the Computers list

(its "status" column should read "Unprepared"),

Right-click on it, and select **Actions > Prepare ESX** to display the **Prepare ESX Server Wizard**. Click **Next**.

Step 3. Select **Yes** to allow the Deep Security Manager automatically bring the ESXi in and out of maintenance mode.

Click **Finish**.

Step 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).

Step 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 installation is described later).

Step 6. This completes the ESXi preparation.

Wait for a few minutes.

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

Step 7. Go back to Computers->vCenter and make sure the status of the ESXi is set to "Prepared".

Step 8. Go to the vCenter Console. Select the ESX Server->Configuration tab ->Networking. Check that the vSwitch has been created.

Step 9. SSH into the ESXi Server 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.

Increasing the Filter Driver Virtual Machine Capacity (Optional)

Note: By default, the DSVA has enough resources to protect up to 25 Virtual Machines per ESXi host. If you have more than 25 machines running on an ESXi, you may have to increase the resources allocated to the DSVA machine.

Enter ESXi Maintenance Mode

Step 1. Go to vCenter Console

Step 2. Configure ESXi to enter Maintenance Mode

Increasing heap memory in the fast path driver

Step 1. The formula is:

<number of VMs> * <1048576 Bytes (1MB) > + 8388608 Bytes (8MB)

e.g. 350 * 1MB + 8MB = 375390208 Bytes

Step 2. SSH into the ESXi Console and run this command:

```
%esxcfg-module –s DSAFILTER_HEAP_MAX_SIZE=375390208 dvfilter-dsa
```

Step 3. To verify the setting, execute this command:

```
%esxcfg-module –g dvfilter-dsa
```

Step 4. The setting will not take effect until the driver is reloaded.

Note: It is highly recommended to reboot the ESXi after making this configuration.

Reboot the ESC Server or execute the following commands to restart the driver:

```
%esxcfg-module –u dvfilter-dsa
%esxcfg-module dvfilter-dsa
```

Exit ESXi Maintenance Mode

Step 1. Go to vCenter Console

Step 2. Exit Maintenance Mode (or you will not be able to deploy the DSVA).

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 on the DSM.
- VMware vShield Endpoint (EPSec) has been deployed on the protected Host ESXi, and vCenter has been added to the DSM'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 Appendix K: Minimum VMware Permissions for DSVA Deployment

Deploy Deep Security Appliance (DSVA) to the ESXi

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

Step 1. From the DSM, select **Computers->vCenter.**

Step 2. Right Click on the ESXi Host being protected and select **Actions->Deploy Appliance**. Click **Next**

Step 3. Enter a **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**.

Step 4. Define the Appliance **Hostname**. Enter the **IPv6 Address** and/or **IPv4 Address** for the Appliance. (DHCP is enabled by default).

Click **Next**.

Step 5. Select Thick Provisioned format (recommended).

(**Thick Provisioned Format** uses all the allocated disk space, while **Thin Provisioned Format** uses the least amount of disk space).

Click **Finish** and wait for few minutes for the DSVA to be uploaded.

Step 6. Accept the SSL Certificate in the next screen and wait for few minutes till the Appliance is deployed.

You should see an "Appliance successfully deployed" message.

Step 7. Under Activate Deep Security Appliance section, select "**No thanks, I will activate it later**".

(Activation is described later).

Click **Close**.

Step 8. Check the vCenter to make sure the DSVA is up and running.

Step 9. The Virtual Appliance is now displayed along with the other Computers in the vCenter Group in the DSM **Computers->vCenter** list.

Verification Steps:

Check 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.

Check 2. Go to the Virtual Machine Properties->**Summary** tab, and click **Edit Settings.**

Check 3. Go to the **Hardware** tab, there are 3 interfaces available.

> **Note:** Network Adapter 1 is always the management network. DSVA uses this interface to communicate with Deep Security Manager.

Network Adapter 2 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-vmknic-pg.**

Check 4. Make sure you can ping the Deep Security Manager.

Type the command:

```
sudo ping <FQDN of Deep Security Manager>
```

Note: Make sure DNS is properly configured and is able to resolve FQDN to IP Addresses used by all machines in this environment. Otherwise use IP Address instead.

Increase the DSVA Memory (Optional)

1GB of memory is assigned to the DSVA by default.

Increase the memory to 4GB for a DSVA protecting 50 Virtual Machines.

Increase the memory to 8GB for a DSVA protecting 100+ Virtual Machines.

Increasing the DSVA Memory

Step 1. From the vCenter Console, go to the DSVA **Console** tab**.**

Step 2. Power-off the DSVA

```
sudo shutdown –h now
```

Step 3. Go to the Summary->Edit Settings->Hardware tab

Step 4 Allocate the required amount of memory to the Virtual Appliance

Step 5 Power-on the DSVA.

Disable DRS and HA on the DSVA

Step 1. From the vCenter Console, go to the DSVA **Console** tab**.**

Step 2. Turn off HA and DRS.

Activate the Deep Security Virtual Appliance

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

Step 1. From the DSM, select **Computers->vCenter**

Step 2. Right Click on the DSVA machine and select **Actions->Activate Appliance.**

Click **Next.**

Step 3. For Security Profile, select Deep Security Virtual Appliance.

Click **Next.**

The activation process is started.

Step 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 DSVA 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 may reboot the vShield Manager and wait for a few minutes after vShield is back on line to attempt DSVA activation again.)

Step 5. Under **Activate Host Virtual Machines**, select "No thanks, I will activate them later".

(This step will be described later)

Click **Close**.

Step 6. The DSVA is successfully activated.

Go back to **Computers->vCenter** and make sure the status of DSVA is set to **Managed(Online).**

Note: Make sure that the Anti-Malware Ready status is set to Yes. If the status is No, check the ESXi Anti-Malware Status. Make sure the vfile, dvfilter and dvfilter-dsa drivers are all running.

Activating Guest Virtual Machines

Assign Guest Virtual Machines to the ESXi

Step 1. Move machines to the ESXi Host.

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

Activating a Virtual Machine

Step 1. From the DSM, select **Computers->vCenter**

Step 2. Right Click on the Virtual Machine and select **Action->Activate**

Step 3. Right Click on the Virtual Machine and select **Action->Assign Security Profile.**

Step 4. To activate Anti-Malware protection, apply **the Windows Anti-Malware Protection** Security Profile. (This only has the anti-malware feature enabled).

Step 5. Check the status of the Virtual Machine and make sure **Anti-Malware** status is **On.**

Step 6. To configure Agentless Integrity Monitoring, right-click on the **Computers** list and from the **Actions** list select **Rebuild Baseline for Computer**.

Once the baseline has been built (this can take a while), you can perform automatic or manual scans for Integrity.

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 need to check.

