

9.5 Deep Security Service Pack 1

Installation Guide [Amazon AWS Marketplace](#)

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: 1.4

Document number: APEM96479/140922

Release date: April 2015

Document generated: Apr 6, 2015 (11:27:17)

Table of Contents

About Deep Security	4
Installation Checklist.....	6
Deep Security Licensing on AWS Marketplace	7
Check Permissions and Communication	8
Database Deployment Considerations.....	9
Installing the Deep Security Manager	11
Upgrading the Deep Security Manager.....	15
Add Amazon EC2 Resources to Deep Security Manager	16
Installing Deep Security Agents	19
Appendices	26
System Requirements	27
Deep Security Manager Performance Features	29
Creating an SSL Authentication Certificate	30
Connecting to your instance via SSH	32

About Deep Security

Deep Security is designed to run on and with Amazon Web Services. It provides advanced server security for physical, virtual, and cloud servers, makes it fast and easy to secure EC2 and virtual, private, cloud (VPC) instances. Management of security is performed from an integrated administrative console that automatically provides a single up-to-date view of your security posture in the AWS environment.

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

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

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

The Web Reputation Service:

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

Firewall

Decreases the attack surface of your physical and virtual servers.

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

Intrusion Prevention

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

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

Defends against web application vulnerabilities

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

Identifies malicious software accessing the network

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

Integrity Monitoring

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

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

Log Inspection

Provides visibility into important security events buried in log files.

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

Deep Security Components

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

- **Deep Security Manager**, the centralized Web-based management console, which administrators use to configure security policy and deploy protection to the enforcement component: the Deep Security Agent.
- **Deep Security Agent** is a security agent deployed directly on a computer which provides Anti-Malware, Web Reputation Service, Firewall, Intrusion Prevention, Integrity Monitoring, and Log Inspection protection to computers on which it is installed.
 - The Deep Security Agent contains a **Relay Module**. A Relay-enabled Agent distributes Software and Security Updates throughout your network of Deep Security components. When you install the AWS Marketplace version of Deep Security Manager, a Relay-enabled Agent is also installed.

Installation Checklist

Complete the tasks in this checklist to install Deep Security

Step	Task	Details	Done
1.	Decide which type of licensing you will use	Deep Security Licensing on AWS Marketplace (page 7)	
2.	Check that permissions, ports, and other settings are configured properly	Check Permissions and Communication (page 8)	
3.	Install and configure a database for use with Deep Security	Database Deployment Considerations (page 9)	
4.	Install Deep Security Manager	Installing the Deep Security Manager (page 11)	
5.	Add your Amazon EC2 instances to Deep Security Manager	Add Amazon EC2 Resources to Deep Security Manager (page 16)	
6.	Perform the initial basic Deep Security system configuration that is required before you can start protecting your computer resources.	See "Quick Start: System Configuration" in the Deep Security Manager Help or Administrator's Guide.	
7.	Protect your computer resources.	See "Quick Start: Protecting a Computer" in the Deep Security Manager Help or Administrator's Guide.	

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

Deep Security Licensing on AWS Marketplace

On the AWS Marketplace, there are two licensing options for Deep Security:

- **BYOL:** Bring-Your-Own-License (BYOL) is for customers who have already obtained a license to use Deep Security 9.5 SP1. If you are using this type of license, you will need to enter the License string/activation code in the Deep Security Manager console after it is installed. (See [Installing Deep Security Manager \(page 11\)](#).)
- **PPU:** Pay-Per-Use (PPU) enables customers to pay based on the size of the AWS instance they are running. With PPU, each EC2 instance type has an associated seat count limit (the seat count is the number of Deep Security Agents that you can run). You can change the size of your instance at any time. You can also run more than one instance to increase your seat count limit. When you install Deep Security Manager on an additional instance, on the Database tab, select "This Deep Security installation will act as an additional Manager node in an already-deployed Deep Security installation". This option specifies that each node will use the same database. Here are the seat count limits for each type of EC2 instance supported for Deep Security Manager:
 - **M3 Large (m3.large):** Up to 25 Agents
 - **M3 XL (m3.xlarge):** Up to 50 Agents
 - **M3 2XL (m3.2xlarge):** Up to 100 Agents
 - **C3 4XL (c3.4xlarge):** Up to 200 Agents

As you launch or shut down Deep Security Manager nodes, the seat-count usage for the hour is re-calculated. To check your seat count limit after installing Deep Security Manager, open the Deep Security Manager console and go to **Administration > Licenses**.

