

# 9.5 Deep Security

## Installation Guide

Basic Components

Advanced Protection for Physical, Virtual, and Cloud Servers



Cloud & Data Center



Complete End User



Cyber Threats

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

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

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

Document version: 1.2

Document number: APEM96336/140306

Release date: Aug 27, 2014

Document generated: Aug 27, 2014 (18:34:39)

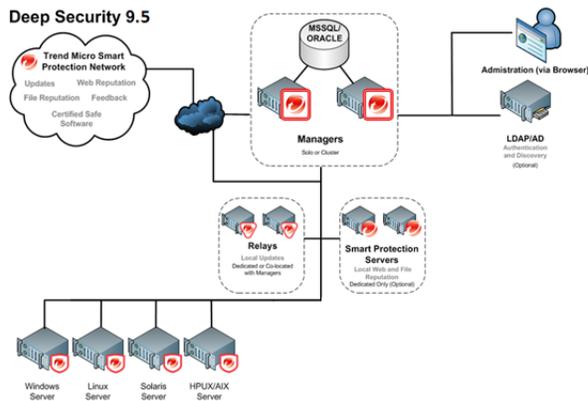
# Table of Contents

Introduction .....	4
About This Document.....	5
About Deep Security .....	7
What's New in Deep Security 9.5 .....	10
Preparation .....	11
System Requirements .....	12
What You Will Need (Basic Components) .....	14
Database Deployment Considerations.....	17
Installation .....	19
Installing the Deep Security Manager .....	20
Installing the Deep Security Agent.....	27
Installing and Configuring a Relay-enabled Agent.....	35
Database Deployment Considerations.....	17
Upgrading .....	38
Upgrading a Basic Agent-based Installation.....	39
Quick Start .....	42
Quick Start: System Configuration .....	43
Quick Start: Protecting a Computer.....	51
Appendices .....	58
Deep Security Manager Memory Usage.....	59
Silent Install of Deep Security Manager .....	60
Deep Security Manager Settings Properties File .....	62
Deep Security Manager Performance Features .....	67
Creating an SSL Authentication Certificate .....	69
Protecting a Mobile Laptop.....	71

# Introduction

# About This Document

## Deep Security 9.5 Installation Guide (Basic)



This document describes the installation and configuration of the basic Deep Security 9.5 software components necessary to provide basic agent-based protection to your computers:

1. The Deep Security Manager
2. The Deep Security Agent (with optional Relay functionality)

This document covers:

1. System Requirements
2. Preparation
3. Database configuration guidelines
4. Installing the Deep Security Manager management console
5. Installing Deep Security Agents
6. Implementing Deep Security protection using Security Policies and Recommendation Scans
7. Guidelines for monitoring and maintaining your Deep Security installation

## Intended Audience

This document is intended for anyone who wants to implement Agent-based Deep Security 9.5 protection. The information is intended for experienced system administrators who have good experience with software deployments and scripting languages.

## Other Deep Security 9.5 Documentation

- Deep Security 9.5 Installation Guide (Cloud)
- Deep Security 9.5 Installation Guide (VMware NSX)
- Deep Security 9.5 Installation Guide (VMware vShield)
- Deep Security 9.5 User's Guide

- [Deep Security 9.5 Supported Features and Platforms](#)
- [Deep Security 9.5 Supported Linux Kernels](#)

# About Deep Security

Deep Security provides advanced server security for physical, virtual, and cloud servers. It protects enterprise applications and data from breaches and business disruptions without requiring emergency patching. This comprehensive, centrally managed platform helps you simplify security operations while enabling regulatory compliance and accelerating the ROI of virtualization and cloud projects. The following tightly integrated modules easily expand the platform to ensure server, application, and data security across physical, virtual, and cloud servers, as well as virtual desktops.

## Protection Modules

### Anti-Malware

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

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

### Web Reputation

**Strengthens protection against web threats for servers and virtual desktops.**

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

### Firewall

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

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

### Intrusion Prevention

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

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

**Defends against web application vulnerabilities**

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

**Identifies malicious software accessing the network**

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

## Integrity Monitoring

**Detects and reports malicious and unexpected changes to files and systems registry in real time. Now available in agentless form factor.**

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

## Log Inspection

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

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

## Deep Security Components

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

- **Deep Security Manager**, the centralized Web-based management console which administrators use to configure security policy and deploy protection to the enforcement components: the Deep Security Virtual Appliance and the Deep Security Agent.
- **Deep Security Virtual Appliance** is a security virtual machine built for VMware vSphere environments that Agentlessly provides Anti-Malware, Web Reputation Service, Firewall, Intrusion Prevention, and Integrity Monitoring protection to virtual machines.
- **Deep Security Agent** is a security agent deployed directly on a computer which provides Anti-Malware, Web Reputation Service, Firewall, Intrusion Prevention, Integrity Monitoring, and Log Inspection protection to computers on which it is installed.
  - The Deep Security Agent contains a **Relay Module**. A Relay-enabled Agent distributes Software and Security Updates throughout your network of Deep Security components.
- **Deep Security Notifier** is a Windows System Tray application that communicates information on the local computer about security status and events, and, in the case of Deep Security Relays, also provides information about the Security Updates being distributed from the local machine.

## Deep Security Manager

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

## Policies

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

## Dashboard

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

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

## Built-in Security

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

## Deep Security Virtual Appliance

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

## Deep Security Agent

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

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

## Deep Security Notifier

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

# What's New in Deep Security 9.5

## VMware vSphere 5.5 Support

- Security for network virtualization and Software-Defined Data Center with NSX
- Support for mixed-model deployments (NSX and vShield)

## Smarter, Lightweight Agent

- Lightweight installer
- Selective deployment of Protection Modules to Agents based on Security Policy requirements results in smaller Agent footprint
- Automatic support for new Linux Kernels

## Trend Micro Control Manager Enhancements

- More dashboard widgets with drill-down capability
- Full Events for Anti-Malware and Web Reputation Service

## Linux Support

- New distributions: CloudLinux, Oracle Unbreakable
- On-demand Anti-Malware scanning for all distributions
- Real-Time Anti-Malware for Red Hat and SuSE

---

**Note:** For a list of supported Deep Security features by software platform, see the document titled **Deep Security 9.5 Supported Features and Platforms**. For a list of specific Linux kernels supported for each platform, see the document titled **Deep Security 9.5 Supported Linux Kernels**.

---

## Improvements to Security and Software Update Management

- Improved visibility into Security and Software Update status
- Improved accessibility to Software Updates

## Multi-Tenant Improvements

- Sign in as a Tenant
- Security Model Usage Report

# Preparation

# System Requirements

## Deep Security Manager

- **Memory:** 8GB, which includes:
  - 4GB heap memory
  - 1.5GB JVM overhead
  - 2GB operating system overhead
- **Disk Space:** 1.5GB (5GB recommended)
- **Operating System:**
  - Windows Server 2012 (64-bit), Windows Server 2012 R2 (64-bit)
  - Windows Server 2008 (64-bit), Windows Server 2008 R2 (64-bit)
  - Windows 2003 Server SP2 (64-bit), Windows 2003 Server R2 (64-bit)
  - Red Hat Linux 5/6 (64-bit)
- **Database:**
  - Oracle 11g, Oracle 11g Express
  - Oracle 10g, Oracle 10g Express
  - Microsoft SQL Server 2014, Microsoft SQL Server 2014 Express
  - Microsoft SQL Server 2012, Microsoft SQL Server 2012 Express
  - Microsoft SQL Server 2008, Microsoft SQL Server 2008 Express
  - Microsoft SQL Server 2008 R2, Microsoft SQL Server 2008 R2 Express
- **Web Browser:** Firefox 24+, Internet Explorer 9.x, Internet Explorer 10.x, Internet Explorer 11.x, Chrome 33+, Safari 6+. (Cookies enabled.)
  - **Monitor:** 1024 x 768 resolution at 256 colors or higher

## Deep Security Agent

- **Memory:**
  - **with Anti-Malware protection:** 512MB
  - **without Anti-Malware protection:** 128MB
- **Disk Space:**
  - **with Anti-Malware protection:** 1GB
  - **without Anti-Malware protection:** 500MB
  - **with Relay functionality enabled:** 8GB
- **Windows:**
  - Windows Server 2012 (64-bit), Windows Server 2012 R2 (64-bit)
  - Windows 8.1 (32-bit and 64-bit)
  - Windows 8 (32-bit and 64-bit)
  - Windows 7 (32-bit and 64-bit)
  - Windows Server 2008 (32-bit and 64-bit), Windows Server 2008 R2 (64-bit)

- Windows Vista (32-bit and 64-bit)
  - Windows Server 2003 SP1 (32-bit and 64-bit) with patch "Windows Server 2003 Scalable Networking Pack"
  - Windows Server 2003 SP2 (32-bit and 64-bit)
  - Windows Server 2003 R2 SP2 (32-bit and 64-bit)
  - Windows XP (32-bit and 64-bit)
  - **With Relay functionality enabled:** All 64-bit Windows versions above
- **Linux:**
    - Red Hat 5 (32-bit and 64-bit)
    - Red Hat 6 (32-bit and 64-bit)
    - Oracle Linux 5 (32-bit and 64-bit)
    - Oracle Linux 6 (32-bit and 64-bit)
    - CentOS 5 (32-bit and 64-bit)
    - CentOS 6 (32-bit and 64-bit)
    - SuSE 10 SP3 and SP4 (32-bit and 64-bit)
    - SuSE 11 SP1, SP2, and SP3 (32-bit and 64-bit)
    - CloudLinux 5 (32-bit and 64-bit)
    - CloudLinux 6 (32-bit and 64-bit)
    - Amazon Red Hat Enterprise 6 EC2 (32-bit and 64-bit)
    - Amazon SuSE 11 EC2 (32-bit and 64-bit)
    - Amazon Ubuntu 12 EC2 (32-bit and 64-bit)
    - Amazon AMI Linux EC2 (32-bit and 64-bit)
    - Ubuntu 10.04 LTS (64-bit)
    - Ubuntu 12.04 LTS(64-bit)
    - Ubuntu 14.04 LTS (64-bit)
    - **With Relay functionality enabled:** All 64-bit Linux versions above

---

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

---

**Note:** *For a list of supported Deep Security features by software platform, see the document titled **Deep Security 9.5 Supported Features and Platforms**. For a list of specific Linux kernels supported for each platform, see the document titled **Deep Security 9.5 Supported Linux Kernels**.*

---

# What You Will Need (Basic Components)

## Deep Security Software Packages

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

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

---

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

---

**Deep Security Agents:** Once the Deep Security Manager is installed, use it to import the Deep Security Agent software packages for the platform you are going to protect.

---

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

---

To import the Deep Security Agent software, see [Installing the Deep Security Agent \(page 27\)](#) and [Installing and Configuring a Relay-enabled Agent \(page 35\)](#).

Other "supporting" packages (such as linux kernel support updates) are available for download as well, but these are imported to Deep Security automatically as required if you have already downloaded the Agent software. For instructions on importing Agent software, see **Installing the Deep Security Agent**.

## License (Activation Codes)

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

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

## Administrator/Root

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

## SMTP Server

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

## Available Ports

### On the Deep Security Manager Host

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 DSV (configurable).

- **Port 1521:** Bi-directional Oracle Database server port.
- **Ports 1433 and 1434:** Bi-directional Microsoft SQL Server Database ports.
- **Ports 389, 636, and 3268:** Connection to an LDAP Server for Active Directory integration (configurable).
- **Port 25:** Communication to a SMTP Server to send email alerts (configurable).
- **Port 53:** For DNS Lookup.
- **Port 514:** Bi-directional communication with a Syslog server (configurable).
- **Port 443:** Communication with VMware vCloud, vCenter, vShield/NSX Manager, and Amazon AWS.

---

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

---

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

You must make sure the following ports on computers running Relay-enabled Agents are open and not reserved for other purposes:

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

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

## Network Communication

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

---

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

---

## Reliable Time Stamps

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

## Performance Recommendations

See [Deep Security Manager Performance Features \(page 67\)](#).

## Deep Security Manager and Database Hardware

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

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

For more information, see [Database Deployment Considerations \(page 17\)](#).

## Dedicated Servers

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

## High Availability Environments

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

---

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

---

**Note:** *If a virtual machine is vMotioned by DRS from an ESXi protected by a DSVA to an ESXi that is not protected by a DSVA, the virtual machine will become unprotected. If the virtual machine is subsequently vMotioned back to the original ESXi, it will not automatically be protected again unless you have created an Event-based Task to activate and protect computers that have been vMotioned to an ESXi with an available DSVA. For more information, see the **Event-Based Tasks** sections of the online help or the Administrator's Guide.*

---

# Database Deployment Considerations

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

## Version

Deep Security requires Microsoft SQL Server 2012 or 2008, or Oracle Database 11g or 10g for enterprise deployments. Deep Security Manager comes with an embedded Apache Derby database but this is only suitable for evaluation purposes. (You cannot upgrade from Apache Derby to SQL Server or Oracle Database.)

