Deep Security
Installation Guide (Microsoft Azure Marketplace)
Advanced Protection for Physical, Virtual, and Cloud Servers
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: APEM07359_160328
Release date: April 2016
Document generated: May 6, 2016 (11:02:09)
# Table of Contents

**Introduction** .................................................................................................................. 4

  About Deep Security ...................................................................................................... 5

**Preparation** .................................................................................................................. 7

  Installation Checklist ..................................................................................................... 8
  Deep Security Licensing on Azure Marketplace .............................................................. 9
  Check Permissions and Communication ........................................................................ 10
  Database Considerations ................................................................................................ 11

**Installation** .................................................................................................................. 12

  Creating a Deep Security Manager VM .......................................................................... 13
  Add Azure Resources to Deep Security Manager ............................................................ 15
  Installing Deep Security Agents .................................................................................... 17

**Appendices** ................................................................................................................ 28

  System Requirements .................................................................................................... 29
  Deep Security Manager Performance Features .............................................................. 31
  Creating an SSL Authentication Certificate ..................................................................... 32
  Connecting to your virtual machine via SSH ................................................................. 34
  Managing trusted certificates ......................................................................................... 35
  Uninstalling Deep Security ........................................................................................... 37
Introduction
About Deep Security

Deep Security is designed to run on and with Azure virtual machines. It provides advanced server security for physical, virtual, and cloud servers, makes it fast and easy to secure Azure and virtual, private, cloud virtual machines. 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 Azure environment.

Protection Modules

Anti-Malware

Provides agent-based anti-malware to protect physical servers, Hyper-V and Xen-based virtual servers, public cloud servers as well as virtual desktops.

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**

Dets 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 virtual machine. 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 a virtual machine.

**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](https://ossec.net).

**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.
Preparation
# Installation Checklist

Complete the tasks in this checklist to install Deep Security

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Details</th>
<th>Done</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Decide which type of licensing you will use</td>
<td>Deep Security Licensing on Azure Marketplace (page 9)</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Check that permissions, ports, and other settings are configured properly</td>
<td>Check Permissions and Communication (page 10)</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Perform the initial basic Deep Security system configuration that is required before you can start protecting your computer resources.</td>
<td>See &quot;Quick Start: System Configuration&quot; in the Deep Security Manager Help or Administrator's Guide.</td>
<td></td>
</tr>
</tbody>
</table>

Deep Security Licensing on Azure Marketplace

On the Azure 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. If you are using this type of license, you will need to enter the License string/activation code in the Deep Security Manager console (under Administration > Licenses) after it is installed.

- **PPU**: Pay-Per-Use (PPU) enables customers to pay based on the size of the Azure virtual machine they create. With PPU, each virtual machine type has an associated seat count limit (the seat count is the number of Deep Security Agents that you can activate). You can run more than one virtual machine to increase your seat count limit. These are the seat count limits for each type of virtual machine supported for Deep Security Manager:
  - **D2_V2**: Up to 25 Agents
  - **D3_V2**: Up to 50 Agents
  - **D4_V2**: Up to 100 Agents
  - **D5_V2**: Up to 200 Agents

As you create or stop 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.
Check Permissions and Communication

Azure AD Account Credentials

You will need to know your Azure account credentials and the account must have the Global Administrator role.

SMTP Server

If you want to sent alert emails, you will need an SMTP server. The Deep Security Manager 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.

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 31).
Database Considerations

Before installing Deep Security Manager, you must have a database installed. If you do not already have an Azure database, Azure Marketplace will create a new Azure SQL database virtual machine.

**Note:** You must configure your database firewall. The default firewall setting allows all ranges of Azure IP addresses to access the database, so you should limit the configuration to allow only Deep Security Manager web servers to access the database.

General Considerations

Database Sizing

See Azure SQL Database resource limits for information on database sizing.

Transport Protocol

The recommended transport protocol is **TCP**.

High Availability and Size

You can use the Azure portal to change the database size or High Availability mode after creating it with Azure Marketplace.
Installation
Creating a Deep Security Manager VM

Create a Deep Security Manager VM

1. Log in to your Azure portal and click the Marketplace blade.
3. Click the version of Deep Security you want to use from the search results:
   - **Deep Security Manager (BYOL):** This version is for customers who have already obtained a license to use Deep Security from another source. 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.
   - **Deep Security Manager:** This version enables customers to pay based on the size of the Azure virtual machine they create. With this pricing model, each virtual machine type has an associated seat count limit (the seat count is the number of Deep Security Agents that you can activate). You can run more than one virtual machine to increase your seat count limit. The seat count limits for each type of virtual machine supported for Deep Security are as follows:
     - D2 v2: up to 25 Agents
     - D3 v2: up to 50 Agents
     - D4 v2: up to 100 Agents
     - D5 v2: up to 200 Agents

As you create or stop Deep Security Manager nodes, the seat count usage for the hour is recalculated. To check your seat count limit after installing Deep Security Manager, open the Deep Security Manager console and go to Administration > Licenses.