Note: *The AWS Marketplace version of Deep Security Manager does not support the use of vCenter and the Deep Security Virtual Appliance (DSVA). Additionally, the PPU license does not provide Multi-Tenant support.*

Check Permissions and Communication

AWS Credentials

You will need to know your AWS account credentials.

Administrator/Root Privileges

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

SMTP Server

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

Proxy Server Information

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

Available Ports on Agents and Relay-enabled Agents

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 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 Agents and Relay-enabled Agents.

Network Communication

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

Performance Recommendations

See [Deep Security Manager Performance Features \(page 29\)](#).

Database Deployment Considerations

Before installing Deep Security Manager, you must install a database. You can install your own database or you can use the Amazon RDS Management Console to create a database instance. You can use a Microsoft SQL RDS or an Oracle RDS. Refer to the [Amazon RDS Documentation](#) for instructions, but keep the following considerations in mind for integration with Deep Security.

Note: You must configure your database security group so that the Deep Security AMI is authorized to access it. The EC2 Security Group created by the AMI is "Deep Security-Deep Security 9-5-AutogenByAWSMP- Security Group".

General Considerations

Version

See [System Requirements \(page 27\)](#) for a list of supported databases.

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.

Deep Security Manager and Database Hardware

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.

Transport Protocol

The recommended transport protocol is **TCP**.

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.

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.

Microsoft SQL Server Considerations

- 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. (For information on Multi-Tenancy, see [Multi-Tenancy \(page 0\)](#).)
- Select the "simple" recovery model property for your database. (See <http://technet.microsoft.com/en-us/library/ms189272.aspx>)

Oracle Database Considerations

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

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

Multi-Tenancy Considerations

For information on Multi-Tenancy, see [Multi-Tenancy \(page 0\)](#). For additional database requirements, see [Installing a Database for Deep Security \(Multi-Tenancy Requirements\) \(page 0\)](#).

Note: *Multi-Tenancy is not supported with a Pay-Per-Use license.*

Installing the Deep Security Manager

Deploy an Instance

To access the Deep Security AMIs, go to the AWS Marketplace and search for Deep Security. You will see the PPU and BYOL AMIs. Select the appropriate AMI. This displays a page that describes the product and pricing information. Click Continue. On the next page, you can select other options and launch your instance.

After the instance is deployed, go to your AWS management console and access the EC2 Dashboard. Under "AMIs", you will see the Deep Security Manager AMI. The Deep Security Manager AMI must contain security group policies that open these ports:

Protocol	Port	Source	Used by
TCP	443		Deep Security Manager web console
TCP	8080	Current IP	Web installer page (used only for initial setup and upgrade)
TCP	4120	10.0.0.0/0 (or other VPC block)	Deep Security Agent heartbeat
TCP	4122	10.0.0.0/0 (or other VPC block)	Relay-enabled Agent
TCP	4118		Communication between Agent, Relay, and Manager

Connecting to your instance via SSH

The AWS Marketplace version of Deep Security Manager is installed on AWS Linux. To connect to your Deep Security Manager instance via SSH, please refer to these instructions from Amazon: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html>.

Note that the username for the Deep Security Manager instance is "trend", and not "root" or "ec2-user".

Configure Deep Security Manager on an Instance

After launching your Deep Security instance, perform the following steps to configure Deep Security Manager:

1. Go to the Deep Security Manager pre-installer page (<https://IP:8080>). Enter the instance ID number for the EC2 instance where you are installing Deep Security Manager and click **Sign In**. The Deep Security AMI Configuration page appears, with a series of tabs.
2. **License Agreement:** On the first tab, review the license agreement. If you agree to the terms, select **I accept the agreement** and click **Next**.
3. **Database:** Select the type of database that you have configured for use with Deep Security and fill in the required configuration parameters. Select **This Deep Security Manager installation will act as a new Manager node**. The installation process will check for database connectivity and display an error if there is a problem. If you selected Microsoft SQL Server, you can also edit the SQL Server Advanced Options. Click **Next**.
4. **Address and Ports:** Enter the hostname or IP address of the machine where Deep Security Manager is being installed. 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. Click **Next**.