## Install before Deep Security

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

## Location

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

## Dedicated Server

The database should be installed on a separate dedicated machine.

## Microsoft SQL Server

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

## Oracle Database

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

## Transport Protocol

The recommended transport protocol is **TCP**.

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

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

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

## Connection Settings Used During Deep Security Manager Installation.

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

The installation supports both SQL and Windows Authentication. When using Windows Authentication, click on the "Advanced" button to display additional options. The screenshot above shows an example for connecting to a named SQL instance using Windows Authentication

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

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

## Keep the database Name Short (SQL Server)

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

## Oracle RAC Support

Deep Security supports:

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

---

**Note:** *Applying the default Linux Server Deep Security Policy to the Oracle RAC nodes should not cause any communication issues with Oracle Automated Storage Management (ASM) and cluster services. However if you experience issues, try customizing the Firewall settings according to the port requirements found in Oracle RAC documentation, or disabling the Firewall altogether.*

[http://docs.oracle.com/cd/E11882\\_01/install.112/e41962/ports.htm#BABECFJF](http://docs.oracle.com/cd/E11882_01/install.112/e41962/ports.htm#BABECFJF)

---

## High Availability

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

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

# Installation

# Installing the Deep Security Manager

## Before You Begin

### Database

Before you install Deep Security Manager, you must install database software, create a database and user account for Deep Security Manager to use. For information on installing a database, see [Database Deployment Considerations \(page 17\)](#).

### Co-Located Relay-enabled Agent

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

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

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

---

**Note:** Depending on your environment, additional Relay-enabled Agents can be installed at a later time. (For instructions on installing a Relay-enabled Agent, see [Installing the Deep Security Agent \(page 27\)](#) and [Configuring a Relay \(page 35\)](#).)

---

### Proxy Server Information

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

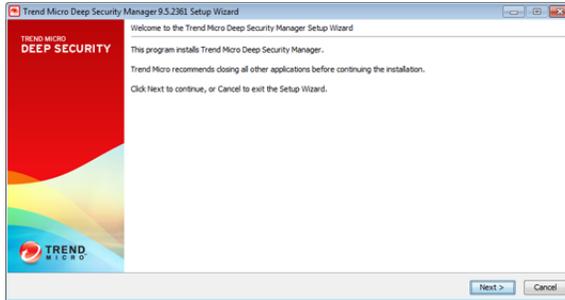
## Download the the Installer Package

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

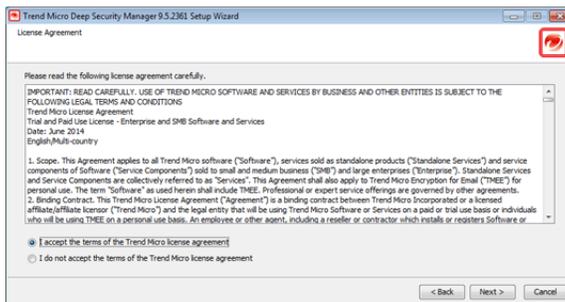
<http://downloadcenter.trendmicro.com/>

## Install the Deep Security Manager for Windows

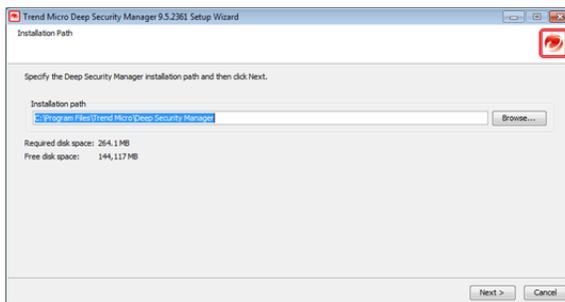
1. Copy the Deep Security Manager installer package to the target machine. Start the Deep Security Manager installer by double-clicking the install package.



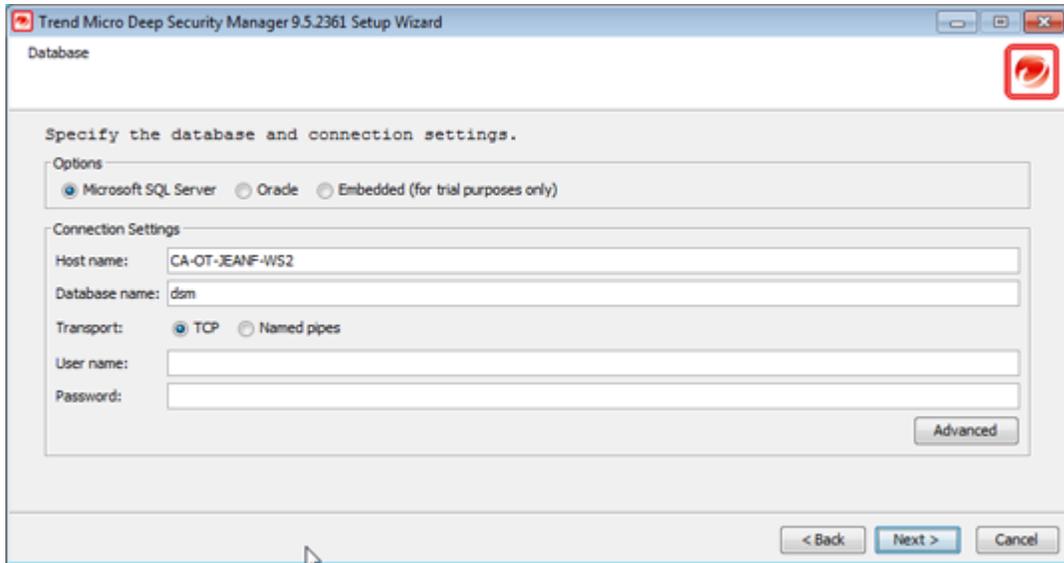
2. **License Agreement:** If you agree to the terms of the license agreement, select **I accept the terms of the Trend Micro license agreement**.



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



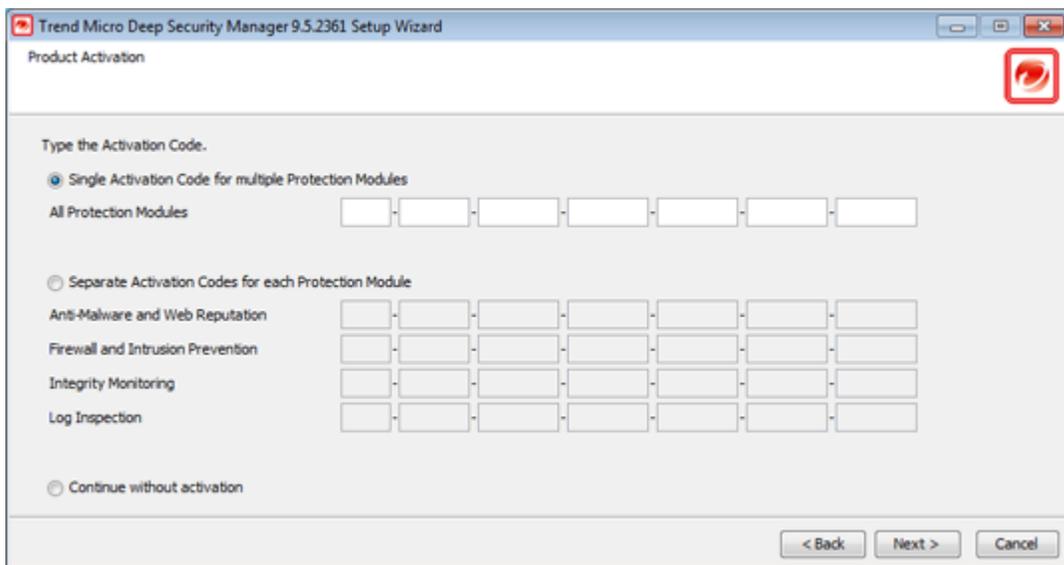
4. **Database:** Select the database you installed previously.



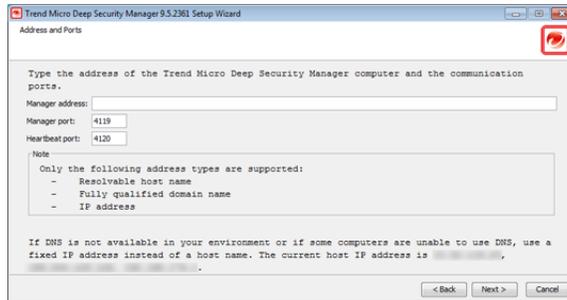
If your database is SQL Server and you are using a named instance, click **Advanced** to enter the specifics.



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



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

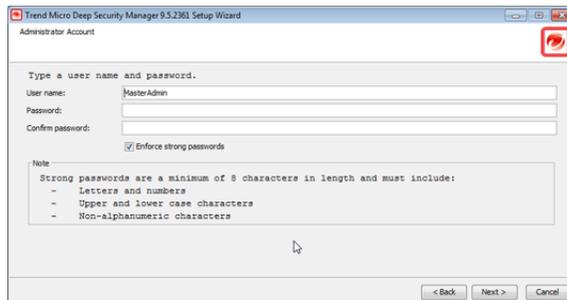


7. **Administrator Account:** Enter a username and password for the Master Administrator account. Selecting the Enforce strong passwords (recommended) requires this and future administrator passwords to include upper and lower-case letters, non-alphanumeric characters, and numbers, and to require a minimum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

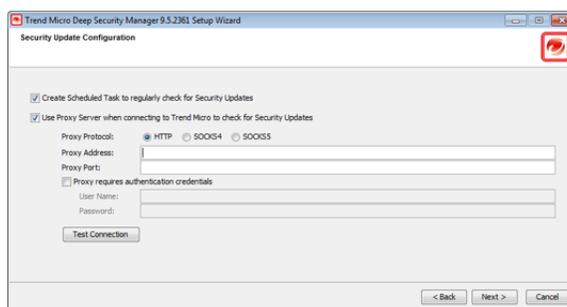
---

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

---



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

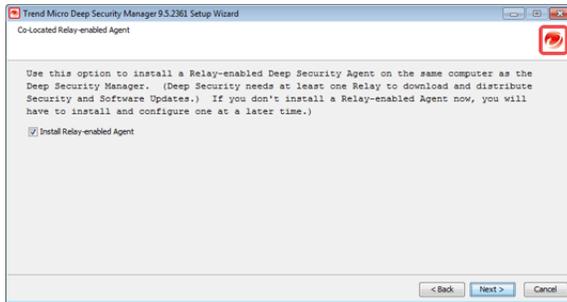


9. **Co-Located Relay-enabled Agent:** If an Agent install package is available either in the local folder or from the Trend Micro Download Center, you will be given the option to install a co-located Relay-enabled Agent. Any Deep Security installation requires at least one Relay to download and distribute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