Check 1. Make sure the VMware tools are up-to-date on the virtual machine

Check 2. Make sure vShield Endpoint Agent is installed and the vsepflt driver is running on the VM**:**

```
sc query vsepflt
```

Check 3. Make sure Deep Security manager is able to synchronize information with vCenter

Check 4. On the DSM's **Computers** list, make sure that the ESX status is "vShield Endpoint: Installed"

Check 5. On the DSM's **Computers** list, make sure that the DSVA status is "vShield Endpoint: Registered"

Check 6. Make sure ESXi and DSVA Anti-Malware status is **Yes.**

Deploying Deep Security Agents

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

A full list of supported platforms can be found in System Requirements

At this point...

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

Follow the instructions in this section for installation of the Deep Security Agent on your chosen platform.

When you have completed the installation, use the Deep Security Manager to configure protection on the computer by following the steps in Basic Deep Security Configuration to:

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

Preparation

Note: The clock on a Deep Security Agent (DSA) machine must be synchronized with Deep Security Manager (DSM) to within a period of 24 hours. If the DSA clock is behind the DSM 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".

Copy the Installer Package

Copy the installation file to the target machine.

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 Linux Agent.

Installing the Deep Security Agent for Windows

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

Step 1. Double-click the installation file to run the installer package.

Click **Next** to begin the installation

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

Step 3. 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 DPI features may not be deselected. These features form part of the core Deep Security Agent architecture and are always installed, even if Firewall and DPI 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**.

Step 4. Click **Install** to proceed with the installation.

Step 5. 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
```

Installing the Deep Security Agent for Linux

Requirements:

The Deep Security Agent for Red Hat requires these versions (or later) of the following package:

```
libstdc++-ssa-3.5ssa-0.20030801.48.i386.rpm
```

These can be installed using yum or up2date.

To install the Deep Security Agent for Linux:

Step 1. To install the Deep Security Agent on a Linux machine, you need to log on as "root". Alternatively, you can use the "sudo" utility to install the Agent.

```
$ su
Password:
```

Step 2. Use "rpm -i" to install the ds_agent package:

```
# rpm -i Agent-RedHat_2.6.18_8.EL5_i686-8.0.0-xxxx.i386.rpm
Preparing...         ##########################################
[100%]
      1:ds_agent     ##########################################
[100%]
Loading ds_filter_im module version 2.4.21-20.EL-i686 [ OK ]
Starting ds_agent: [ OK ]
```

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

Step 3. The Deep Security Agent will be started automatically upon installation.

To start, stop and reset the Agent 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
```

Installing the Deep Security Agent for Solaris

Requirements:

For Solaris Sparc/8 and Sparc/9:

```
libgcc 3.4.6 or better (www.sunfreeware.com)
libiconv 1.11 or better (www.sunfreeware.com)
pfil_Solaris_x.pkg
Agent-Solaris_5.x_sparc-7.x.x-yyy.sparc.pkg.gz
```

Note: "x" will be 8 or 9 depending on the version of the Solaris operating system you are installing on.

For Solaris Sparc/10:

```
SUNWgccruntime, GCC Runtime libraries
pfil_Solaris_10sparc.pkg (see note below)
Agent-Solaris_5.10_sparc-7.x.x-yyy.sparc.pkg.gz
```

For Solaris X86/10:

```
SUNWgccruntime, GCC Runtime libraries
pfil_Solaris_10x86.pkg (see note below)
Agent-Solaris_5.10_i386-7.x.x-xxx.x86_64.pkg.gz
```

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

To install the Solaris 10 Agent:

Note: For Solaris 10 Update 4 and above, you only need to perform steps 5 and 6.

Step 1. Acquire all of the required packages (see above)

Step 2. Prepare to remove the Sun version of ipfilter and pfil

a. Note the version numbers and other information

```
modinfo | grep pfil
modinfo | grep ipf
pkginfo -l SUNWipfr
pkginfo -l SUNWipfu
```

b. To check the status

```
svcs -x ipfilter
svcs -x pfil
```

c. If either of these commands gives errors, then the problem should be corrected before proceeding further. Also check that Sun's version of pfil loads correctly.

```
ifconfig  ce0 modlist    (use your network interface)
```

And see if pfil is in the list between "ip" and your network interface. If it isn't, then check that your interface type is uncommented in /etc/ipf/pfil.ap, reboot and try again. Don't proceed further until you are convinced that Sun's version of ipfilter/pfil is working correctly.

d. Export current ipfilter and pfil service configurations

```
svccfg export network/pfil > /var/tmp/pfil.svc
svccfg export network/ipfilter > /var/tmp/ipfilter.svc
```

e. Disable the two services

```
svcadm -v disable pfil
svcadm -v disable ipfilter
```

f. Reboot the system

Step 3. Remove the Sun version of ipfilter and pfil

a. Check that the kernel modules are not loaded after reboot

```
modinfo | grep ipf
modinfo | grep pfil
```

b. Save copies of some of the Sun pfil files before removing the Sun packages.

Removing the Sun packages will remove these files and you will need them to launch the public domain version of pfil.

```
cp /lib/svc/method/pfil   /lib/svc/method/pfil.dist
cp /usr/sbin/pfild /usr/sbin/pfild.dist
cp /etc/ipf/pfil.ap /etc/ipf/pfil.ap.dist
```

c. Remove the Sun IPFilter packages

```
pkgrm SUNWipfu
pkgrm SUNWipfr
```

d. Reboot the system

Step 4. Install pfil

a. Restore the pfil service configuration file

```
cp /lib/svc/method/pfil.dist  /lib/svc/method/pfil
```

b. Install pfil

```
pkgadd -d pfil_Solaris_10xxxx.pkg all
```

c. After installation, remove the Solaris 9 startup scripts as they are not needed, pfil will be using "svcadm"

```
rm /etc/rc2.d/S10pfil
rm /etc/rcS.d/S10pfil
rm /etc/init.d/pfil
```

d. Restore the pfil configuration file, NOTE, the config files for the public domain pfil are in /etc/opt/ipf, while Sun's config files are in /etc/ipf, because the service config files saved in step 4.d still refer to Sun's config file path, you should use /etc/ipf for consistency with Solaris 10.

```
cp /etc/ipf/pfil.ap.dist   /etc/ipf/pfil.ap
```

e. Configure pfil network device

```
vi /etc/ipf/pfil.ap  (uncomment appropriate device(s))
```

f. Enable the pfil service

```
svcadm -v enable pfil
```

if you receive an error on this command, then the service configuration file for pfil was removed and needs to be revived from the exported copy in step 4.d

```
svccfg -v import /var/tmp/pfil.svc
svcadm -v enable pfil
```

g. Reboot the system

h.. Verify the pfil service started

```
modinfo | grep pfil
```

This should show the public domain version of pfil

(pfil Stream module 2.1.11)
(pfil Streams driver 2.1.11)

Also check that pfil is loaded into the tcp/ip stack correctly

```
ifconfig ce0 modlist   (use your network interface)
```

If it isn't, then check that your interface type is uncommented in the pfil configuration file /etc/ipf/pfil.ap, reboot and try again

Step 5. Make sure SUNWgccruntime is installed. If it isn't, locate the package and install it:

```
pkgadd –d . SUNWgccruntime
```

Step 6. Install the Agent:

```
gunzip Agent-Solaris_5.x_sparc-7.x.x-xxxx.sparc.pkg.gz
pkgadd -d Agent-Solaris_5.x_sparc-7.x.x-xxxx.sparc.pkg all
```

To install the Solaris Sparc 8 and Sparc 9 Agents:

Note: For Solaris 8, SUN patch 113685 is required by the pfil driver. If you do not have SUN patch 113685 installed then you can obtain an alternate version of the pfil package by contacting Trend Micro.