Note: *If your instance has a public IP and DNS entry, it is recommended that you use the public DNS entry for the Manager Address (default). Using the IP address may result in loss of connectivity if the IP changes.*

5. **Credentials:** Enter a username and password that you will use to log in to the Deep Security Manager console. You should use a strong password that includes upper and lower-case letters, non-alphanumeric characters, and numbers. Click **Next**.
6. **Confirm Settings:** Review the installation settings to ensure they are correct and then click **Install**.
7. The Deep Security Status page will indicate that Deep Security Manager is being installed.

- When the installation is complete, the Deep Security Manager console will be displayed. You can log in with the username and password that you specified during the Deep Security Manager installation process. Note the URL used to access the Deep Security Manager console.

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 \(page 30\)](#).*

Running Deep Security Manager on Multiple Nodes

Deep Security Manager can be run as multiple nodes operating in parallel using a single database. Running the Manager as multiple nodes provides increased reliability, redundant availability, virtually unlimited scalability, and better performance. It also enables you to increase your seat count limit (for details, see [Deep Security Licensing on AWS Marketplace \(page 7\)](#)).

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

Installing Deep Security Manager on Multiple Nodes

When you install Deep Security Manager on an additional instance, on the **Database** tab, select **This Deep Security installation will act as an additional Manager node in an already-deployed Deep Security installation**. This option specifies that each node will use the same database.

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

Upgrading Deep Security Manager on Multiple Nodes

All nodes must be running the same version of the Manager software. Before upgrading any of your nodes, you must shut down and delete all but one of your Deep Security Manager nodes. You can upgrade Deep Security Manager on the remaining node and then deploy new nodes with the same version from AWS Marketplace.

Enter your activation codes in Deep Security Manager (BYOL)

If you are using BYOL, you will need to enter your activation code(s) in Deep Security Manager after it is installed. This step is not required for PPU licensing.

To enter your activation codes:

- In the Deep Security Manager console, go to **Administration > Licenses**.
- Click **Enter New Activation Code** and enter the code for All Protection Modules or the codes for the individual modules for which you have purchased a license.

Enable Agent-initiated Communication

If you want to use Deployment Scripts to deploy Agents on the AWS instances that you want to protect, Deep Security Manager must be configured to use **Agent-initiated** communication.

By default, Agent-initiated communication is enabled with the AWS Marketplace version of Deep Security Manager.

To ensure that Agent-initiated communication is enabled:

1. In the Deep Security Manager console, go to **Administration > System Settings > Agents > Agent-Initiated Activation**.
2. Ensure that **Allow Agent-Initiated Activation** is selected.
3. Ensure that **Allow Agent to specify hostname** is selected.
4. Click **Save**.

Manually Importing Additional Deep Security Software

Deep Security Agents software packages must be imported into Deep Security Manager before you install the Agent on a computer. The AWS Marketplace version of Deep Security Manager automatically imports these Deep Security Agent software packages:

- Red Hat 5 (32-bit and 64-bit)
- Red Hat 6 (32-bit and 64-bit)
- SUSE 10 (32-bit and 64-bit)
- SUSE 11 (32-bit and 64-bit)
- 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)
- Windows (32-bit and 64-bit)

You can import additional Deep Security Agent software packages from within the Deep Security Manager, on the **Administration > Updates > Software > Download Center** page.

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.

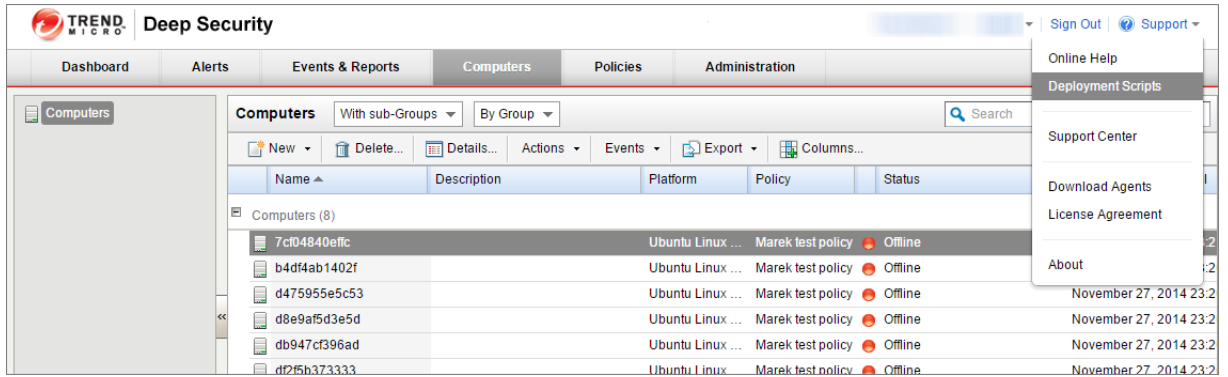
The software is now imported into the Deep Security Manager.