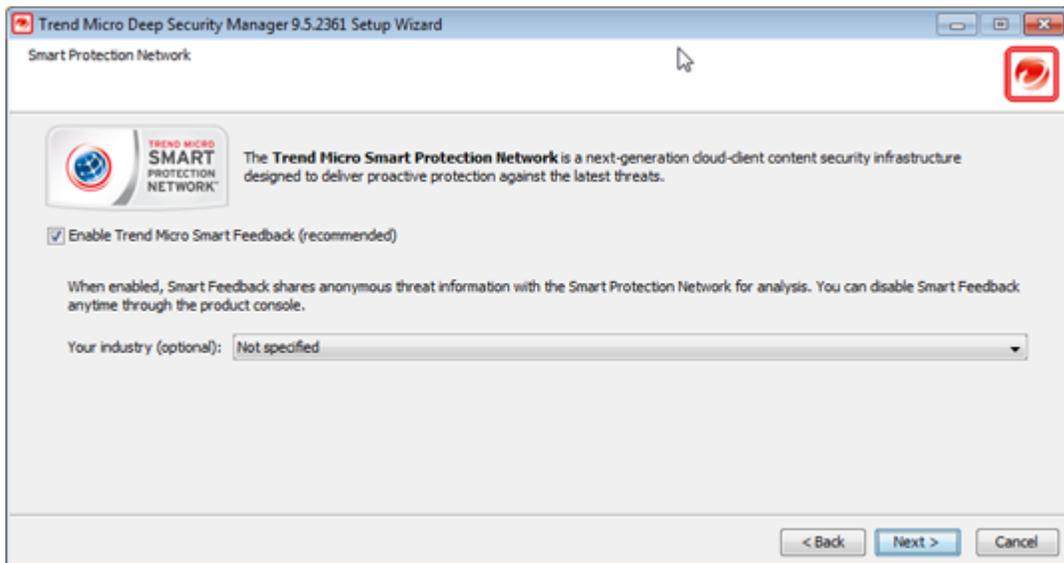
---

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

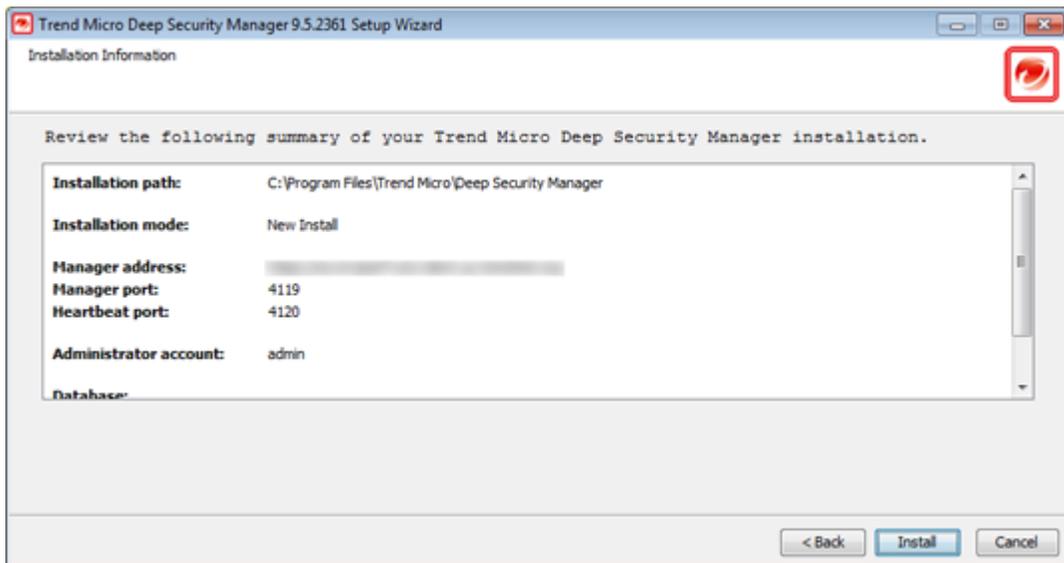
---



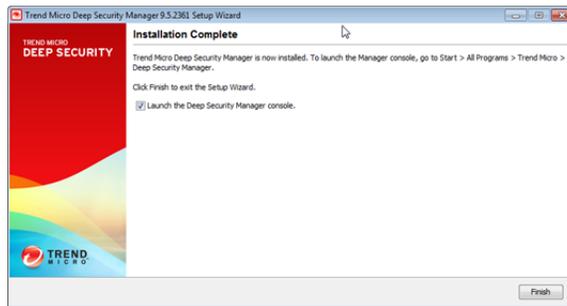
10. **Smart Protection Network:** Select whether you want to enable Trend Micro Smart Feedback (recommended). (You can enable or configure Smart Feedback later using the Deep Security Manager). Optionally enter your industry by selecting from the drop-down list.



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



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



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

## Installing the Deep Security Manager for Linux

The sequence of steps for installing Deep Security Manager on a Linux OS with X Window System are the same as those described for Windows (above). For information on performing a silent Linux installation, see [Silent Install of Deep Security Manager \(page 60\)](#).

---

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

---

## Starting Deep Security Manager

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

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

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

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

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

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

---

**Note:** *The Deep Security Manager creates a 10-year self-signed certificate for the connections with Agents/Appliances, Relays, and Users' web browsers. However, for added security, this certificate can be replaced with a certificate from a trusted certificate authority (CA). (Such certificates are maintained after a Deep Security Manager upgrade.) For information on using a certificate from a CA, see [Creating an SSL Authentication Certificate \(page 69\)](#).*

---

## Manually Importing Additional Deep Security Software

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

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

1. Download the software from the Trend Micro Download Center web site to a local directory.
2. In the Deep Security Manager, go to **Administration > Updates > Software > Local** and click **Import...** in the toolbar to display the **Import Software** wizard.
3. Use the **Browse...** option to navigate to and select your downloaded software.
4. Click **Next** and then **Finish** to exit the wizard.

The software is now imported into the Deep Security Manager.

# Installing the Deep Security Agent

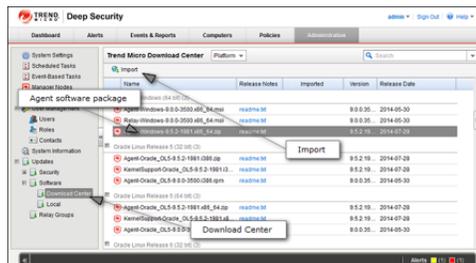
This section describes how to install and activate Deep Security Agents and how to enable Relay functionality (if required).

## Importing Agent Software

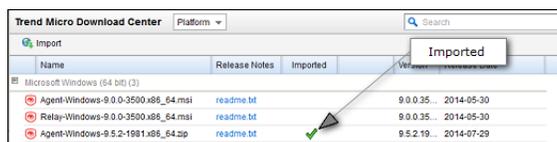
A Deep Security Agent is initially installed with core functionality only. It is only when a Protection Module is enabled on an Agent that the plug-ins required for that module are downloaded and installed. *For this reason, Agent software packages must be imported into Deep Security Manager before you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

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

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



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



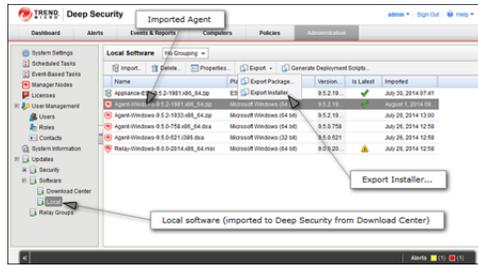
### To export the Agent installer:

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

---

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

---



3. Save the Agent installer to a local folder.

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

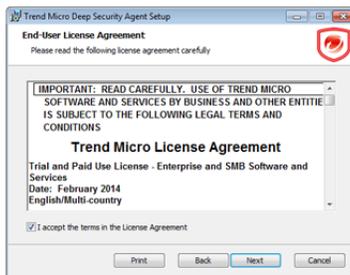
The Deep Security Agent "zip" files are made available on the Trend Micro Download Center for users who need to manually import the Agents into their Deep Security environment because their Deep Security Manager is air-gapped and cannot connect directly to the Download Center web site. Users whose Deep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

## Installing the Windows Agent

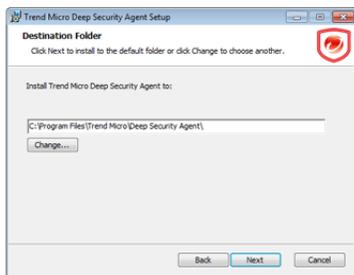
1. Copy the Agent installer file to the target machine and double-click the installation file to run the installer package. At the Welcome screen, click **Next** to begin the installation.



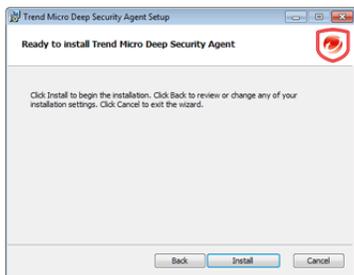
2. **End-User License Agreement:** If you agree to the terms of the license agreement, select **I accept the terms of the license agreement** and click **Next**.



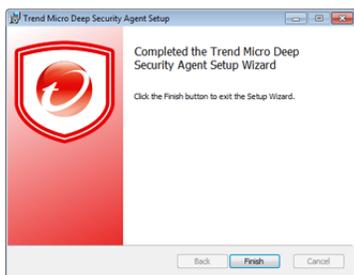
3. **Destination Folder:** Select the location where you would like Deep Security Agent to be installed and click **Next**.



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



5. **Completed:** when the installation has completed successfully, click **Finish**.



The Deep Security Agent is now installed and running on this computer, and will start every time the machine boots.

---

**Note:** *During an install, network interfaces will be suspended for a few seconds before being restored. If you are using DHCP, a new request will be generated, potentially resulting in a new IP address for the restored connection.*

---

**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 Red Hat, SuSE, or Oracle Linux Agent

---

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

---

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

---

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

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

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

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

## Installing the Ubuntu Agent

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

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

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

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

Command-line options:

To start the Agent:

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

To stop the Agent:

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

To reset the Agent:

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

To restart the Agent:

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

## Using Deployment Scripts to Install Agents

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

**To generate a deployment script:**

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

---

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

---

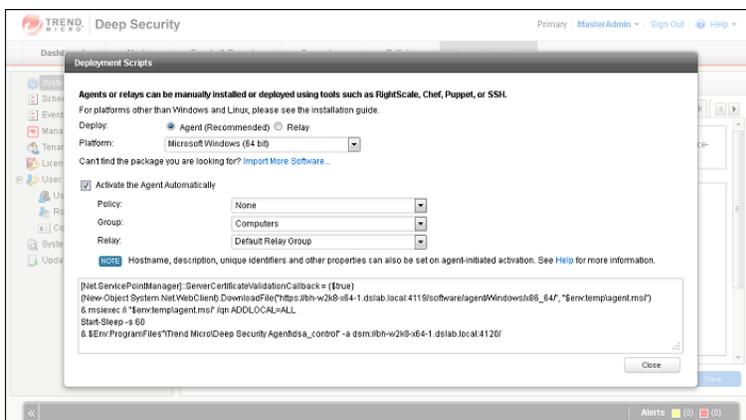
3. Select **Activate the Agent Automatically**. (Optional, but Agents must be activated by the Deep Security Manager before a protection Policy can be implemented.)
4. Select the Policy you wish to implement on the computer (optional)
5. Select the computer Group (optional)
6. Select the Relay Group

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

---

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

---




---

**Note:** *The deployment scripts generated by Deep Security Manager for Windows Agents must be run in Windows Powershell version 2.0 or later. You must run Powershell as an Administrator and you may have to run the following command to be able to run scripts:*

```
Set-ExecutionPolicy RemoteSigned
```

---

**Note:** *On windows machines, the deployment script will use the same proxy settings as the local operating system. If the local operating system is configured to use a proxy and the Deep Security Manager is accessible only through a direct connection, the deployment script will fail.*

---

## Iptables on Linux

Iptables on linux are supported and remains enabled with 9.5 only. If you have an older agent you must proceed as described below:

To run the Deep Security Agent without affecting iptables, create the following empty file:

```
/etc/use_dsa_with_iptables
```

If the Deep Security Agent detects the presence of the file, iptables will not be affected when the `ds_filter` service starts.

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

in:

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

after

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

add the line:

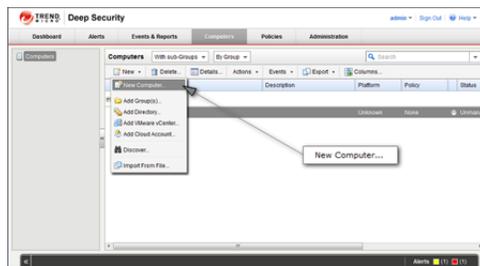
```
# Required-Stop:
```

## Activating the Agent

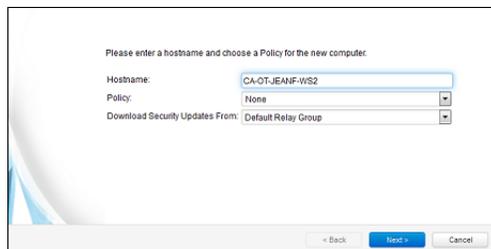
The Agent must be activated from the Deep Security Manager before it can be configured to act as a Relay or to protect the host computer.

**To activate the newly installed Agent:**

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



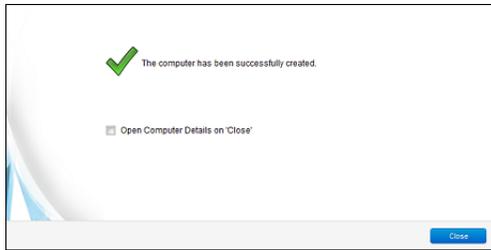
2. Enter the hostname or IP address of the computer. If you want to use the Agent to provide protection for the host computer as well as function as a Relay, select a Deep Security Policy from the **Policy** menu. Otherwise leave **Policy** set to "None".



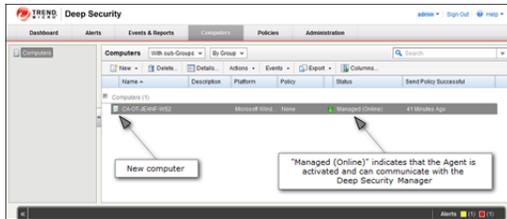
3. The wizard will confirm that it will activate the Agent on the computer and apply a Security Policy (if one was selected).



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



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



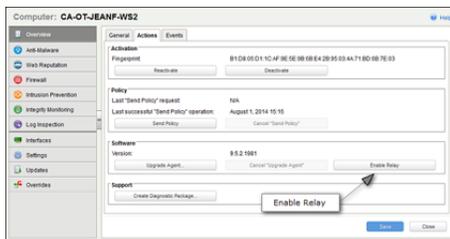
## Enabling Relay Functionality

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

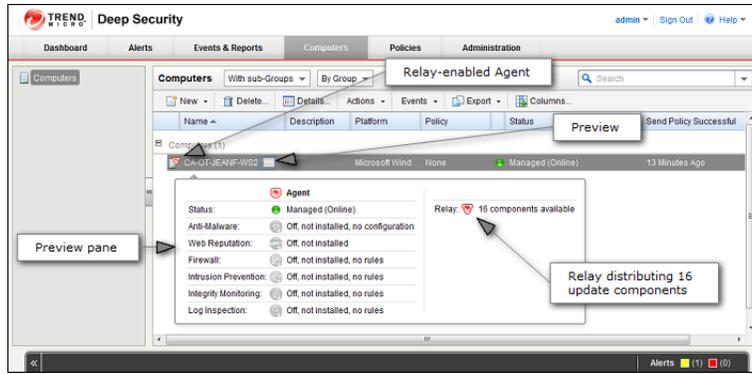
**Note:** Once enabled on an Agent, Relay functionality cannot be disabled.