Note: For Solaris 8, SUN patch 112438 (/dev/random) is required by the Deep Security Agent.

Step 1. Acquire all of the required packages (see above)

Step 2. Install libiconv-1.8-solx-sparc.gz:

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

Step 3. 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
```

Step 4. Install pfil:

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

Step 5. 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.)

Step 6. Install the Agent:

```
gunzip Agent-Solaris_5.x_sparc-5.x.x-xxxx.sparc.pkg.gz
pkgadd -d Agent-Solaris_5.x_sparc-5.x.x-xxxx.sparc.pkg all
```

To start, stop and reset the Agent on Solaris 10

```
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 8 and 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 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 Basic Deep Security Configuration 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)
```

Installing the Deep Security Agent for AIX

Step 1. Log in as Root

Step 2. Copy the package to a temporary folder ("/tmp")

Step 3. Unzip the package using gunzip:

```
/tmp> gunzip Agent-AIX_5.3-7.x.x-x.powerpc.bff.gz
```

Step 4. Install the Agent:

```
/tmp> installp –a –d /tmp ds_agent
```

To start and stop the Agent on AIX:

Enter either one of the following:

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

To install the Deep Security Agent for HP-UX:

Step 1. Log in as Root

Step 2. Copy the package to a temporary folder ("/tmp")

Step 3. Unzip the package using gunzip:

```
/tmp> gunzip Agent-HPUX_11.23_ia64-7.x.x-x.ia64.depot.gz
```

Step 4. 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_11.23_ia64-7.x.x-x.ia64.depot
ds_agent
```

To start and stop the Agent on HP-UX:

Enter one of the following:

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

Installing the Deep Security Notifier

The Deep Security Notifier is a utility for physical or virtual machines on Windows only, and provides local notifications of malware detection.

The stand-alone installation described in this section is intended for use on Agentless machines being protected by the Deep Security Virtual Appliance.

The Deep Security Notifier is automatically installed as part of the Deep Security Relay and Deep Security Agent installation on Windows, so it is not necessary to install using the steps below.

Copy the Installation Package

Copy the installation file to the target machine.

VMCI Settings for Agentless Notifier

To use the Notifier on an Agentless VM, you must enable VMCI:

Step 1. Stop the VMware image

Step 2. In vCenter, select the image and **Edit Settings**

Step 3. On the **Hardware** tab, select **VMCI Device**

Step 4. Select the **Enable VMCI Between VMs** option.

Step 5. Click **OK**.

Step 6. Restart the VMware image and install the Deep Security Notifier.

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.

Step 1. Double-click the installation file to run the installer package.

Click **Next** to begin the installation

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

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

Step 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 (you can manually disable notifications by double-clicking the tray icon to open the Notifier status and configuration window).

Basic Deep Security Configuration

This section describes some recommended Deep Security Manager configuration procedures.

Configure Email Notifications

Various warning and error conditions will raise Alerts in Deep Security Manager.

You should provide the Deep Security Manager to send email notifications via an existing SMTP server when Alerts are raised.

To setup email notifications:

1. In the Deep Security Manager, go to **System > System Settings > System.**
2. In the **SMTP** area, enter the address, credentials, and other details of your SMTP server.
3. Click the **Test SMTP Settings** button to test your SMTP configuration. If the configuration is successful, a success notification will be displayed. If it is not successful, a warning notification will be displayed. (If you receive the warning, make sure the SMTP server is running, accessible, and that the required ports are open as indicated in Preparation.) When you are done click **Save**.
4. Now go to **System > System Settings > Notifications**.
5. In the **Alert Notifications (from the Manager)** area, enter the email address to which you want the notifications to be sent. Click **Save**.

Note: This email address is not associated with any individual User's Deep Security account. The accounts of individual Users can be configured to receive email notifications as. To enable email notifications for a User, edit the User's **Properties** on the **System > Users** screen.

By default, the Manager will send a notification for every Alert.

You can refine the conditions under which notifications are sent by going to **System > System Settings > System** and clicking on **View Alert Configuration…** in the **Alert Configuration** area. The notification conditions can be configured for each Alert on the Alert's **Properties** screen.

For more information on Alerts and Notifications, see the corresponding sections in the online help or the Administrator's Guide.

Create Roles and User Accounts

Deep Security uses role-based access control to restrict Users' access to various parts of the Deep Security system. Once you have installed the Deep Security Manager you should create individual accounts for each User and assign each User a Role which will restrict their activities to all but those necessary for the completion of their duties.

Deep Security comes pre-configured with two Roles:

Full Access: The Full Access Role grants the User all possible privileges in terms of managing the Deep Security system including creating, editing, and deleting computers, computer groups, Security Profiles, Rules, Anti-Malware configurations, components, and others.

Auditor: The Auditor Role gives the User the ability to view all the information in the Deep Security system but without the ability to make any modifications except to their own personal settings, such as password, contact information, dashboard layout preferences, and others.

You can create new Roles which can restrict Users from editing or even seeing elements of the Deep Security system such as specific computers, the properties of security Rules, or the System Settings.

Before creating User accounts, identify the Roles that your Users will take and itemize what elements of the Deep Security system those Roles will require access to and what the nature of that access will be (viewing, editing, creating, etc.). Once you have created your Roles, you can then begin creating User accounts and assigning them specific Roles.

For details on how to create Roles and User accounts, see the corresponding sections of the online help or the Administrator's Guide.

Configure 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. Go to **System > System Information**. On the Network Map with Activity Graph, click the Manager name. On the **Manager Properties** screen, change the **Hostname** to use the IP address of the Manager computer.

2. From the **Computers** screen, **Add** the computer on which the Deep Security Relay is installed, and **Activate** it.
3. Check that the Relay Agent status is **Managed (Online).**
4. 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 System > 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 **System > Updates**. You should see the newly added Relay as a member of the Relay Group in the Relays section.
5. In the **Security Updates** section, the list of Components will all show "Not updated yet". Click **Update Components Now**, and then in the Component Update Wizard click **Finish**.
6. Updating the Components on the Deep Security Relay may take a few minutes.
7. When the Component Update Wizard shows that the update has completed, click **Finish**.
8. Return to **System > 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.