Add a Deployment Script to your Instance

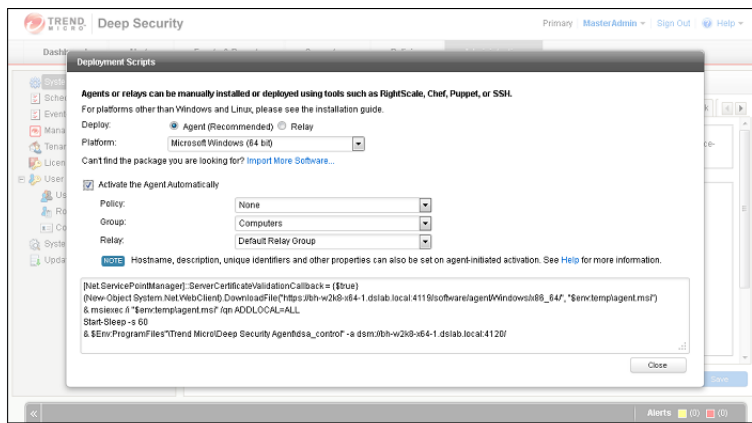
Deep Security Manager enables you to generate a script that you can add to instances that you want to protect.

Generate a deployment script

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



2. Select the platform to which you are deploying the software. Platforms listed in the drop-down menu will correspond to the software that you have imported into the Deep Security Manager from the Trend Micro Download Center.
3. Select **Activate the Agent Automatically**. (Agents must be activated by the Deep Security Manager before a protection Policy can be implemented.)



4. As you make the selections, the Deployment Script Generator will generate a script that you can add to your Deep Security instance. Copy the script.

Add the script to the instance that you want to protect

To add the script to a new instance that you want to protect, go to the AWS Marketplace and add the new instance. When you reach step **3 (Configure Instance)**, open the **Advanced Details** section. Next to **User data**, select **As text** and paste the script into the box provided. Continue with the instance activation as usual. The Agent will be added and activated as soon as the image boots up.

You can also run the script as a shell script or batch file on instances that are already up and running.

Upgrading the Deep Security Manager

Note: We strongly recommend backing up your database before proceeding with the upgrade.

Note: If you are running Deep Security Manager on multiple nodes, decommission all but one of the nodes, upgrade the remaining node, and then add new nodes, as required.

To upgrade Deep Security Manager:

1. When a new Deep Security Manager AMI is available, an alert appears at the top of the Deep Security Manager console. In the alert, click **Upgrade Deep Security AMI**.

You can also go to **Administration > Updates > Software**. If "A new version of the Deep Security Manager AMI is available" is displayed, click **Upgrade Deep Security AMI**.

2. A pop-up appears, warning that the upgrade will make the Deep Security Manager console unavailable for approximately 5 minutes. Click **OK**.

Add Amazon EC2 Resources to Deep Security Manager

Once you have imported the resources from the Cloud Provider account into the Deep Security Manager, the computers in the account are managed like any computer on a local network.

To import cloud resources into their Deep Security Manager, Deep Security Users must first have an account with which to access the cloud provider service resources. For each Deep Security User who will import a cloud account into the Deep Security Manager, Trend Micro Recommends creating dedicated account for that Deep Security Manager to access the cloud resources. That is, Users should have one account to access and control the virtual machines themselves, and a separate account for their Deep Security Manager to connect to those resources.

Note: *Having a dedicated account for Deep Security ensures that you can refine the rights and revoke this account at any time. It is recommended to give Deep Security an Access/Secret key with read-only rights at all times.*

Note: *The Deep Security Manager only requires read-only access to import the cloud resources and manage their security.*

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

Creating an Amazon Web Services account for the Deep Security Manager

To create an Amazon Web Services account for access by a Deep Security Manager:

1. Log in to your Amazon Web Services Console and go to **Identity and Access Management (IAM)**.
2. In the left navigation pane, click **Policies**.