### To enable Relay functionality:

- In the Deep Security Manager, go to the **Computers** page, double-click the computer with the newly-activated Agent to display its **Details** editor window.
- In the computer editor, go to the **Overview > Actions > Software** area and click **Enable Relay**. Click **Close** close the editor window.



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



# Installing and Configuring a Relay-enabled Agent

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

## Install and Activate a Deep Security Agent

If you do not already have an agent installed on a computer, do so by following the instructions in [Installing the Deep Security Agent \(page 27\)](#). You skip ahead to the section on "Manual Installation".

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

### To Activate the Agent,

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

## Enable Relay Functionality on a Deep Security Agent

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

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

---

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

---

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

---

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

---

---

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

---

# Database Deployment Considerations

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

## Version

Deep Security requires Microsoft SQL Server 2012 or 2008, or Oracle Database 11g or 10g for enterprise deployments. Deep Security Manager comes with an embedded Apache Derby database but this is only suitable for evaluation purposes. (You cannot upgrade from Apache Derby to SQL Server or Oracle Database.)

## Install before Deep Security

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

## Location

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

## Dedicated Server

The database should be installed on a separate dedicated machine.

## Microsoft SQL Server

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

## Oracle Database

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

## Transport Protocol

The recommended transport protocol is **TCP**.

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

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

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

## Connection Settings Used During Deep Security Manager Installation.

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

The installation supports both SQL and Windows Authentication. When using Windows Authentication, click on the "Advanced" button to display additional options. The screenshot above shows an example for connecting to a named SQL instance using Windows Authentication

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

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

## Keep the database Name Short (SQL Server)

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

## Oracle RAC Support

Deep Security supports:

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

---

**Note:** *Applying the default Linux Server Deep Security Policy to the Oracle RAC nodes should not cause any communication issues with Oracle Automated Storage Management (ASM) and cluster services. However if you experience issues, try customizing the Firewall settings according to the port requirements found in Oracle RAC documentation, or disabling the Firewall altogether.*

[http://docs.oracle.com/cd/E11882\\_01/install.112/e41962/ports.htm#BABECFJF](http://docs.oracle.com/cd/E11882_01/install.112/e41962/ports.htm#BABECFJF)

---

## High Availability

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

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

# Upgrading

# Upgrading a Basic Agent-based Installation

The steps for upgrading a basic Agent-based Deep Security 9.0 installation to Deep Security 9.5 are:

1. Upgrade your Deep Security Manager to version 9.5
2. Install at least one Deep Security 9.5 Agent with Relay functionality enabled.
3. Upgrade your Deep Security Agents and Relays to 9.5 (as required)

---

**Note:** *The upgrade process does not delete or overwrite any data but backing up your system before an upgrade is always a good idea. **To back up your 9.0 Deep Security data**, see "Database Backup and Recovery" in the your Deep Security 9.0 online help or Administrator's Guide.*

---

## Upgrade your 9.0 Deep Security Manager to version 9.5

**To upgrade Deep Security Manager 9.0 to Deep Security Manager 9.5:**

1. Download the Deep Security Manager 9.5 install package from the Trend Micro Download Center web site (<http://downloadcenter.trendmicro.com/>) to a local directory.
2. Run the installer package following the steps as for a new installation, described in [Installing Deep Security Manager \(page 20\)](#) except when given the option choose **Upgrade** instead of **Overwrite**.

## Upgrading vs. Overwriting an Existing Installation

When the Deep Security Manager installer detects the 9.0 version of Deep Security Manager on your system, it will give you the option to "upgrade the existing installation", or to "overwrite the existing installation". Upgrading the installation will upgrade the Deep Security Manager to the latest version but will not overwrite your Security Profiles, IPS Rules, Firewall Rules, Application Types, etc. or change any of the security settings that were 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.

## Deploy a Deep Security 9.5 Relay-enabled Agent

In Deep Security 9.0, the Deep Security Relay was a distinct piece of Deep Security software that provided the Security and Software Update distributions in that version. In Deep Security 9.5, the Relay functionality has been included as a module in every 64-bit Windows and Linux Agent.

Deep Security Manager 9.5 still supports 9.0 Relays, however:

- 9.5 Agents cannot be updated by 9.0 Relays (and therefore a 9.5 Relay-enabled Agent is required)
- 9.0 Relays and 9.5 Relay-enabled Agents cannot be in the same Relay Group

The recommended procedure is to replace your Deep Security 9.0 Relays with 9.5 Relay-enabled Agents. Windows Relays can be upgraded from the Deep Security Manager. Linux Relays must be manually uninstalled and replaced with a fresh install of a 9.5 Linux Agent.

**To perform a fresh install of a 9.5 Deep Security Agent and enable it as a Relay**, see [Installing the Deep Security Agent \(page 27\)](#).

---

**Note:** *If you want to test the functionality of the 9.5 Relay-enabled Agent before replacing all your 9.0 Relays you can install a single 9.5 Relay-enabled Agent, place it in its own Relay Group (because 9.0 Relays cannot be with 9.5 Relay-enabled Agents in the same Relay Group) , and assign a few VMs to the new Relay Group.*

---

## Upgrade existing Deep Security Agents and Relays

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

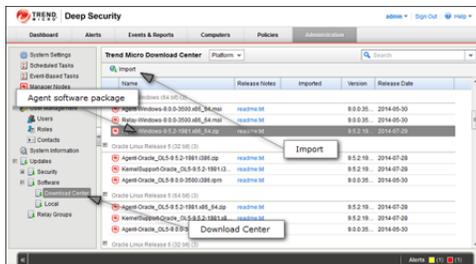
**Note:** *When planning the upgrade of your Agents and Relays from 9.0 to 9.5, ensure that your 9.5 Agents are assigned to Relay Groups that contain only 9.5 Relays. You should upgrade all Relays in a Group to 9.5 (or create a new 9.5 Group) before configuring any 9.5 Agents to receive updates from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

Deep Security 9.0 Agents can be upgraded using the Deep Security Manager interface (or by manual local upgrade), but the Agent software must first be imported into the Deep Security Manager.

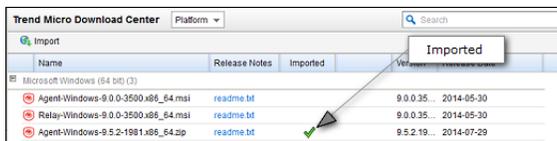
Deep Security 9.0 Windows Relays can be upgraded to 9.5 Relay-enabled Agents using the Deep Security Manager interface (or by manual local upgrade). Deep Security 9.0 Linux Relays cannot be upgraded. They must be uninstalled and replaced with a fresh install of a 9.5 Linux Agent. (See Upgrade a Relay on Linux, below, for instructions.)

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

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



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



### To Upgrade Deep Security Agents and Windows Deep Security Relays using the Deep Security Manager:

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

**Note:** *You can manually upgrade the any Agents or Relays locally on a computer. To do this, follow the instructions in [Installing the Deep Security Agent \(page 27\)](#).*

## Protection Module State after Upgrade

Changes to the 9.5 Deep Security Windows and Linux Agents since version 9.0 mean that, depending on the platform, not all Protection Modules that were enabled on a 9.0 Agent will remain enabled on a 9.5 Agent after upgrading. The following table shows which Modules are affected by an Upgrade:

Feature	Windows	Linux
AM	No change	Uninstalled
IM	Uninstalled	Uninstalled
WRS/FW/IPS	Uninstalled	Uninstalled
LI	Uninstalled	Uninstalled

## Upgrade a Relay on Linux

You cannot use the command on the **Actions** menu to update a Relay from 9.0 SP1 to 9.5 on Linux.

### To upgrade a 9.0 Relay to 9.5 on Linux:

1. Upgrade Deep Security Manager to version 9.5.
2. Import `Agent-platform-9.5.build.zip` into Deep Security Manager.
3. Deactivate the Relay that you want to upgrade and then uninstall it.
4. Install `Agent-Core-platform-9.5.build.rpm` on the Agent computer.
5. Enable the Relay.

### To convert a 9.0 Relay to a 9.5 Agent on Linux:

1. Upgrade Deep Security Manager to version 9.5.
2. Import `Agent-platform-9.5.build.zip` into Deep Security Manager.
3. Deactivate the Relay that you want to upgrade.
4. Delete the Relay from Deep Security Manager.
5. Uninstall the Relay.
6. Install `Agent-Core-platform-9.5.build.rpm` on the Agent computer.
7. In Deep Security Manager, add the computer (**Computers > New > New Computer**).

# Quick Start

# Quick Start: System Configuration

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

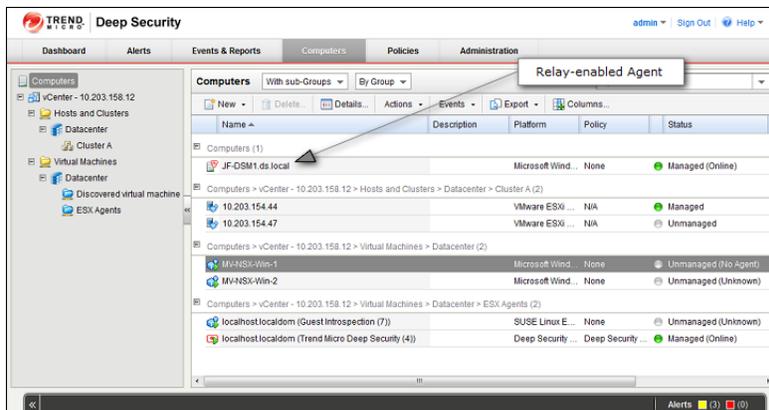
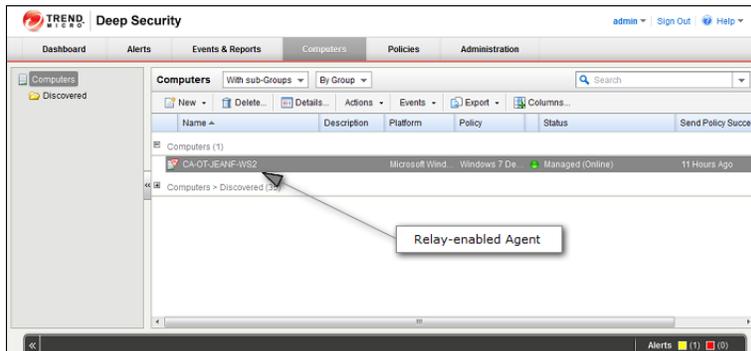
To complete basic Deep Security system configuration, you will need to:

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

## Make sure your Relay-enabled Agent is operational

**Note:** *The Relay is responsible for retrieving Security Updates from Trend Micro and distributing them to your protected computers. If you did not install a co-located Relay-enabled Agent during the installation of the Deep Security Manager, you need to install a Relay-enabled Agent before proceeding. (See [Installing and Configuring a Relay-enabled Agent \(page 35\)](#).)*

Start the Deep Security Manager management console and navigate to the **Computers** page. Your Relay-enabled Agent should appear on the **Computers** list identified by a "computer" icon with a Relay badge on it (  ). It's status column should display "Managed (Online)".



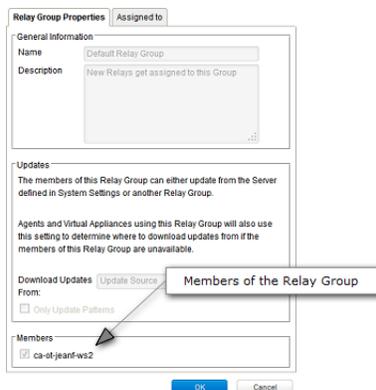
Relays are always organized into Relay Groups, even if it's only the one "Default Relay Group" to which all new Relays are assigned. You can create multiple Relay Groups if you have a large number of computers and want to create a hierarchical Relay structure or if your computers are spread out over large geographical areas. For more information on Relay Groups, see **Relay Groups** in the online help.

To view your Deep Security Relays, go to the **Administration > Updates > Relay Groups**.