Relays can be arranged in hierarchies to optimize bandwidth.

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

To select a Relay for an Agent / Appliance, on the **Computers** screen right-click the Agent / Appliance and from the **Actions** menu, select **Assign Relay Group**.

Add Computers to the Deep Security Manager

Add computers that have Deep Security Agents to Deep Security Manager's Computers list.

There are four ways of adding computers to the Deep Security Manager **Computers** screen:

- Adding computers individually by specifying their IP addresses or hostnames
- Discovering computers 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.

This Quick Start Guide describes how to add an individual computer by specifying its IP address or hostname. To use one of the other methods, consult the online help or Administrator's Guide.

Go to the **Computers** screen by clicking **Computers** in the navigation pane and click **New** in the toolbar.

Type the hostname or IP address of the new computer in the **Hostname** textbox. The **New Computer** wizard also lets you specify a Security Profile which it will apply to the new computer if it finds the computer and determines that an unactivated Agent is present. Choose the default Security Profile that matches your computer's type and functionality. When you click **Next**, the wizard will find the computer and activate the Agent. When Agent activation has completed, the wizard will give you the option of opening the computer's **Details** screen which lets you configure many of the Agent's settings. Skip the **Details** screen for now.

Enable protection on computers

Activate the Deep Security Agents

Agents need to be activated by the Manager before rules can be assigned to them. The activation process includes the exchange of unique fingerprints between the Agent and the Manager. This ensures that only this Deep Security Manager (or one of its nodes) can send instructions to the Agent.

Note: Computers added individually to the **Computers** list have their Agents activated automatically. The Agent status will read "Managed (Online)" once the Agent has been activated.

To manually activate an Agent on a computer:

- Right-click on a computer in the **Computers** list and select **Actions > Activate**. The status column for the computer will change to "Managed (Online)".

Note: If you install an Agent on a virtual machine that was previously being protected only by a Deep Security Virtual Appliance, the virtual machine will have to be activated again from the Manager to register the presence of the Agent on the computer.

Apply Protection by Assigning a Security Profile to the Computer

Security Profiles contain rules for all Deep Security Protection Modules.

To assign a Security Profile to the computer:

1. Right-click on the computer to be protected in the **Computers** list and select **Actions > Assign Security Profile...**. Assign the default Security Profile that matches your computer's type and functionality. The default Security Profiles are configured with rules for Anti-Malware, Firewall, DPI, Integrity Monitoring and Log inspection protection.
2. After clicking **OK**, the Manager will send the Security Profile to the Agent. The **Computer Status** column and the Manager's status bar will display messages that the Agent is being updated. Once the Agent on the computer has been updated, the status column will read "Managed (Online)".

Note: When you change the configuration of an Agent/Appliance on a computer using the Deep Security Manager e.g. assigning a new Security Profile, the Deep Security Manager has to send the new information to the Agent/Appliance. This is a configuration update. Configuration updates usually happen immediately but you can force an update by clicking the "Update Configuration" button.

Basic Firewall Configuration

Many Firewall Rules and other elements of Deep Security make use of reusable components such as IP Lists, Mac Lists, and Schedules. If you are enabling Firewall protection and if the computers you are protecting are operating in a Windows Domain environment, modify the IP List named Domain Controller(s) to enable communication from the Domain Controller to the domain clients:

1. In the Deep Security Manager, go to **Components > IP Lists** and double-click on the **Domain Controller(s)** IP List to display its **Properties** window.
2. Edit the **IP(s)** text area replacing the IP 127.0.0.1 with the list of IPs that represent the Domain Controller(s) with which your protected computers may communicate.

3. Click **OK** to save your changes.

Then make sure the following two Firewall Rules are in effect:

- TCP from Domain Controller
- UDP from Domain Controller

When using Ethernet, ARP forms the basis of the TCP/IP stack. ARP facilities provide translation from IP addresses to Ethernet addresses, which are essential for sending packets to other systems on the local LAN segment. Without this conversion, there can be no other form of peer-to-peer IP communication.

It is thus very important that Deep Security Manager does not configure a Deep Security Agent to drop ARP packets, unless that is actually desired (configuration uses static ARP tables). If your network relies on dynamic ARP, make sure the following Firewall Rule is in effect:

- ARP

Java Security

The Deep Security Manager runs within a Java Virtual Machine (JVM), and the JVM places certain controls on network behavior. Java uses a cache to store both successful and unsuccessful DNS lookups. By default, successful lookups are cached forever as a guard against DNS spoofing attacks. However, this caching may prevent the Deep Security Manager from communicating with computers that use DHCP or whose IP address has changed. Deep Security Manager uses a value of 60 seconds for this setting.

Alternatively, in environments where DNS spoofing is a risk, the DNS cache can be configured to an unlimited lifetime. To configure the lifetime of the DNS cache for Deep Security Manager you need to do the following:

1. Open the java.security file located in [Manager install directory]\jre\lib\security
2. Find the line for the networkaddress.cache.ttl and set the value to -1:

```
networkaddress.cache.ttl=-1
```

3. Save the file and restart the Deep Security Manager service

For more information on the Java network cache settings see:

http://java.sun.com/javase/6/docs/technotes/guides/net/properties.html

Upgrading Deep Security 8.0 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.

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, DPI 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.

Upgrading the Deep Security Relay

Note: Remember that before upgrading a Deep Security Relay, you will need to make sure that Agent Self Protection is not enabled for the Seep Security Relay that you intend to upgrade. You can do this from Deep Security Manager **System >System Settings > Computers**. 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.

Upgrading Deep Security Relay for Windows

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

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.

Upgrading Deep Security Relay for Linux:

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

```
# rpm -U Relay-RedHat_2.6.18_8.EL5_i686-8.0.0-xxxx.i386.rpm
```

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 Deep Security Manager **System >System Settings > Computers**. 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.

Upgrading the Deep Security Agent for Windows

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

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 upgrade the Deep Security Agent for Linux:

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

```
# rpm -U Agent-RedHat_2.6.18_8.EL5_i686-8.0.0-xxxx.i386.rpm
```

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

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

Upgrading Deep Security with Agentless Anti-Malware

The following upgrade procedures apply to VMware environments where Deep Security is providing *Agentless Anti-Malware protection*.

Note: For upgrade procedures that apply to VMware environments where Deep Security is providing *Agentless Firewall and DPI protection only*, see Upgrading from Deep Security 7.5 with Agentless FW and DPI Only.

Note: For upgrade procedures that apply to VMware environments where Deep Security is providing *In-guest Agent-based protection only*, see Upgrading from Deep Security 7.5 with In-guest Agent-based Protection Only.

If you are running Deep Security 7.5 in a VMware vSphere 4 Environment and you are implementing Agentless Anti-Malware protection, both the Deep Security and vSphere software need to be upgraded at the same time. The Deep Security 7.5 components need to be upgraded to version 8.0 and the vSphere components need to be upgraded to version 5.0.