Note: *If this is your first time on this page, you'll have to click **Get Started**.*

3. Select **Create Policy**.
4. Select **Create Your own Policy**.
5. Give the Policy a name and description, then copy the following JSON code into the **document Policy** area:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "cloudconnector",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeTags"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

6. Click **Create Policy**. Your policy is now ready for use.
7. Back in the **Identity and Access Management** page's navigation pane, click on **Users**.

8. Click **Create New Users** to display the **Create User** page.
9. Enter a username and select the **Generate an access key for each User** option.
10. click **Download Credentials** to download the generated User Security credentials (Access Key and Secret Key) and then close the dialog window.
11. Back on the Users page, click on the User to display the User properties, then scroll to the **Permissions** section of the page.
12. In the expanded **Permissions** section, click on **Attach Policy** at the bottom of the window to display the **Attach Policy** page.
13. Select the Policy you just created and click **Attach Policy** to apply the policy to the new user account.

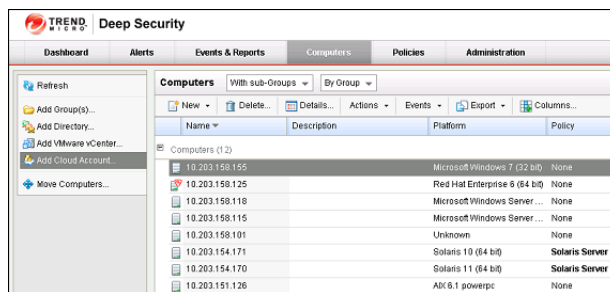
The Amazon Web Services account is now ready for access by a Deep Security Manager.

Note: To import the Amazon AWS resources into the Deep Security Manager, the User will be prompted for the **Region** the resources are hosted in. If resources are hosted in multiple regions, the User will have to add the resources independently for each region.

Importing Computers from a Amazon Web Services account

To import Amazon Web Services cloud resources:

1. In the Deep Security Manager, go to the **Computers** section, right-click **Computers** in the navigation panel and select **Add Cloud Account**.



2. The **Add Cloud Provider Wizard** appears. Enter this information and then click **Next**:
 - **Provider Type:** Select Amazon.
 - **Provider Region:** Select the region where the cloud resources are hosted. If resources are hosted in multiple regions, you will have to add the resources independently for each region.
 - **Name** and **Description:** Name and description of the resources you are adding. These are only used for display purposes in the Deep Security Manager.
 - **Access Key Id** and **Secret Access Key:** Provided to you by your AWS administrator.

Please provide the following information for the cloud provider being added.

Cloud Provider

Provider Type: Amazon

Provider Region: US East (Virginia)

Name: Amazon

Description:

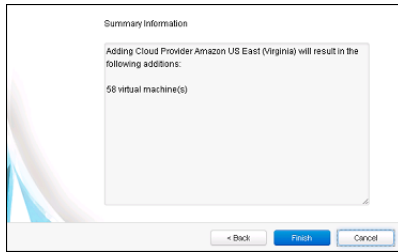
Access Information

Access Key Id: AKIAJSHAT9327NLYDU5A

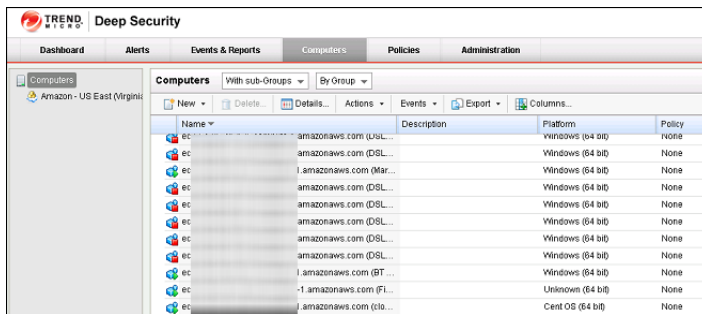
Secret Access Key:

Buttons: Back, Next, Cancel

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



4. Upon successfully importing the Cloud Provider resources, the wizard will display the results of the action.
5. The Amazon AWS resources now appear in the Deep Security Manager under their own branch under **Computers** in the navigation panel.