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

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



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

---

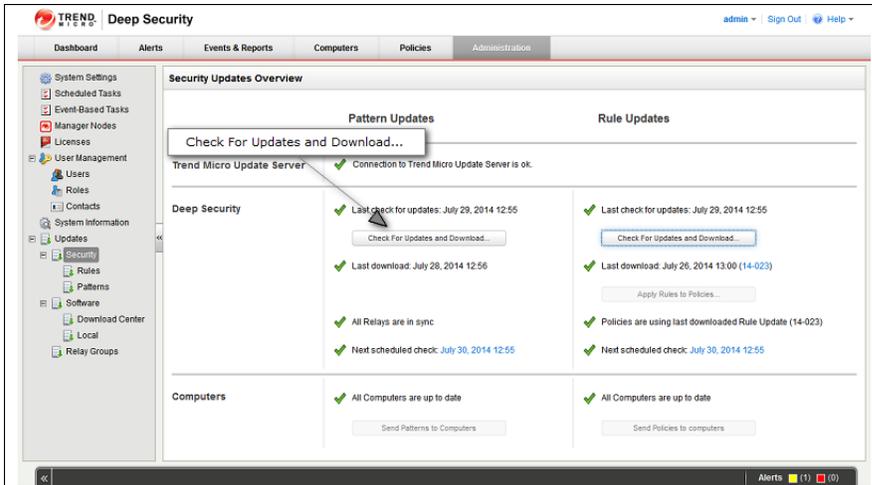
**Note:** *If there are no computers in the Members area see **Configuring the Deep Security Relay** in the Installation Guide.*

---

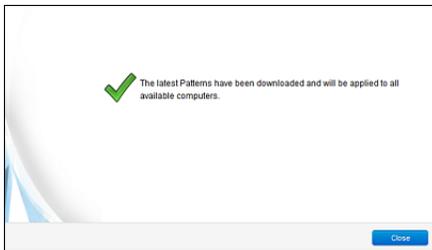
## Configure Deep Security's ability to retrieve Updates from Trend Micro

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

Go to the **Administration > Updates > Security** page and click the **Check For Updates and Download...** button under **Pattern Updates**.



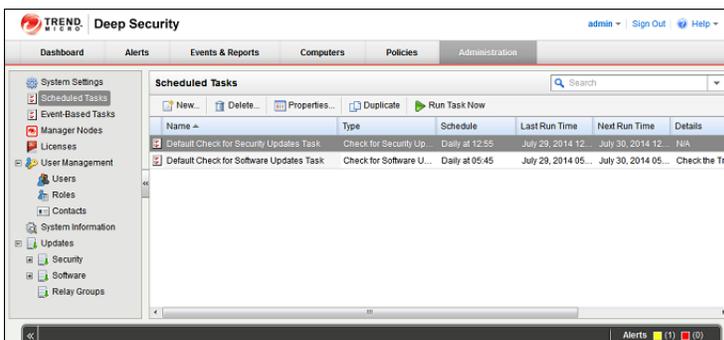
This will display the **Download Patterns** Wizard which contacts the Trend Micro Update Servers and downloads the latest Anti-Malware Pattern Updates and distributes them to your computers. (This is the default behavior. You can configure the automatic distribution of Security Updates on the **Administration > System Settings > Updates** tab.) If upon completion the wizard displays the success message it means your Relay-enabled Agent can communicate with the Update servers:



## Check that you have a Scheduled Task to perform regular Updates

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

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



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

The screenshot shows a 'Task Details' dialog box with two main sections: 'General Information' and 'Schedule Information'. In 'General Information', the 'Name' is 'Default Check for Security Updates Task' and the 'Type' is 'Check for Security Updates'. In 'Schedule Information', the frequency is set to 'Daily', the 'Start date' is 'July 26, 2014', and the 'Start time' is '12:55'. Under 'Daily Schedule Details', 'Every Day' is selected, with 'Weekdays' and 'Every 2 days' also visible but not selected. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Notice that (in this case) the **Daily Check For Security Updates Task** is set to perform a Security Update every day at 12:55.

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

## Updates Configuration in the System Settings

To configure the finer details of Update behavior, in the Deep Security Manager, go to the **Updates** tab in **Administration > System Settings**.

The screenshot shows the 'System Settings' dialog box with the 'Updates' tab selected. The 'Security Updates' section includes:
 

- Primary Security Update Source:** Trend Micro Update Server (https://aus.trendmicro.com/au\_server.dll)
- Patterns:**
  - Allow Agents/Appliances to download Pattern updates directly from Primary Security Update Source if Relays are not accessible
  - Allow Agents/Appliances to download Pattern updates when Deep Security Manager is not accessible
- Rules:**
  - Automatically apply Rule Updates to Policies
- Relays:**
  - Support 9.0 (and earlier) Agents
  - Import Patterns for all Regions
- Software Updates:**
  - Automatically download updates to imported software
- Alternate software update distribution server(s) to replace Deep Security Relays:** (Empty list with 'Add' and 'Remove' buttons)

 A note below states: "NOTE See 'Configuring a Software Update Server' in the online help for information on how to configure your own software update distribution servers."

In the **Security Updates** area you can configure the following options (although the default settings are recommended):

- **Primary Update Source:** this is the source that the Relays in all Relay Groups go to for Deep Security Rule and Pattern Updates which they can then distribute to Agents and Virtual Appliances. (Only change this if you have been instructed to do so by your support provider.)
- **Patterns:** Patterns are used by the Anti-malware Module. The default settings permits Agents and Virtual Appliances to download Pattern Updates directly from the Primary Security Update Source (above) if for some reason they cannot contact a Relay or the Deep Security Manager. (For example because of local connectivity issues, or if the computer is a roaming laptop.)

- **Rules:** Updates to the Deep Security Rules used by the Firewall, Intrusion Prevention, Log Inspection, and Integrity Monitoring Protection Modules must be integrated into Policies at the Deep Security Manager level before they can be sent out to Agents and Virtual Appliances. This setting (on by default) automatically integrates Rule Updates with the Policies in the Deep Security Manager.

---

**Note:** *In each Security Policy, there is a further setting (also on by default) to automatically update computers when there has been a change to the Security Policy that is in use. This setting is found in the Policy/Computer Editor (the **Details** window) in **Settings > Computer > Send Policy Changes Immediately**.*

---

- **Relays:** The two settings under Relays determine if Deep Security will import updates for older 9.0 and earlier versions of the Agents and Appliances. Security Update architecture has changed substantially since 9.0 and the formats of the Updates for 9.0 and 9.5 are different. Do not download Updates for older Agents if you do not them as this would consume unnecessary bandwidth and storage space. Similarly, only download Patterns for all "Regions" (determined by language) if you have Agents or Appliances running in multiple Regions. Leaving this option unchecked will distribute only the package designed for the Region in which your Deep Security Manager is installed.

In the **Software Updates** area you can configure the following options (although the default settings are recommended):

- **Trend Micro Download Center:** By default, Deep Security will "Automatically download updates to imported software." Trend Micro will periodically issue updated builds of already released Agent and Appliance software. Setting this option will automatically download updates to any software that you have already imported to Deep Security (visible on the **Administration > Updates > Software > Local** page) from the Trend Micro Download Center (the software available from the Trend Micro Download Center can be seen on the **Administration > Updates > Software > Download Center** page.)

---

**Note:** *The installation of the software once it has been downloaded must be initiated manually. This last step cannot be automated.*

---

In the **Virtual Appliance Version Control** section, you can control the versions of the Protection Modules are installed on a newly activated Virtual Appliance. The Deep Security Virtual Appliance is shipped with basic versions of the Protection Module plug-ins. The Appliance relies on the plug-ins that are shipped with the 64-bit Red hat Agent software package for Updates. By default, the Appliance will use the latest version of the Red Hat package that has been imported to Deep Security (on the **Updates > Software > Local** page.) However you may wish to control over the version of the Protection Modules get installed and you can do using this setting.

---

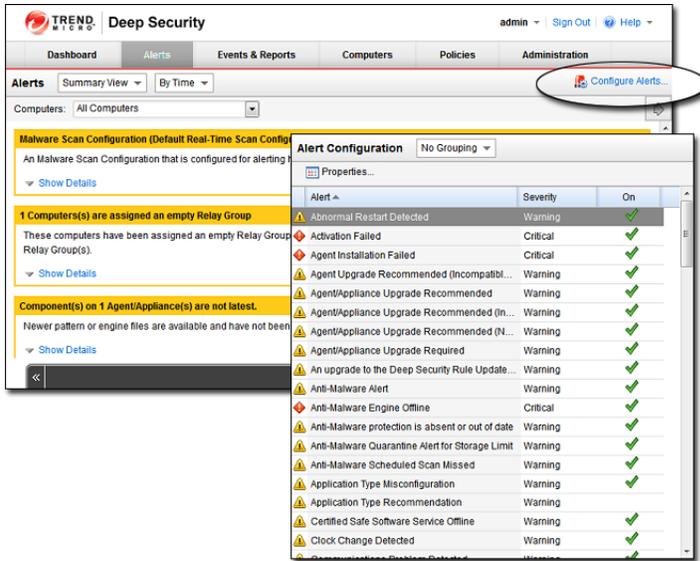
**Note:** *For more information about the configuration options available on this page, see the associated online help for it in the Deep Security Manager.*

---

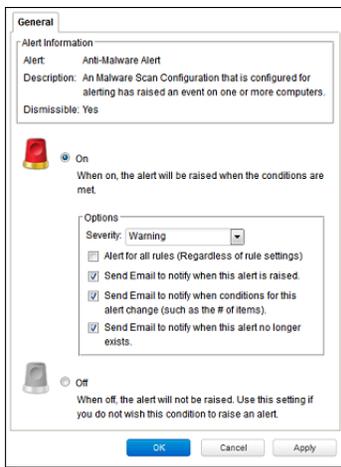
## Set up email notification of important events

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

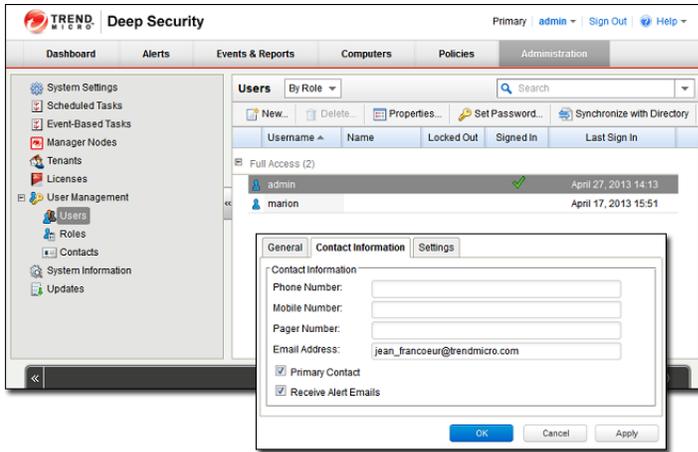
To configure which Alerts will generate an email notification, go to the **Alerts** page and click **Configure Alerts...** to display the list of Deep Security Alerts:



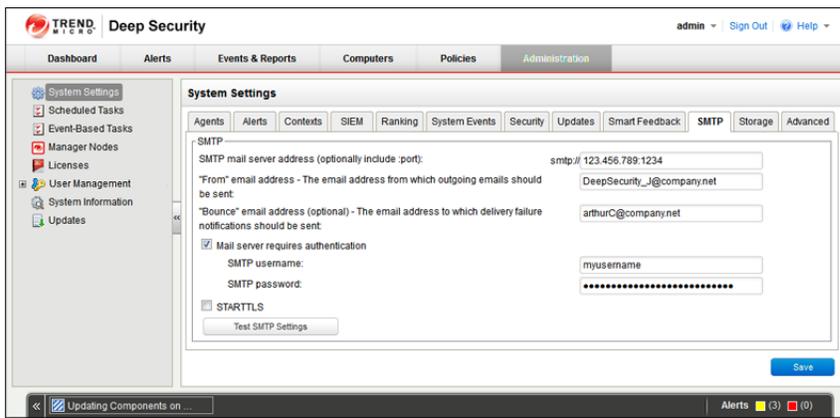
Double-click on an Alert see its **Properties** window where you can you can set the Alert options for email notification:



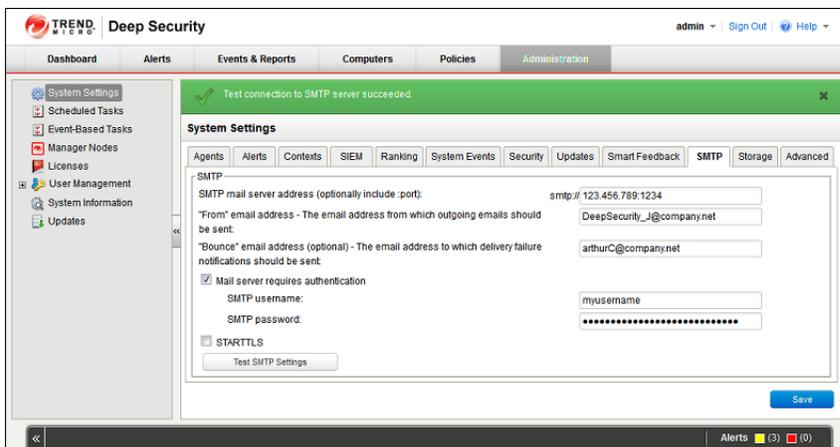
Now you need to configure your User account to receive the email notifications Deep Security will send out. Go to **Administration > User Management > Users** and double-click on your User account to display its **Properties** window. Go to the **Contact Information** tab and enter an email address and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



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



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



---

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

---

## Basic Configuration is complete

This completes the basic Deep Security system configuration. Deep Security is now configured to regularly contact Trend Micro for security Updates and distribute those Updates on regular basis, and it will send you email notifications when Alerts are raised. Now you need to apply Deep Security protection to your computers. For more information on protecting computer resources, see [QuickStart: Protecting a Computer \(page 51\)](#).