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 ESX
2. Restore the ESX (to uninstall the Deep Security Filter Driver)
3. Uninstall vShield Endpoint from the ESX
4. Uninstall the vShield Endpoint Guest Drivers from VMs on the ESX
5. Upgrade your vCenter
6. Upgrade the ESX and apply patch "ESX 5.0 (build 474610)"

7. Upgrade the vShield Manager
8. Configure the vShield Manager to integrate with the vCenter
9. Install vShield Endpoint on the ESX
10. Install vShield Endpoint guest drivers on the VMs
11. Restart the ESX

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: Although VMware will support a combination of ESX 4.1 and ESX 5.0 running on the same vCenter with vShield Manager 5.0, Deep Security will not be able to provide Agentless protection to the VMs on an ESX 4.1 if the vShield Manager has been upgraded to 5.0.

Note: Your VMs will not have Agentless protection on the ESX 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. Deploy and configure a Deep Security Relay
3. Add a security certificate to the Deep Security Manager for the vCenter and the vShield Manager
4. Import Deep Security 8 installation packages into the Deep Security Manager
5. Prepare the newly upgraded ESX (this installs the Deep Security Filter Driver on the ESX)
6. Reactivate your Deep Security Virtual Appliance in preparation for upgrade
7. Upgrade the Deep Security Virtual Appliance on your ESX
8. Activate the guest VMs on the ESX

9. 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. The Deep Security Manager 8 release notes include references to locations on VMware's Web site where you can find the latest information and knowledge base articles.

The following table lists the components that will be upgraded during this phase:

Component	Pre-Upgrade Version	Post-Upgrade Version
vCenter Server	4.1 U1	5.0 (4.1.0 build 258902+)
ESX	4.1 U1	5.0 (4.1.0 build 348481+)
vShield Manager	4.1	5.0 (4.1.0 build 310451+)
Endpoint (for ESX)	3.0.8	5.0 (3.0.8 build 30897+)
Endpoint guest drivers	1.0.0.2	5.0

Step 1. Deactivate the Deep Security Virtual Appliance on the ESX

In the Deep Security Manager, go to the **Computers** screen, right-click on the Virtual Appliance and select **Actions > Deactivate Appliance**.

Step 2. Restore the ESX

On the **Computers** screen of the Deep Security Manager, right-click the ESX and select **Actions > Restore ESX...** and follow the steps in the wizard. (This procedure will uninstall the 7.5 Deep Security Filter Driver from the ESX.)

Step 3. Uninstall vShield Endpoint from the ESX

Using vShield Manager 4.1, uninstall vShield Endpoint from the ESX.

Step 4. Uninstall the vShield Endpoint Guest Drivers from VMs on the ESX

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

Step 5. Upgrade your vCenter

Run the VIM installer following the directions provided by VMware.

Step 6. Upgrade the ESX and apply patch "ESX 5.0"

Upgrade the ESX to ESX 5.0 and apply patch "ESX 5.0 Patch (build 474610)".

Step 7. Upgrade the vShield Manager

Follow the directions in VMware's *vShield_Quick_Start_Guide.pdf* to upgrade the vShield Manager.

Step 8. Configure the vShield Manager to integrate with the vCenter

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 reintegrate it with the vCenter.

Step 9. Install vShield Endpoint on the ESX

Use the vShield Manager to install vShield Endpoint on the ESX.

Step 10. Install vShield Endpoint guest drivers on the VMs

Use VMware Tools to install the vShield Endpoint guest drivers ("vShield Drivers") on the VMs.

Step 11. Restart the ESX

Restart the ESX to complete the VMware phase of the upgrade process.

When the ESX 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. 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 following table lists the components that will be upgraded during this phase. The software must be downloaded from the Trend Micro Download Center to a location from which it can be imported into the Deep Security Manager.

Component	Pre-Upgrade Version	Post-Upgrade Version
Deep Security Manager	7.5	8.0 (1448+)

Component	Pre-Upgrade Version	Post-Upgrade Version
Deep Security Filter Driver	7.5	8.0 (1189+)
Deep Security Virtual Appliance	7.5	8.0 (1199+)
Deep Security Agent(s)	7.5	8.0 (1201+)
Deep Security Relay	n/a	8.0 (1201+)

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.

Step 1. Upgrade the Deep Security Manager

Upgrade the Deep Security Manager to version 8.0. Follow the same procedures as described in Installing Deep Security Manager.

Step 2. Deploy and configure a Deep Security Relay

Follow the instructions described in Deploying the Deep Security Relay.

Step 3. Add a security certificate to the Deep Security Manager for the vCenter and the vShield Manager

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.

Step 4. Import Deep Security 8 installation packages into the Deep Security Manager

In the Deep Security Manager, go to **System > Updates > Software Packages** and import the Deep Security Agent 8, Deep Security Relay 8, Deep Security Filter Driver 8, and Deep Security Virtual Appliance 8 installation packages.

Step 5. Prepare the newly upgraded ESX (this installs the Deep Security Filter Driver

on the ESX)

After upgrading the ESX in phase one, the ESX will be "unprepared". Follow the instructions in Preparing ESXi for Deep Security Virtual Appliance Deployment to prepare the ESX.

Step 6. Reactivate the Deep Security Virtual Appliance in preparation for upgrade

On the **Computers** screen in the Deep Security Manager, right-click on the Deep Security Virtual Appliance and select **Action > Activate Appliance**. Do not activate the VMs at this time.

Step 7. Upgrade the Deep Security Virtual Appliance on your ESX

On the **Computers** screen in the Deep Security Manager, right-click on the Deep Security Virtual Appliance and select **Action > Upgrade Appliance…**

Step 8. Activate the guest VMs on the ESX

Follow the instructions described in Activating Guest Virtual Machines.

Step 9. Deploy Deep Security Agents (if required)

Follow the instructions described in Deploying Deep Security Agents.

Upgrading VMware 4 and Deep Security 7.5 with Agentless Anti-Malware protection is now complete.

Upgrading from Deep Security 7.5 with Agentless FW and DPI Only

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

Note: For upgrade procedures that apply to VMware environments where Deep Security is providing *Agentless Anti-Malware protection*, see Upgrading from Deep Security 7.5 with Agentless Anti-Malware.

Note: For upgrade procedures that apply to VMware environments where Deep Security is providing In-guest *Agent-based protection only*, see Upgrading from Deep Security 7.5 with In-guest Agent-based Protection Only.

If you are running Deep Security 7.5 in a VMware vSphere 4 Environment and you are implementing Agentless Firewall and DPI protection only, both the Deep Security and

vSphere software need to be upgraded at the same time. The Deep Security 7.5 components need to be upgraded to version 8.0 and the vSphere components need to be upgraded to version 5.0.

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.