After adding the Cloud Provider resources, you must install an Agent and assign a Policy to the computer (see [Manually Installing the Deep Security Agent \(page 19\)](#).)

Installing Deep Security Agents

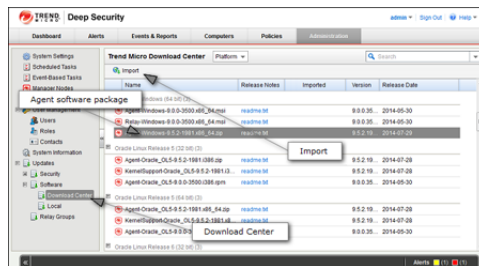
This section describes how to install and activate Deep Security Agents and how to enable Relay functionality (if required).

Importing Agent Software

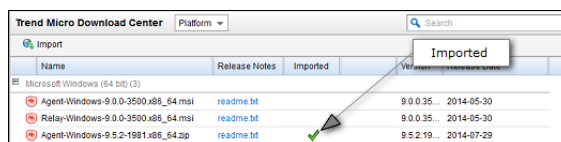
A Deep Security Agent is initially installed with core functionality only. It is only when a Protection Module is enabled on an Agent that the plug-ins required for that module are downloaded and installed. *For this reason, Agent software packages must be imported into Deep Security Manager before you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



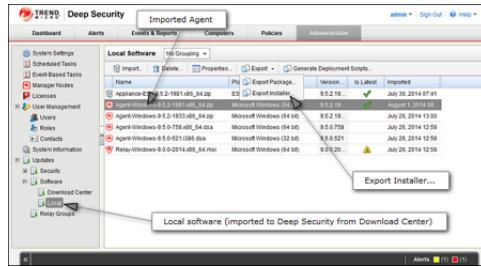
3. When the software has finished downloading, a green check mark will appear in the **Imported** column for that Agent.



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.*



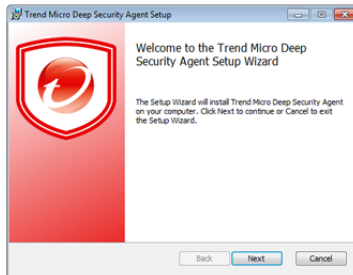
3. Save the Agent installer to a local folder.

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.

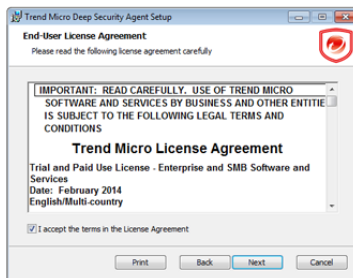
The Deep Security Agent "zip" files are made available on the Trend Micro Download Center for users who need to manually import the Agents into their Deep Security environment because their Deep Security Manager is air-gapped and cannot connect directly to the Download Center web site. Users whose Deep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

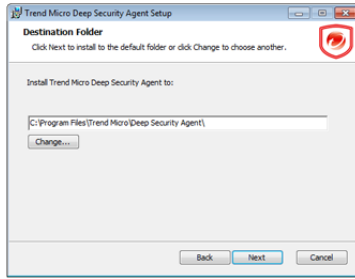
1. Copy the Agent installer file to the target machine and double-click the installation file to run the installer package. At the Welcome screen, click **Next** to begin the installation.



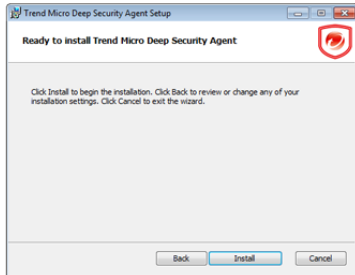
2. **End-User License Agreement:** If you agree to the terms of the license agreement, select **I accept the terms of the license agreement** and click **Next**.



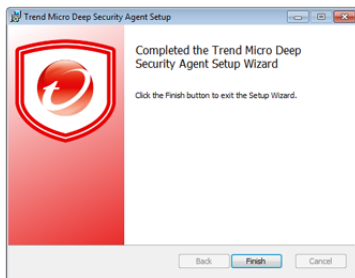
3. **Destination Folder:** Select the location where you would like Deep Security Agent to be installed and click **Next**.