## Quick Start: Protecting a Computer

The following describes how to use Deep Security to protect a Windows Server 2008 computer.

It will involve the following steps:

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

---

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

---

## Adding the computer to the Deep Security Manager

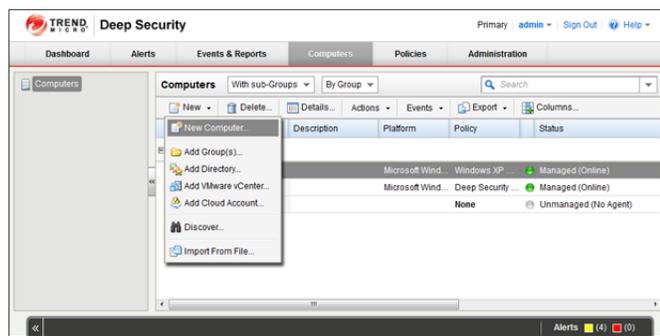
There are several ways of adding computers to the Deep Security Manager's **Computers** page. You can add computers by:

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

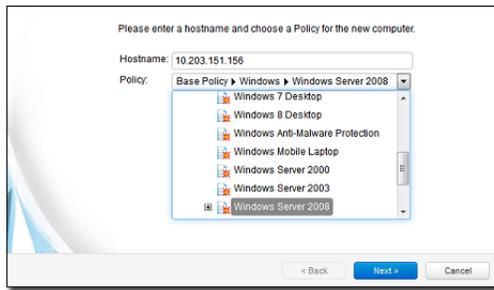
For the purposes of this exercise, we will add a computer from a local network but once a computer is added to the Manager, the protection procedures are the same regardless of where the computer is located.

**To add a computer from a local network:**

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



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



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

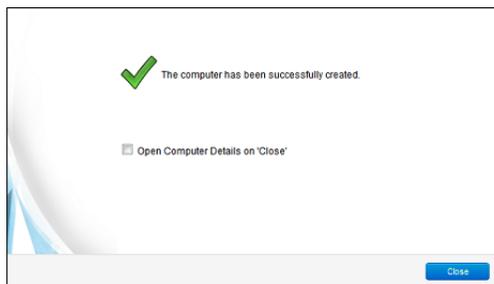



---

**Note:** An Agent can be configured to automatically initiate its own activation upon installation. For details, see **Command-Line Utilities** in the Reference section of the online help.

---

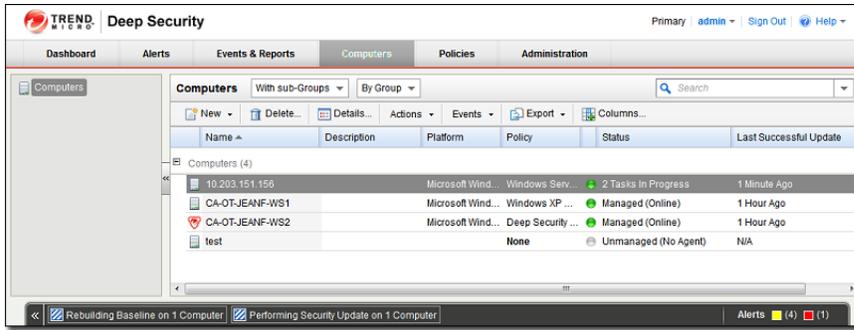
4. When the computer has been added the wizard will display a confirmation message:



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

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

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



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

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

## Configuring and Running a Recommendation Scan

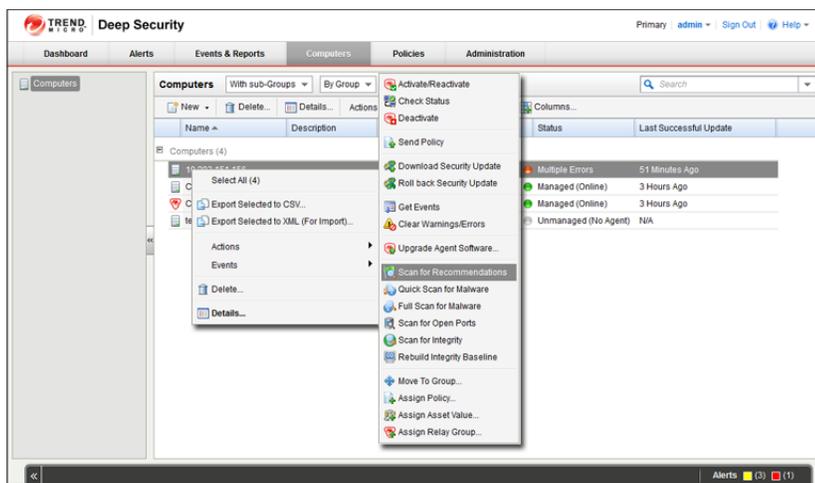
The security Policy that we assigned to the computer is made up of a collection of Rules and settings designed for a computer running the Windows Server 2008 operating system. However, a static Policy can soon fall out of date. This can be because of new software being installed on the computer, new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

Recommendation Scans make recommendations for the following protection modules:

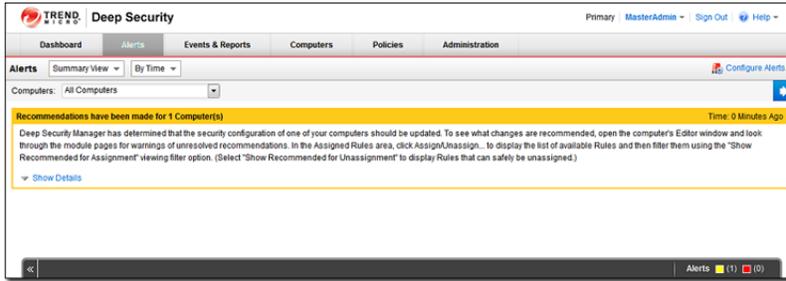
- **Intrusion Prevention**
- **Integrity Monitoring**
- **Log Inspection**

**To run a Recommendation Scan on your computer:**

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



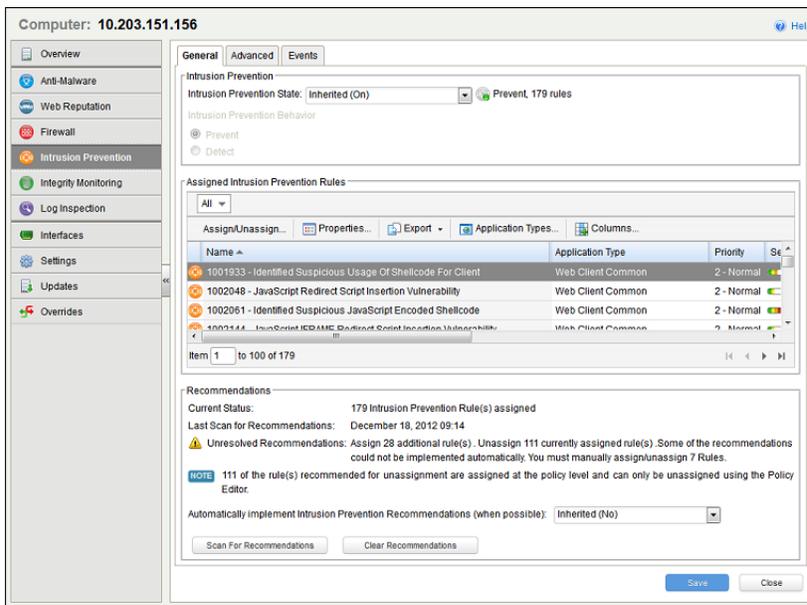
During the Recommendation Scan, your computer's Status will display **Scanning for Recommendations**. When the scan is finished, if Deep Security has any recommendations to make, you will see an Alert on the Alerts screen:



**To see the results of the Recommendation Scan:**

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

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



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

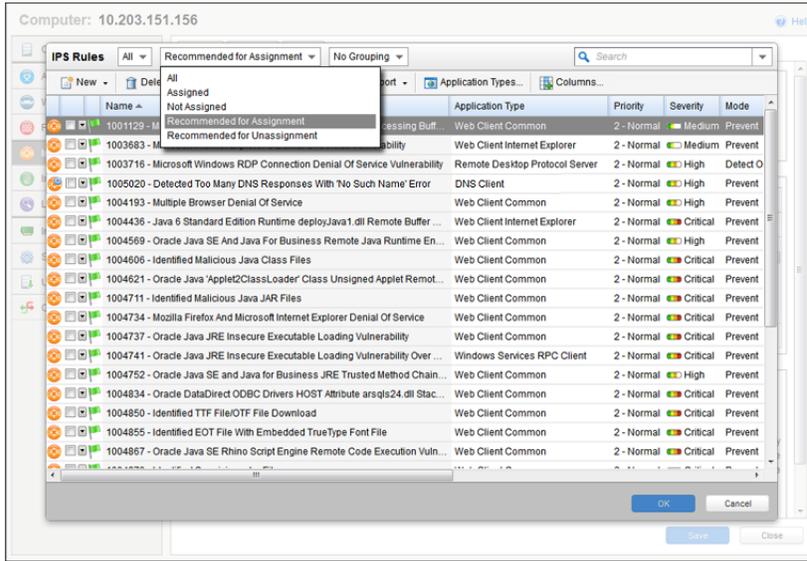
**Last Scan for Recommendations** tells us that the last scan took place on December 18th, 2012, at 09:14.

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

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

We are also told that 7 of the Rules that are recommended for assignment can't be automatically assigned. Usually these are either Rules that require configuration or Rules that are prone to false positives and whose behavior should be observed in detect-only mode being being

enforced in prevent mode. To see which Rules have been recommended for assignment, click **Assign/Unassign...** to display the **IPS Rules** rule assignment modal window. Then select Recommended for Assignment from the second drop-down filter list:



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

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

---

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

---

## Automatically implement scan recommendations

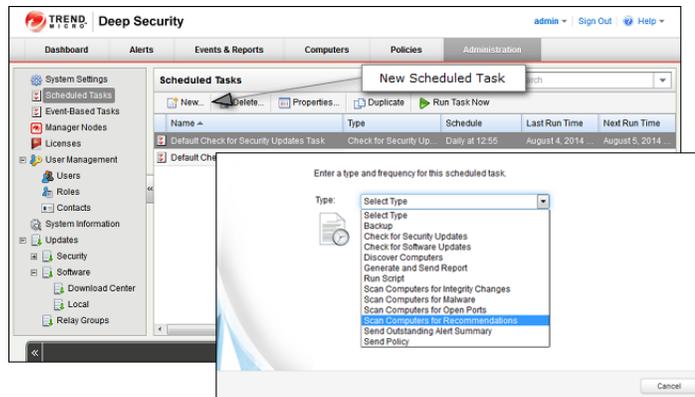
You can configure Deep Security to automatically assign and unassign Rules after a Recommendation Scan. To do so, open the computer or Policy editor and go to the individual protection module pages that support Recommendation Scans (Intrusion, Prevention, Integrity Monitoring, and Log Inspection). In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

## Create a Scheduled task to perform regular Recommendation Scans

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

### To create a Scheduled Task:

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



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

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

## Schedule Regular Security Updates

If you follow the steps described in [Quick Start: System Configuration \(page 43\)](#), your computer will now be regularly updated with the latest protection from Trend Micro.

## Monitor Activity Using the Deep Security Manager

### The Dashboard

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

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

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

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

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

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

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

---

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

---

## Logs of Firewall and Intrusion Prevention Events

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

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

---

**Note:** For the meaning of the different packet rejection reasons, see **Firewall Events** and **Intrusion Prevention Events** in the Reference section of the online help.

---

## Reports

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

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

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

# Appendices

# Deep Security Manager Memory Usage

## Configuring the Installer's Maximum Memory Usage

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

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

1. Go to the directory where the installer is located.
2. Create a new text file called "Manager-Windows-9.5.xxxx.x64.vmoptions" or "Manager-Linux-9.5.xxxx.x64.vmoptions", depending on your installation platform (where "xxx" is the build number of the installer).
3. Edit the file by adding the line: "-Xmx800m" (in this example, 800MB of memory will be made available to the installer.)
4. Save the file and launch the installer.

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

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

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

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

# Silent Install of Deep Security Manager

## Windows

### To initiate a silent install on Windows:

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

## Linux

### To initiate a silent install on Linux:

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

## Parameters

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

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

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

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

The **<PropertiesFile>** argument is the complete/absolute path to a standard Java properties file. Each property is identified by its equivalent GUI screen and setting in the Windows Deep Security Manager installation (described above). For example, the Deep Security Manager address on the "Address and Ports" screen is specified as:

```
AddressAndPortsScreen.ManagerAddress=
```

Most of the properties in this file have acceptable defaults and may be omitted. The only required values for a simple installation using an embedded database are:

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

For a complete description of available settings, see [Deep Security Manager Settings Properties File \(page 62\)](#).