Note: Deep Security Manager 8 can manage 7.5 Deep Security Virtual Appliance on a 4.1 ESX with the 7.5 Deep Security Filter Driver.

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 ESX
2. Restore the ESX (to uninstall the Deep Security Filter Driver)
3. Upgrade your vCenter
4. Upgrade the ESX and apply patch "ESX 5.0"

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 8 installation packages into the Deep Security Manager
4. Prepare the newly upgraded ESX (this installs the Deep Security Filter Driver on the ESX)
5. Reactivate your Deep Security Virtual Appliance in preparation for upgrade
6. Upgrade the Deep Security Virtual Appliance on your ESX
7. Deploy and configure a Deep Security Relay
8. Activate the guest VMs on the ESX
9. Deploy Deep Security Agents (if required)

Phase One: Upgrading Your VMware Components

The following table lists the components that will be upgraded during this phase:

Component	Pre-Upgrade Version	Pre-Upgrade Version
vCenter Server	4.1 U1	5.0 (4.1.0 build 258902)
ESX	4.1 U1	5.0 (4.1.0 build 348481)

Step 1. Deactivate the Deep Security Virtual Appliance on the ESX

In the Deep Security Manager, go to the **Computers** screen, right-click on the Virtual Appliance and select **Actions > Deactivate Appliance**.

Step 2. Restore the ESX

On the **Computers** screen of the Deep Security Manager, right-click the ESX and select **Actions > Restore ESX...** and follow the steps in the wizard.

Step 3. Upgrade your vCenter

Run the VIM installer following the directions provided by VMware.

Step 4. Upgrade the ESX and apply patch "ESX 5.0"

Upgrade the ESX to ESX 5.0 and apply patch "ESX 5.0 Patch (build 474610)".

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 following table lists the components that will be upgraded during this phase. The software must be downloaded from the Trend Micro Download Center to a location from which it can be imported into the Deep Security Manager.

Component	Pre-Upgrade Version	Post-Upgrade Version
Deep Security Manager	7.5	8.0 (1448+)

Component	Pre-Upgrade Version	Post-Upgrade Version
Deep Security Filter Driver	7.5	8.0 (1189+)
Deep Security Virtual Appliance	7.5	8.0 (1199+)
Deep Security Agent(s)	7.5	8.0 (1201+)
Deep Security Relay	n/a	8.0 (1201+)

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.

Step 1. Upgrade the Deep Security Manager

Upgrade the Deep Security Manager to version 8.0. Follow the same procedures as described in Installing Deep Security Manager.

Step 2. Add a security certificate to the Deep Security Manager for the vCenter and the vShield Manager

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.

Step 3. Import Deep Security 8 installation packages into the Deep Security Manager

In the Deep Security Manager, go to **System > Updates > Software Packages** and import the Deep Security Agent 8, Deep Security Relay 8, Deep Security Filter Driver 8, and Deep Security Virtual Appliance 8 installation packages.

Step 4. Prepare the newly upgraded ESX (this installs the Deep Security Filter Driver on the ESX)

After upgrading the ESX in phase one, the ESX will be "unprepared".

Follow the instructions in Preparing ESXi for Deep Security Virtual Appliance Deployment to prepare the ESX.

Step 5. Reactivate the Deep Security Virtual Appliance in preparation for upgrade

On the **Computers** screen in the Deep Security Manager, right-click on the Deep Security Virtual Appliance and select **Action > Activate Appliance**. Do not activate the VMs at this time.

Step 6. Upgrade the Deep Security Virtual Appliance on your ESX

On the **Computers** screen in the Deep Security Manager, right-click on the Deep Security Virtual Appliance and select **Action > Upgrade Appliance…**

Step 7. Deploy and configure a Deep Security Relay

Follow the instructions described in Deploying the Deep Security Relay.

Step 8. Activate the guest VMs on the ESX

Follow the instructions described in Activating Guest Virtual Machines.

Step 9. Deploy Deep Security Agents (if required)

Follow the instructions described in Deploying Deep Security Agents.

Upgrading VMware 4 and Deep Security 7.5 with Agentless Firewall and DPI protection only is now complete.

Upgrading from Deep Security 7.5 with In-guest Agent-Based Protection Only

The following upgrade procedures apply to VMware environments where Deep Security is providing *in-guest Agent-based protection only*.

Note: For upgrade procedures that apply to VMware environments where Deep Security is providing *Agentless Anti-Malware protection*, see Upgrading from Deep Security 7.5 with Agentless Anti-Malware.

Note: For upgrade procedures that apply to VMware environments where Deep Security is providing *Agentless Firewall and DPI protection only*, see Upgrading from Deep Security 7.5 with Agentless FW and DPI Only.

If you are running Deep Security 7.5 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 8.0.

The Upgrade Procedure

The following table lists the components that will be upgraded. These 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.

Component	Pre-Upgrade Version	Post-Upgrade Version
Deep Security Manager	7.5	8.0 (1448+)
Deep Security Filter Driver	7.5	8.0 (1189+)
Deep Security Agent(s)	7.5	8.0 (1201+)
Deep Security Relay	n/a	8.0 (1201+)

The procedures for upgrading from Deep Security 7.5 to Deep Security 8.0 in a VMware environment when providing in-guest Agent-based protection only are as follows:

Step 1. Upgrade the Deep Security Manager from 7.5 to 8.0

Follow the same instructions as described in Installing Deep Security Manager.

Step 2. Import the Deep Security 8 installation packages

Go to **System > Updates > Software Packages** and import the Deep Security Agent 8.0, Relay 8.0, Filter Driver 8.0, and Virtual Appliance 8.0 installation packages.

Step 3. Deploy at least one Deep Security Relay

Follow the instructions as described in Deploying the Deep Security Relay.

Step 4. Upgrade any Deep Security Agents

Follow the instructions described in Deploying Deep Security Agents.

Upgrading Deep Security 7.5 with in-guest Agent-based protection only is now complete.

.

Appendix A

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 some mandatory entries and some optional entries.

Note: For optional entries, if you enter a property value that is not one of the allowed values, then the DSM install will use the default value instead.

Mandatory Settings

LicenseScreen

Enter the applicable activation code(s).

Property	Acceptable Values	Default value	Note
LicenseScreen.License.-1=<value>	<AC for all modules>	blank	blank is not acceptable

OR

Property	Acceptable Values	Default value	Note
LicenseScreen.License.0=<value>	<AC for Anti-Malware>	blank	blank is not acceptable
LicenseScreen.License.1=<value>	<AC for Firewall/DPI>	blank	blank is not acceptable
LicenseScreen.License.2=<value>	<AC for Integrity Monitoring>	blank	blank is not acceptable
LicenseScreen.License.3=<value>	<AC for Log Inspection>	blank	blank is not acceptable

CredentialsScreen

Property	Acceptable Values	Default value	Note
CredentialsScreen.Administrator.Username=<value>	<username for master administrator>	blank	blank is not acceptable
CredentialsScreen.Administrator.Password=<value>	<password for the master administrator>	blank	blank is not acceptable

Optional Settings

UpgradeVerificationScreen

Note: this screen/setting is not used unless an existing installation is detected.