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.*

Installing the Red Hat, SUSE, or Oracle Linux Agent

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

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

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

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

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

Installing the Ubuntu Agent

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

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

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

Starting, stopping and resetting the Agent on Linux:

Command-line options:

To start the Agent:

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

To stop the Agent:

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

To reset the Agent:

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

To restart the Agent:

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

Using Deployment Scripts to Install Agents

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

To generate a deployment script:

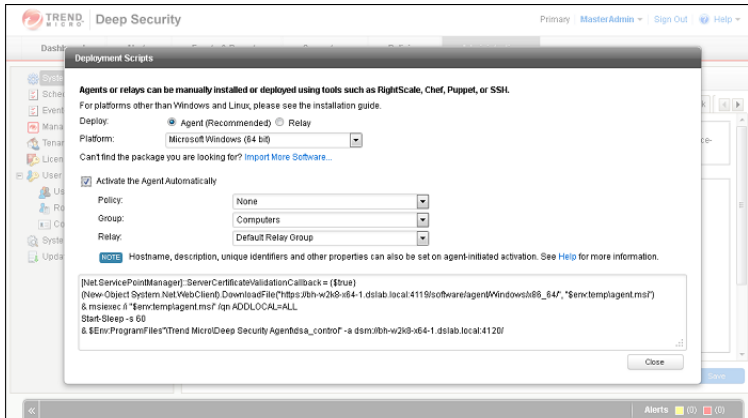
1. Start the Deployment Script generator by clicking **Deployment Scripts...** from the Deep Security Manager's Support menu (at the top right of the Deep Security Manager window).
2. Select the platform to which you are deploying the software.

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

3. Select **Activate 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

Deep Security 9.5 or later does not disable Linux iptables during installation. If you are using a pre-9.5 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:

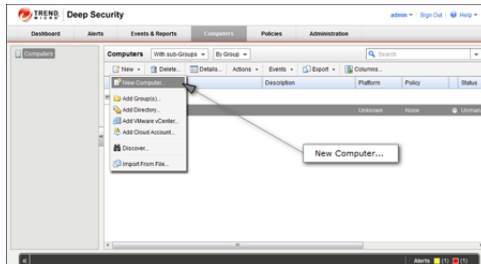
```
# Required-Stop:
```

Activating the Agent

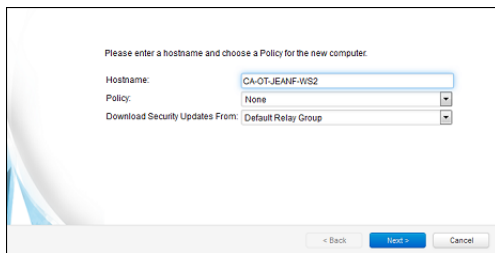
The Agent must be activated from the Deep Security Manager before it can be configured to act as a Relay or to protect the host computer.

To activate the newly installed Agent:

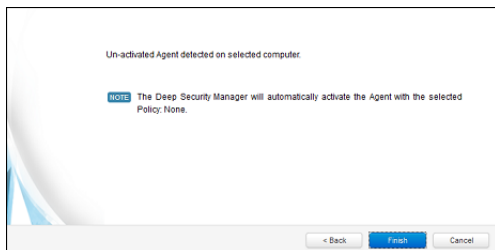
1. In the Deep Security Manager, go to the Computers page and click **New > New Computer...** to display the **New Computer Wizard**.



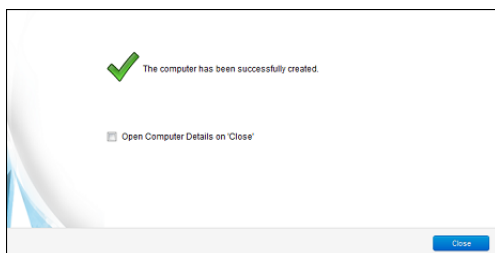
2. Enter the hostname or IP address of the computer. If you want to use the Agent to provide protection for the host computer as well as function as a Relay, select a Deep Security Policy from the **Policy** menu. Otherwise leave **Policy** set to "None".



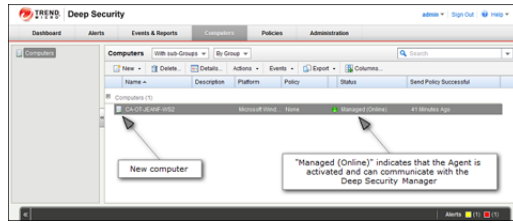
3. The wizard will confirm that it will activate the Agent on the computer and apply a Security Policy (if one was selected).