## Sample Properties File

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

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

```
DatabaseScreen.DatabaseName=XE
DatabaseScreen.Username=DSM
DatabaseScreen.Password=xxxxxxx
AddressAndPortsScreen.ManagerPort=4119
AddressAndPortsScreen.HeartbeatPort=4120
CredentialsScreen.Administrator.Username=masteradmin
CredentialsScreen.Administrator.Password=xxxxxxx
CredentialsScreen.UseStrongPasswords=False
SecurityUpdateScreen.UpdateComponents=True
SecurityUpdateScreen.UpdateSoftware=True
RelayScreen.Install=True
SmartProtectionNetworkScreen.EnableFeedback=False
```

# 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 (silent Install) of the Deep Security Manager. (See [Silent Install of Deep Security Manager \(page 60\)](#).)

## Settings Properties File

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

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

The settings properties file has required and optional values.

---

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

---

## Required Settings

### LicenseScreen

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

OR

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

### CredentialsScreen

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

## Optional Settings

### LanguageScreen

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

## UpgradeVerificationScreen

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

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

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

## DatabaseScreen

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

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

Property	Possible Values	Default Value	Notes
DatabaseScreen.DatabaseType=<value>	Embedded Microsoft SQL Server Oracle	Microsoft SQL Server	
DatabaseScreen.Hostname=<value>	The name or IP address of the database host Current host name	Current host name	
DatabaseScreen.DatabaseName=<value>	Any string	dsm	Not required for embedded
DatabaseScreen.Transport=<value>	Named Pipes TCP	Named Pipes	Required for SQL Server only
DatabaseScreen.Username=<value>			Not required for Embedded
DatabaseScreen.Password=<value>		blank	Not required for Embedded
DatabaseScreen.SQLServer.Instance=<value>			Blank implies default instance. Optional, required for SQL Server only
DatabaseScreen.SQLServer.Domain=<value>			Optional, required for SQL Server only
DatabaseScreen.SQLServer.UseDefaultCollation=<value>	True False	False	Optional, required for SQL Server only

## AddressAndPortsScreen

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

Property	Possible Values	Default Value	Notes
AddressAndPortsScreen.ManagerAddress=<value>	<hostname, URL or IP address of the Manager host>	<current host name>	
AddressAndPortsScreen.ManagerPort=<value>	<valid port number>	4119	
AddressAndPortsScreen.HeartbeatPort=<value>	<valid port number>	4120	
AddressAndPortsScreen.NewNode=<value>	True False	False	True indicates that the current install is a new node. If the installer finds existing data in the database, it will add this installation as a new node. (Multi-node setup is always a silent install). Note: The "New Node" installation information about the existing database to be provided via the DatabaseScreen properties.

## CredentialsScreen

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

## SecurityUpdateScreen

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

## SmartProtectionNetworkScreen

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

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

## Sample Properties Files

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

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

```
DatabaseScreen.Transport=TCP
DatabaseScreen.DatabaseName=XE
DatabaseScreen.Username=DSM
DatabaseScreen.Password=xxxxxxx
AddressAndPortsScreen.ManagerPort=4119
AddressAndPortsScreen.HeartbeatPort=4120
CredentialsScreen.Administrator.Username=masteradmin
CredentialsScreen.Administrator.Password=xxxxxxx
CredentialsScreen.UseStrongPasswords=False
SecurityUpdateScreen.UpdateComponents=True
SecurityUpdateScreen.UpdateSoftware=True
RelayScreen.Install=True
SmartProtectionNetworkScreen.EnableFeedback=False
```

## Installation Output

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

### Successful Install

```
Stopping Trend Micro Deep Security Manager Service...
Detecting previous versions of Trend Micro Deep Security Manager..
Upgrade Verification Screen settings accepted...
Database Screen settings accepted...
License Screen settings accepted...
Address And Ports Screen settings accepted...
Credentials Screen settings accepted...
All settings accepted, ready to execute...
Uninstalling previous version
Stopping Services
Extracting files...
Setting Up...
Connecting to the Database...
Creating the Database Schema...
Updating the Database Data...
Creating MasterAdmin Account...
Recording Settings...
Creating Temporary Directory...
Installing Reports...
Creating Help System...
Setting Default Password Policy...
Importing Example Security Profiles...
Applying Security Update...
Assigning IPS Filters to Example Security Profiles...
Correcting the Port for the Manager Security Profile...
Correcting the Port List for the Manager...
Creating IP List to Ignore...
Creating Scheduled Tasks...
Creating Asset Importance Entries...
Creating Auditor Role...
Auditing...
Optimizing...
Recording Installation...
Creating Properties File...
Creating Shortcut...
Configuring SSL...
Configuring Service...
```

```
Configuring Java Security...  
Configuring Java Logging...  
Cleaning Up...  
Starting Deep Security Manager...  
Finishing installation...
```

## Failed Install

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

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

# Deep Security Manager Performance Features

## Performance Profiles

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

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

## Low Disk Space Alerts

### Low Disk Space on the Database Host

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

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

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

### Low Disk Space on the Manager Host

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

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

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

You must restart the Manager manually.

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

## Agentless Protection

### Scan Caching

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

In addition,

- Integrity Monitoring scan caching speeds up Integrity Monitoring scans by sharing Integrity Monitoring scan results

- Anti-Malware on-demand caching speeds up scans on subsequent cloned/similar VMs
- Anti-Malware Real-time caching speeds up VM boot and application access time
- Concurrent Scan feature allows further overall scan time improvement by allowing multiple VMs to be scanned concurrently

## 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 server. You must actively change the DRS settings for all the Virtual Appliances to "Manual" or "Disabled" (recommended) so that they will not be vMotioned by the DRS. If a Virtual Appliance (or any virtual machines) is set to "Disabled", vCenter Server does not migrate that virtual machine or provide migration recommendations for it. This is known as "pinning" the virtual machine to its registered host. This is the recommended course of action for Virtual Appliances in a DRS environment. (An alternative is to deploy the Virtual Appliance onto 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 server 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 "Event-Based Tasks" in the Deep Security Manager Help.*

---

# Creating an SSL Authentication Certificate

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

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

## To create your SSL authentication certificate:

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

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

5. Choose password: **changeit**

---

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

---

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

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

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

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

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

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

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

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

(say yes to warning message)

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

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

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

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

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

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

16. Replace the password in the following string:

```
keystorePass=xxxx
```

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

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

# Protecting a Mobile Laptop

The following describes the steps involved in using Deep Security to protect a mobile laptop. It will involve the following steps:

1. Adding Computers to the Manager
  1. Adding individual computers
  2. Performing a Discovery Operation on your network
  3. Importing computers from a Microsoft Active Directory
2. Create a new Policy for a Windows laptop
  1. Creating and naming the new Policy
  2. Setting which interfaces to monitor
  3. Setting the network engine to Inline Mode
  4. Assigning Firewall Rules (including some with Location Awareness) and enabling Firewall Stateful Configuration
  5. Assigning Intrusion Prevention Rules
  6. Assigning Log Inspection Rules
  7. Assigning Integrity Monitoring Rules
3. Applying the Policy to the computer
4. Monitoring Activity using the Manager

We will assume that you have already installed the Manager on the computer from which you intend to manage the Deep Security Agents throughout your network. We will also assume that **you have installed (but not activated) Deep Security Agents on the mobile laptops you wish to protect**. If you have not done so, consult the installation instructions for the steps to get to this stage.

## Adding computers to the Manager

You can add computers to the Deep Security **Computers** page by:

1. Adding computers individually by specifying their IP addresses or hostnames
2. Discovering computers by scanning the network
3. Connecting to a Microsoft Active Directory and importing a list of computers
4. Connecting to a VMware vCenter and importing a list of computers (not covered in this section because we are dealing with mobile laptops.)

### Adding computers individually by specifying their IP addresses or hostnames

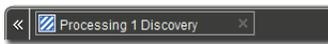
To add an individual computer by specifying its IP address or hostname, go to the **Computers** page and click **New** in the toolbar.

Type the hostname or IP address of the new computer in the **Hostname** text box. The **New Computer** wizard also lets you specify a Policy which it will apply to the new computer if it finds the computer and determines that an unactivated Agent is present. (For now, don't select a Policy.) 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 Editor** window (the Details window) which lets you configure many the Agent's settings. Skip the **Details** window for now.

### Adding computers by scanning the network (Discovery)

**To discover computers by scanning the network:**

1. Go to the **Computers** page.
2. Click **Discover...** in the toolbar to display the **Discover Computers** dialog.
3. Type a range of IP addresses you want to scan for computers. If you wish, you can enter a masked IP address to do the same thing.
4. Select **Automatically resolve IPs to hostnames** to instruct the Manager to automatically resolve hostnames as it performs the discovery.
5. You have the option to add discovered computers to a computer group you have created. For now, leave the **Add Discovered Computers to Group** drop-down list choice set to "Computers".
6. Finally, clear the **Automatically perform a port scan of discovered computers** checkbox. (Port scanning detects which ports are open on the discovered computers.)
7. Click **OK**. The dialog box will disappear and "Discovery in progress..." will appear in the Manager's status bar at the bottom of your browser. (The discovery process can be cancelled by clicking the "X".)



In a few minutes, all visible computers on the network will have been detected and the Manager will have identified those with Deep Security Agents installed. These Agents now need to be activated.

8. Activate the Agents by right-clicking an Agent (or multiple selected Agents), and select "Activate/Reactivate" from the shortcut menu. Once the Agents are activated, their status light will turn green and "Managed (Online)" will appear in the status column.

## Importing Computers from a Microsoft Active Directory

Computers imported from an Active Directory are treated the same as any other computers in the **Computers** page.

### To import computers from a Microsoft Active Directory:

1. Click the down arrow next to "New" in the **Computers** page toolbar and select **Add Directory...** to start the **Add Directory** wizard.

---

*Note:* Synchronization of computers from other LDAP-based directories may be possible but would require some customization. For assistance contact your support provider.

---

2. Type the Active Directory server name, a name and description for your imported directory as it will appear in the Manager (it doesn't have to match that of the Active Directory), the IP and port of the Active Directory server, and finally your access method and credentials. Click **Next**.

---

*Note:* You must include your domain name with your username in the **User Name** field.

---

3. If you select SSL or TLS as the Access method, the wizard will ask you to accept a security certificate. You can view the certificate accepted by the Deep Security Manager by going to **Administration > System Settings > Security** and clicking "View Certificate List..." in the Trusted Certificates area. Click **Next**.
4. The second page of the **New Directory** wizard asks for schema details. (Leave the default values). Click **Finish**.
5. The next page will tell you if there were any errors. Click **Next**.
6. The final page will let you create a Scheduled Task to regularly synchronize the Manager's **Computers** page with the Active Directory. Leave option this cleared for now. Click **Close**.

The directory structure now appears under **Computers** in the navigation panel.

## Additional Active Directory Options

Right-clicking an Active Directory structure gives you the following options that are not available for ordinary computer groups listed under **Computers**.

1. Remove Directory
2. Synchronize Now

### Remove Directory

When you remove a directory from the Deep Security Manager, you have the following options:

- **Remove directory and all subordinate computers/groups from DSM:** removes all traces of the directory.
- **Remove directory, but retain computer data and computer group hierarchy:** turns the imported directory structure into identically organized regular computer groups, no longer linked with the Active Directory server.
- **Remove directory, retain computer data, but flatten hierarchy:** removes links to the Active Directory server, discards directory structure, and places all the computers into the same computer group.

### Synchronize Now

Synchronizes the directory structure in the Deep Security Manager with the Active Directory Server. (Remember that you can automate this procedure as a **Scheduled Task**.)

Now that the Agents are active, they can be assigned Firewall Rules and Intrusion Prevention Rules. Although all the individual security objects can be assigned individually to an Agent, it is convenient to group common security objects into a Policy and then assign the Policy to one or more Agents.

---

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

---

## Activating the Agents on Computers

Agents need to be "activated" by the Manager before Policies and 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:* An Agent can be configured to automatically initiate its own activation upon installation. For details, see **Command-Line Utilities** in the Reference section of the online help.

---

To manually activate an Agent on a computer, right-click one or more selected computers and select **Actions > Activate/Reactivate**.

## Create a Policy for a Windows laptop

Now that the Agents are activated, it's time to assign some rules to protect the computer. Although you can assign rules directly to a computer, it's more useful to create a Policy which contains these rules and which can then be assigned to multiple computers.