Property	Acceptable Values	Default value	Note
UpgradeVerificationScreen.Overwrite=<value>	True	False	**True** selects a completely new Manager installation, discarding all existing data
	False		

Note: If you set this value to **True**, the install 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	Acceptable Values	Default value	Note
DatabaseScreen.DatabaseType=<value>	Embedded	Embedded	
	Microsoft SQL Server		
	Oracle		
DatabaseScreen.Hostname=<value>	The name or IP address of the database host	Current host name	
DatabaseScreen.DatabaseName=<value>	Any string	dsm	Not required for Embedded
DatabaseScreen.Transport=<value>	Named Pipes	Named Pipes	Required for SQL Server only
	TCP		
DatabaseScreen.Username=<value>		blank	blank is not an acceptable value. Not required for Embedded
DatabaseScreen.Password=<value>		blank	blank is

Property	Acceptable Values	Default value	Note
			not an acceptable value. Not required for Embedded
DatabaseScreen.SQLServer.Instance=<value>		blank	blank implies default instance. Optional, required for SQL Server only
DatabaseScreen.SQLServer.Domain=<value>		blank	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	Acceptable Values	Default value	Note
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	
AddressAndPorts.NewNode=<value>	True	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
	False		

Property	Acceptable Values	Default value	Note
			"New Node" installation information about the existing database to be provided via the DatabaseScreen properties.

Credentials Screen

Property	Acceptable Values	Default value	Note
CredentialsScreen.UseStrongPasswords=<value>	True	True	**True** indicates the DSM should be set up to enforce strong passwords
	False		

SecurityUpdateScreen

Property	Acceptable Values	Default value	Note
SecurityUpdateScreen.UpdateComponents=<value>	True	True	**True** indicates that you want Deep Security Manager to automatically retrieve the latest Components
	False		
SecurityUpdateScreen.UpdateSoftware=<value>	True	True	**True** indicates that you want to setup a task to automatically check for new software.
	False		

RelayScreen

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

Property	Acceptable Values	Default value	Note
RelayScreen.Install=<value>	True	True	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.
	False		

SmartProtectionNetworkScreen

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

Property	Acceptable Values	Default value	Note
SmartProtectionNetworkScreen.EnableFeedback=<value>	True	True	True enables Trend Micro Smart Feedback.
	False		
SmartProtectionNetworkScreen.IndustryType=<value>	Not specified	blank	blank corresponds to **Not specified**
	Banking		
	Communications and media		
	Education		
	Energy		
	Fast-moving		

Property	Acceptable Values	Default value	Note
	consumer goods (FMCG)		
	Financial		
	Food and beverage		
	Government		
	Healthcare		
	Insurance		
	Manufacturing		
	Materials		
	Media		
	Oil and gas		
	Real estate		
	Retail		
	Technology		
	Telecommunications		
	Transportation		
	Utilities		
	Other		

Installation Output

This section shows an example output from a successful install, followed by an example output from a failed install (invalid license). The **[Error]** tag in the trace is used to clearly indicate 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...
```

Appendix B

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:

Step 1. Go to the directory where the installer is located.

Step 2. Create a new text file called "Manager-Windows-8.0.xxxx.xxx.vmoptions" or

"**Manager-Linux-8.0.xxxx.xxx.vmoptions**", depending on your installation platform

(where "xxxx.xxx" is the build number of the installer and platform).

Step 3. Edit the file by adding the line: **"-Xmx800m**" (in this example, 800MB of memory will be made available to the installer.)

Step 4 Save the file and launch the installer.

Configuring the Deep Security Manager's Maximum Memory Usage

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

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

Step 1. Go to the Deep Security Manager directory (the same directory as Deep Security Manager.exe), e.g. C:\Program Files\Trend Micro\Deep Security Manager.

Step 2. Create a new file called "Deep Security Manager.vmoptions".

Step 3. Edit the file by adding the line: " **-Xmx3g**" (in this example, "3g" will make 3 GB memory available to the DSM.)

Step 4. Save the file and restart DSM.

Step 5. You can verify the new setting by going to **System > System Information** and in the **System Details** area, expand **Manager Node > Memory**. The **Maximum Memory** value should now indicate the new configuration setting.

Appendix C

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 (Anti-Malware only)	Recommended memory allocation (Anti-Malware and DPI)
0 – 10 VMs	512MB	1GB
10 – 32 VMs	1GB	1GB
33 - 64 VMs	2GB	2GB

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:

Step 1. In your VMware vSphere Client, right-click on the DSVA and select **Power > Shut Down Guest.**

Step 2. Right-click on the DSVA again and select **Edit Settings…** The Virtual Machine Properties screen displays.

Step 3. On the **Hardware** tab, select **Memory** and change the memory allocation to the desired value.

Step 4. Click **OK**.

Step 5. Right-click the DSVA again and select **Power > Power On**.

Appendix D

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 **System > 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 **How To…** 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.

Appendix E

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 real certificate. (The certificate is maintained on Deep Security Manager upgrades.)

More information on generating the certificate can be found at Thawte Tomcat Support.

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:

Step 1. Go to the Deep Security Manager installation directory (C:\Program Files\Trend Micro\Deep Security Manager) and make a new folder called "**Backupkeystore**"

Step 2. Copy **.keystore** and **configuration.properties** to the newly created folder Backupkeystore

Step 3. Open command prompt and go to the following location:

```
C:\Program Files\ Trend Micro \Deep Security Manager\jre\bin
```

Step 4. Run the following command which will create a self signed certificate:

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

Step 5. Choose password: changeit

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

Step 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

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

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

Step 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
```

Step 9. Send the **certrequest.csr** to your CA to sign. In return you will get two files. One is a certificate response and the second is the CA certificate itself.