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



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



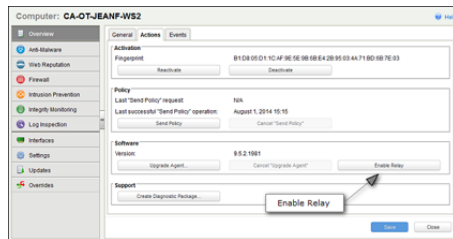
Enabling Relay Functionality



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

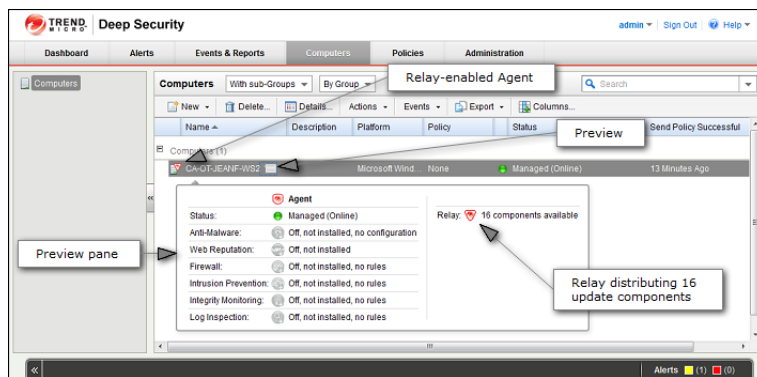
Note: Once enabled on an Agent, Relay functionality cannot be disabled.

To enable Relay functionality:

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



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



Appendices

System Requirements

Deep Security Manager

Deep Security Manager is available as an AWS Marketplace Linux Instance.

- **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

Database

Deep Security Manager requires a database. You can install your own database or you can use the Amazon RDS Management Console to create a database instance. For additional information, see [Database Deployment Considerations \(page 9\)](#).

- Oracle Database 11g, Oracle Database 11g Express
- Oracle Database 10g, Oracle Database 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

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 SP1 Supported Features and Platforms**. For a list of specific Linux kernels supported for each platform, see the document titled **Deep Security 9.5 SP1 Supported Linux Kernels**.*

Deep Security Notifier System Requirements

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

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. By default, new installations use the "Aggressive" performance profile which is optimized for a dedicated Manager. 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-initiated connections that the Manager will accept. The default of each of the performance profiles effectively balances the amount of accepted, delayed and rejected heartbeats.

Low Disk Space Alerts

Low Disk Space on the Database Host

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

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

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

Low Disk Space on the Manager Host

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

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

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

You must restart the Manager manually.

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

Creating an SSL Authentication Certificate

The Deep Security Manager creates a 10-year self-signed certificate for the connections with Agents, 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 Linux SSL authentication certificate:

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

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

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

5. Choose a password when prompted.
6. There is a new `.keystore` file created under the user home directory. If you are logged in as "Administrator", You will see the `.keystore` file under `./root/`
If the file is hidden, use the following command: `find -type f -iname ".keystore" -ls`
7. View the newly generated certificate using the following command:

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

8. Run the following command to create a CSR for your CA to sign:
- ```
opt\dsm\jre\bin# keytool -certreq -keyalg RSA -alias tomcat -file certrequest.csr
```
- If you see "**Keytool unrecognized option '-keyalg'**", use '**-sigalg**' instead.
9. Send the `certrequest.csr` to your CA to sign. In return you will get two files. One is a "certificate reply" and the second is the CA certificate itself.
  10. Run the following command to import the CA cert in JAVA trusted keystore:

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

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

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

(say yes to warning message)

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

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

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

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

14. Copy the .keystore file from your user home directory `.\root\` to `\opt\dsm\`
15. Open the configuration.properties file in folder `C:\Program Files\Trend Micro\Deep Security Manager`. It will look something like:

```
keystoreFile= opt\\dsm\\.keystore
port=443
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.

## Connecting to your instance via SSH

The AWS Marketplace version of Deep Security Manager is installed on AWS Linux. To connect to your Deep Security Manager instance via SSH, please refer to these instructions from Amazon: <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html>.

Note that the username for the Deep Security Manager instance is "trend", and not "root" or "ec2-user".







**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: APEM96790/141124