Creating the Policy will involve the following steps:

1. Creating and naming the new Policy
2. Setting which interfaces to monitor
3. Setting the network engine to Inline Mode
4. Assigning Firewall Rules (including some with location awareness) and enable Stateful Inspection
5. Assigning Intrusion Prevention Rules
6. Assigning Integrity Monitoring Rules
7. Assigning Log Inspection Rules

8. Assigning the Policy to the computer

## Creating and naming the New Policy

To create and name the new Policy:

1. Go to the **Policies** section, click on Policies in the navigation panel on the left to go to the **Policies** page.
2. Click **New** in the toolbar to display the **New Policy** wizard.
3. Name the new Policy "My New Laptop Policy" and select **Base Policy** from the **Inherit from:** menu. Click **Next**.
4. The next page asks if you would like to base the Policy on an existing computer's current configuration. If you were to select **Yes**, you would be asked to pick an existing managed computer and the wizard would take all the configuration information from that computer and create a new Policy based on it. This can be useful if, for instance, you have fine-tuned the security configuration of an existing computer over a period of time and now wish to create a Policy based on it so that you can apply it to other functionally identical computers. For now, select **No** and click **Next**.
5. The last page confirms that the new Policy has been created. Select the **Open Policy Details on 'Close'** option and click **Close**.

## Setting which interfaces to monitor

**To set which interfaces to monitor:**

1. Because you set the **Open Policy Details on 'Close'** option, the new Policy editor window is displayed.
2. The laptops to which this Policy will be assigned are equipped with two network interfaces (a local area connection and a wireless connection) and we intend to tune the security configuration to take into account which interface is being used. Click **Interface Types** in the navigation panel and select the **Rules can apply to specific interfaces** option. Enter names for the interfaces and strings (with optional wildcards) which the Agent will use to match to interface names on the computer: "LAN Connection" and "Local Area Connection \*", and "Wireless" and "Wireless Network Connection \*" in the first two Interface Type areas. Click **Save** at the bottom right of the page.

## Setting the network engine to Inline Mode

The Agent's network engine can operate Inline or in Tap Mode. When operating Inline, the live packet stream passes through the network engine. Stateful tables are maintained, Firewall Rules are applied and traffic normalization is carried out so that Intrusion Prevention Rules can be applied to payload content. When operating in Tap Mode, the live packet stream is cloned and diverted from the main stream. In Tap Mode, the live packet stream is not modified; all operations are carried out on the cloned stream.

For now, we will configure our Policy to direct the engine to operate Inline.

**To set the network engine to Inline Mode:**

1. Still in the My New Laptop Policy editor, go to **Settings** and click on the **Network Engine** tab.
2. Set the Network Engine Mode to **Inline**. By default, the setting should already be set to "Inherited (Inline)" since the **Base** policy default mode is **Inline** and your new Policy inherits its settings from there.

## Assigning Firewall Rules (including some with location awareness) and turn on Stateful Inspection

**To assign Firewall Rules:**

1. Click **Firewall** in the navigation panel and in the **Firewall** area of the **General** tab, select **On** from the **Firewall State** drop-down menu.

---

**Note:** Selecting "Inherit" will cause this setting on this Policy to be inherited from its parent Policy. This setting in the parent Policy may already be "On" but for now you will enforce the setting at the level of this Policy regardless of any parent Policy settings. For information on Inheritance, see **Policies, Inheritance and Overrides** in the Reference section of the online help.

---

2. Now we will assign some Firewall Rules and Firewall Stateful Configuration rules to this Policy. Click **Assign/Unassign** to display the list of available predefined Firewall Rules. (You can create your own Firewall Rules, but for this exercise we will select from the list of existing ones.) Select the following set of Firewall Rules to allow basic communication:
  - Allow Solicited ICMP replies
  - Allow solicited TCP/UDP replies
  - Domain Client (UDP)
  - ARP
  - Wireless Authentication
  - Windows File Sharing (This is a force-allow rule to permit incoming Windows File Sharing traffic.)

Notice the gray down-arrow next to the Firewall Rule checkboxes. These appear if you have defined multiple interfaces in the previous step. They allow you to specify whether the Firewall Rule will apply to all interfaces on the computer or just to interfaces that you specify. Leave these at the default setting for now. Click the **Save** button.

We assigned a Firewall Rule that permitted Windows File Sharing. Windows File Sharing is a very useful feature in Windows but it has had some security issues. It would better to restrict this ability to when the laptop is in a secure office environment and forbid it when the laptop is out of the office. We will apply Location Awareness to the Firewall Rule when used with this Policy to implement this policy.

#### To implement location awareness:

1. In the **My New Laptop Policy** Policy editor, go to **Firewall > General > Assigned Firewall Rules**, right-click the "Windows File Sharing Firewall" Rule and select **Properties....** This will display the **Properties** window for the Firewall Rule (but the changes we make to it will only apply to the Firewall Rule when it is applied as part this new Policy).
2. In the **Properties** window, click the **Options** tab.
3. In the **Rule Context** area, select **New...** from the drop-down list. This displays the **New Context** Properties window. We will create a Rule Context that will only allow the Firewall Rule to be active when the laptop has local access to its Domain Controller. (That is, when the laptop is in the office.)
4. Name the new Rule Context "In the Office". In the **Options** area, set the **Context applies when connection is:** option and select **Locally Connected to Domain** below it. Then click **Ok**.
5. Click **OK** in the Windows File Sharing Firewall Rule **Properties** window.

Now the Windows File Sharing Firewall Rule will only be in effect when the laptop has local access to its Windows Domain Controller. The Windows File Sharing Firewall Rule is now displayed in bold letters in the Policy **Details** window. This indicates that the Firewall Rule has had its properties edited for this Policy only.

---

**Note:** Location Awareness is also available for Intrusion Prevention Rules.

---

The final step in the Firewall section is to enable Stateful inspection.

#### To enable Stateful Inspection:

1. Still in the **My New Laptop Policy** Policy editor window, go to **Firewall > General > Firewall Stateful Configurations**.
2. For the **Global (All Interfaces)** setting, select **Enable Stateful Inspection**.
3. Click **Save** to finish.

## Assigning Intrusion Prevention Rules

#### To assign Intrusion Prevention rules to the Policy:

1. Still in the **My New Laptop Policy** editor window, click **Intrusion Prevention** in the navigation panel.
2. On the General tab, in the **Intrusion Prevention** area, set the **Intrusion Prevention State** to **On**.

---

**Note:** *Intrusion Prevention can be set to either Prevent or Detect mode when the Network Engine is operating Inline (as opposed to Tap Mode). Detect mode is useful if you are trying out a new set of Intrusion Prevention Rules and do not want to risk dropping traffic before you are sure the new rules are working properly. In Detect Mode, traffic that would normally be dropped will generate events but will be allowed to pass. Set Intrusion Prevention to "On".*

---

**Note:** *Note the **Recommendations** area. The Deep Security Agent can be instructed to run a Recommendation Scan. (On the Manager's **Computers** page, right-click a computer and select **Actions > Scan for Recommendations**.) The Recommendation engine will scan the computer for applications and make Intrusion Prevention Rule recommendations based on what it finds. The results of the Recommendation Scan can be viewed in the computer editor window by going to **Intrusion Prevention > Intrusion Prevention Rules > Assign/Unassign...** and selecting **Recommended for Assignment** from the second drop-down filter menu.*

---

3. For now, leave the **Recommendations > Automatically implement Intrusion Prevention Recommendations (when possible):** option set to **Inherited (No)**.
4. In the Assigned Intrusion Prevention rules area, click **Assign/Unassign...** to open the rule assignment window.
5. Intrusion Prevention Rules are organized by Application Type. Application Types are a useful way of grouping Intrusion Prevention Rules; they have only three properties: communication direction, protocol, and ports. For our new laptop Policy, assign the following Application Types:
  - Mail Client Outlook
  - Mail Client Windows
  - Malware
  - Malware Web
  - Microsoft Office
  - Web Client Common
  - Web Client Internet Explorer
  - Web Client Mozilla Firefox
  - Windows Services RPC Client
  - Windows Services RPC Server

---

**Note:** *Make sure the first two drop-down filter menus are showing **All** and that the third sorting filter menu is sorting **By Application Type**. It's easier to page through the Application Types if you right-click in the Rules list and select **Collapse All**. There are many Application Types (and Intrusion Prevention Rules), so you will have to use the pagination controls at the bottom right of the page to find them all, or use the search feature at the top right of the page. Select an Application Type by putting a check next to the Application Type name.*

---

**Note:** *Some Intrusion Prevention Rules are dependent on others. If you assign a rule that requires another rule to also be assigned (which has not yet been assigned) a popup window will appear letting you assign the required rule.*

---

**Note:** *When assigning any kinds of Rules to a computer, do not let yourself be tempted to be "extra secure" and assign all available rules to your computer. The Rules are designed for a variety of operating systems, applications, vulnerabilities and may not be applicable to your computer. The traffic filtering engine would just be wasting CPU time looking for patterns that will never appear. Be selective when securing your computers!*

---

6. Click **OK** and then **Save** to assign the Application Types to the Policy.

## Assigning Integrity Monitoring Rules

**To assign Integrity Monitoring Rules to the Policy:**

1. Still in the **My New Laptop Policy** editor window, click **Integrity Monitoring** in the navigation panel.
2. On the **General** tab, set **Integrity Monitoring State** to **On**.
3. Set **Automatically implement Integrity Monitoring Recommendations (when possible)**: to **No**.
4. Now click **Assign/Unassign...** in the **Assigned Integrity Monitoring Rules** area.
5. In the Search box at the top right of the page type the word "Windows" and press Enter. All the rules that apply to Microsoft Windows will be displayed in the rules list. Right-click one of the rules and choose "Select All", then right-click again and choose "Assign Rule(s)". This will assign all the rules that came up in the search result to the Policy.

## Assigning Log Inspection Rules

### To assign Log Inspection Rules to the Policy:

1. Still in the **My New Laptop Policy** editor window, click **Log Inspection** in the navigation panel.
2. Deselect **Inherit** and set Log Inspection to **On**.
3. Set **Automatically implement Log Inspection Rule Recommendations (when possible)**: to **No**.
4. Now click **Assign/Unassign...** in the **Assigned Log Inspection Rules** area.
5. Select the "1002792 - Default Rules Configuration" Rule (required for all other Log Inspection Rules to work), and the "1002795 - Microsoft Windows Events" rule. (This will log events any time Windows auditing functionality registers an event on the laptop.)
6. Click **OK** and then **Save** to apply the rules to the Policy.

We are now finished editing the new Policy. You can now close the My New Policy **Details** window.

## Edit the Domain Controller(s) IP List

Finally, since the new Policy includes three Firewall Rules that use the "Domain Controller(s)" IP List, we will have to edit that IP List to include the IP addresses of the local Windows Domain Controller:

### To edit the Domain Controllers IP list:

1. In the main window of the Deep Security Manager console, go to the **Policies > Common Objects > Lists > IP Lists**.
2. Double-click the **Domain Controller(s)** IP List to display its **Properties** window.
3. Type the IP(s) of your domain controller(s).
4. Click **OK**.

## Apply the Policy to a Computer

Now we can apply the Policy to the computer:

### To apply the Policy to the computer:

1. Go to the **Computers** page.
2. Right-click the computer to which you will assign the Policy and select **Actions > Assign Policy...**
3. Choose "My New Laptop Policy" from the drop-down list in the **Assign Policy** dialog box.
4. click **OK**

After clicking **OK**, the Manager will send the Policy 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)".

## Configure SMTP Settings

Configuring the Deep Security Manager's SMTP settings allows email Alerts to be sent out to Users.

**To configure SMTP settings:**

1. Go to **Administration > System Settings** and click the **SMTP** tab.
2. Type the configuration information and click the **Test SMTP Settings** to confirm Deep Security Manager can communicate with the mail server.
3. Go to the **Alerts** tab.
4. In the **Alert Event Forwarding (From the Manager)** section, type the default email address to which you want notifications sent.
5. Click **Save**.

---

**Note:** Whether a User gets emailed Alerts can be configured on that User's **Properties** window (**Administration > User Management > Users**). Whether a particular Alert generates emailed notifications can be configured on that Alert's **Properties** window.

---

## Monitor Activity Using the Deep Security Manager

### The Dashboard

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

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

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

- Firewall Computer Activity (Prevented)
- Firewall Event History [2x1]
- Firewall IP Activity (Prevented)

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

- The **Firewall Computer Activity (Prevented)** widget displays a list of the most common reasons for packets to be denied (that is, blocked from reaching a computer by the Agent on that computer) along with the number of packets that were denied. Items in this list will be either types of Packet Rejections or Firewall Rules. Each "reason" is a link to the corresponding logs for that denied packet.
- The **Firewall Event History [2x1]** widget displays a bar graph indicating how many packets were blocked in the last 24 hour period or seven day period (depending on the view selected). Clicking a bar will display the corresponding logs for the period represented by the bar.
- The **Firewall IP Activity (Prevented)** widget displays a list of the most common source IPs of denied packets. Similar to the **Firewall Activity (Prevented)** widget, each source IP is a link to the corresponding logs.

---

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

---

## Logs of Firewall and Intrusion Prevention Events

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

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

## Reports

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

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

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



**TREND MICRO INCORPORATED**

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

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

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

Item Code: APEM96491/140716