Step 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"
```

Step 11. Run the following command to import the CA cert 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)

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

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

```
certresponse.txt
```

Step 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
```

Step 14. Copy the .keystore file from your user home directory C:\Documents and Settings\Administrator to C:\Program Files\ Trend Micro \Deep Security Manager\

Step 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$85ef650a5c40bb0f914993ac1ad855f48216fd0664ed254
4bbec6de80160b2fe9800f79f913f28e80381c8e71f2fed96a2aa522ada039a
7abfa01542d42dbe36 installed=true serviceName= Trend Micro Deep
Security Manager
```

Step 16. Replace the password in the following string:

```
keystorePass=xxxx
```

where “xxxx” is the password you supplied in step five

Step 17. Save and close the file

Step 18. Restart the Deep Security Manager service

Step 19. Connect to the Deep Security Manager with your browser and you will notice that the new SSL certificate is signed by your CA.

Appendix F

Interoperability with Agent and Appliance Releases

The following table summarizes the interoperability of *currently supported* versions of Deep Security software components. Keep in mind that an older version of a Deep Security Agent or Deep Security Virtual Appliance may not provide the functionality introduced in a newer version of the Deep Security Manager.

	DSM 8.0	DSM 7.5	DSM 7.0
DSA 8.0	✓	✗	✗
DSA 7.5	✓	✓	✗
DSA 7.0	✓	✓	✓
DSA 6.1	✗	✓	✓
DSVA 8.0	✓	✗	✗
DSVA 7.5	✓	✓	✗
DSVA 7.0	✗	✗	✓

DSM: Deep Security Manager
DSA: Deep Security Agent

DSVA: Deep Security Virtual Appliance

 **:** Interoperable
 **:** Not Interoperable

Note: DS 7.5 DSVA can only run on VMware ESX version 4.1, and must be deployed after preparation with a DS 7.5 Filter Driver. DS 7.5 Filter Driver and DSVA can be deployed from DSM 8.0.

Appendix G

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" DPI 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 ESX.

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 **System >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

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

Configuration

Problem

Traffic Analysis is not working.

Solution

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

Problem

Many DPI 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 DPI false positives. The false positives are caused by the contents of the DPI Rules (when saving to the database) triggering the DPI 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:

1. 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.

2. 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 DPI 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 "DPI Rules" page for computer and unassign DPI 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" DPI Rules view but note that it will only show DPI 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 DPI Rules that has a footprint that is too large for some Computers. If the Security Profile itself still has too many DPI 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 DPI Rules are actually recommended to be applied to the various Computers. This should allow you to reduce the number of DPI 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 **System > 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.

Appendix H

FAQs

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 8.0?

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

Where can I download the technical documents for Deep Security 8.0?

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

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 **System > Users,** right-click on the User select **Set Password…**.

How can I unlock a locked out User?

In the Manager, go to **System > 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 System > 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 8.0?

Your existing protection modules will be supported. When upgrading from Deep Security 7.0 or earlier, you will need contact a sales representative for a new Activation Code to enter during the upgrade process.

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 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.

Appendix I

Known Incompatibilities

Note: Please consult the Deep Security Manager, Deep Security Virtual Appliance, or Deep Security Agent readme files for the most recent list of known incompatibilities.

Appendix J

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 it's 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

12. 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 Deep Security Manager **System >System Settings > Computers**. 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_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.

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 Deep Security Manager **System >System Settings > Computers**. 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.

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:

```
/tmp> 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

Note: Remember that before uninstalling a Deep Security Manager, you should de-activate and uninstall any Deep Security Agents or Relays that are managed by that Manager. If you do not want to uninstall the Agents at this time, you should make sure that you can do so later by configuring the Agent Self Protection from Deep Security Manager **System >System Settings > Computers**.

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 uninstall from the command line:

```
Uninstall.exe
```

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

Note: In the 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:

```
Uninstall.exe
```

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

Note: In the 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").

Appendix K

Minimum VMware Permissions for DSVA Deployment

The following tables list the VMware environment permissions required by an administrator to deploy the Deep Security Virtual Appliance.

These permissions 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 permissions 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.

Preparing the ESXi Host

Host -> Configuration -> Change Settings	Permissions Required to Query Modules on ESXi
Host -> Configuration -> Maintenance	Permissions Required to Enter and Exit Maintenance Mode
Host -> Configuration -> Network Configuration	Permissions required to add new virtual switch, port group, virtual nic etc.
Host -> Configuration -> Advanced Settings	Permissions required to setup networking for dvfilter communication on ESXi
Host -> Configuration -> Query Patch	Permissions required to install Filter Driver
Host -> Configuration -> Connection	Permissions to disconnect/reconnect a host
Host -> Configuration -> Security profile and firewall	Permissions to reconfiguration outgoing FW connections to allow retrieval of Filter Driver package from DSM
Global -> Cancel Task	Permissions required to cancel a task if required

Deploying the Virtual Appliance

vApp -> Import	Permissions to deploy DSVA from OVF file
Datastore -> Allocate Space	Permissions required to allocate space for DSVA on datastore.
Host -> Configuration -> Virtual machine autostart configuration	Permissions to set DSVA to autostart on ESXi
Network -> Assign Network	Permissions to assign DSVA to networks
Virtual Machine -> Configuration -> Add new disk	Permissions to add disks to DSVA
Virtual Machine -> Interaction -> Power On	Permissions to power on DSVA
Virtual Machine -> Interaction -> Power Off	Permissions to power off DSVA

Activating the Virtual Machine (the protected computer)

Virtual Machine -> Configuration -> Advanced	Permissions to reconfigure virtual machine for dvfilter

Ongoing Operations

Host -> Configuration -> Change Settings	Permissions Required to Query Modules on ESXi
Virtual Machine -> Configuration -> Advanced	Permissions to reconfigure virtual machine for dvfilter

Appendix L

Manual Install/Uninstall of dvfilter-dsa Driver

Manual Uninstall of the dvfilter-dsa Driver

Step 1.	SSH into the ESXi and login using root account.
Step 2.	Run the following command to get the dvfilter-dsa driver complete name: `# esxcli software vib list | grep dvfilter-dsa`
Step 3.	Run the following command to uninstall the dvfilter-dsa driver: `# esxcli software vib remove -maintenancemode -n dvfilter-dsa`

Manual Install of the dvfilter-dsa Driver

Step 1.	Copy the Deep Security Filter Driver .zip package to the ESXi host using scp. Copy the file to the /tmp folder.
Step 2.	Make sure all the Virtual Machines are powered-off or migrated to another ESXi host.
Step 3.	Put the ESXi into maintenance mode.
Step 4.	SSH into the ESXi and login using root account.

Step 5.	Install the Filter Driver using the following command: `# esxcli software vib install -maintenancemode -d <Filter Driver .zip file>`
Step 6.	Reboot the ESXi by typing `reboot`.
Step 7.	Exit ESXi maintenance mode.
Step 8.	The ESXi should automatically show **Prepared** status on the Deep Security Manager console.

Step 9	Verify the status of the Filter Driver:
	
	`# esxcli software vib list`
	`# vmkload_mod –l | grep dvfilter`

Appendix M

Support for Earlier Versions of VMware ESX

Deep Security 8.0 is designed to provide protection in a Virtual environment using VMware ESXi 5.0 operating system.

If you are using VMware ESX/ESXi version 4.1, you can use Deep Security Manager 8.0 with Deep Security Virtual Appliance 7.5 (which must be installed on an ESX prepared with Deep Security Filter Driver 7.5).

Deep Security Manager will not be able to protect VMs hosted on ESX/ESXi 4.1 and ESXi 5.0 hypervisors being managed by the same vCenter.

Deep Security Agents are supported on Virtual Machines ESX/ESXi 3.5, 4.0 and 4.1.