4. Review the pricing information and click Create.
5. Follow the seven steps of the Create Deep Security Manager journey to create a Deep Security virtual machine.
   a. Specify the name of the Deep Security Manager VM and configure other general settings on the Basics blade and then click OK.
      - The credentials you specify in this blade are what you will use to log on to the Deep Security Manager virtual machine.
      - Depending on the type of authentication you select, you have to enter a strong password or an SSH public key.
      - Type in a name into Resource group to create a new Resource group or click Select existing to use an existing one.
      - Select an Azure region from the Location list.
   b. Select a virtual machine size, configure the Deep Security Manager URL and ports on the Deep Security Manager VM blade, and then click OK.
      - You will use the DNS name you enter in Deep Security Manager URL (for example, azurevmdemo01) and the port you specify as the Deep Security Manager console port (for example, 443) to access and log into Deep Security Manager (for example, https://azurevmdemo01.eastus.cloudapp.azure.com:443).
      - The heartbeat port is used by the Deep Security Agents to communicate with Deep Security Manager.
   c. Create a new database or enter the name of an existing one on the Database Settings blade and then click OK.
      - Do not type anything into Database Hostname if you create a new database. However, if you click Use Existing then the database hostname is required.
      - You can view the names of existing Azure SQL databases by going to the SQL databases blade and viewing the properties of a database (Settings blade > Properties blade > Server name).
   d. Enter the name of the administrator account you will use to sign in to the Deep Security Manager console on the Deep Security Credentials blade and enter and confirm the password for that account and click OK.
6. When installation has completed, open a browser and go to the following address:

https://[DNS_name]:8443

The DNS name is the name you specified on the Deep Security Manager blade (for example, azurevmdemo01.eastus.cloudapp.azure.com). You can view the DNS name for your Deep Security virtual machine by clicking the value in Public IP address/DNS name label in the Settings blade.

7. If installation is successful, you will be redirected to the Deep Security Manager console. If installation fails, you will see an error message. If this happens, click Install Deep Security Manager again and verify all settings as you step through the installation again.
Add Azure Resources to Deep Security Manager

Once you have added your Azure cloud account to Deep Security Manager, the virtual machines in the account are managed like any computer on a local network.

Before importing cloud resources into Deep Security Manager, you must confirm that your Azure account is assigned as a Global Administrator role.

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

Assign administrator roles

For instructions, see the “Assign or remove administrator roles” procedure on the Assigning administrator roles in Azure Active Directory page in the Azure documentation.

Add your Azure cloud account to Deep Security

You can also think of this as importing your Azure VMs into Deep Security.

1. Sign in to Deep Security Manager and click the **Computers** tab.
2. Click **New > Add Cloud Account**.
3. Select **Azure** as the Cloud Provider and click **Next**.
4. Enter the account credentials used to log in to the Azure portal and click **Signin**.

**Note:** The account must be the global administrator of the default Azure Active Directory.

5. Click **Accept** on the Deep Security Connector permissions page.
6. Select the **Azure Active Directory** and **Subscription Name** and click **Next**.
7. Review the summary information and click **Finish**. After the Azure VM has been imported, it will appear on the Computers page of the Deep Security Manager console.

Add the Deep Security extension to your Azure VM

When you create an Azure virtual machine, you can add the Trend Micro Deep Security Agent to your virtual machine in the Extensions setting. This installs the Deep Security Agent software and also registers the Deep Security Agent with the Deep Security Manager.

1. Log in to the Azure portal, click the VM you want to protect with Deep Security in the Virtual Machines blade, and click **All Settings**.
2. Click **Extensions** in the Settings blade, click **+Add extension in the Extensions blade**, select **Trend Micro Deep Security** in the New Resource blade, and then click **Create**.
3. Enter the required information for the extension and then click **OK**:
   - **Manager Address:** The DNS name of the Azure Marketplace Deep Security Manager.
   - **Activation Port:** The heartbeat port of the Azure Marketplace Deep Security Manager.
   - **Tenant Identifier:** This is not applicable to Deep Security VM for Azure Marketplace, so type NA here.
   - **Tenant Activation Password:** This is not applicable to Deep Security VM for Azure Marketplace, so type NA here.
• **Security Policy Identifier (optional):** The policy ID or name in your Deep Security Manager that you want to assign to this Azure VM. It is displayed in the deployment script generated by Deep Security Manager.
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 (the .msi or the .rpm file) on its own to install the Deep Security Agent. If you extract the full Agent zip package and then run the Agent installer from the same folder that holds the other zipped Agent components, all the Security Modules will be installed (but not turned on). If you use the Agent installer, individual Modules will be downloaded from Deep Security Manager and installed on an as-needed basis, minimizing the impact on the local computer.

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

### Installing the Windows Agent

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

   **Note:** On Windows Server 2012 R2 Server Core, you must launch the installer using this command: `msiexec /i Agent-Core-Windows-9.6.x-xxxx.x86_64.msi`

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

2. **End-User License Agreement:** If you agree to the terms of the license agreement, select I accept the terms of the license agreement and click Next
3. **Destination Folder**: Select the location where you would like Deep Security Agent to be installed and click **Next**.

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

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

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

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

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

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

   sudo dpkg -i <installer file>

Starting, stopping and resetting the Agent on Linux:

Command-line options:

To start the Agent:

   /etc/init.d/ds_agent start

To stop the Agent:

   /etc/init.d/ds_agent stop

To reset the Agent:

   /etc/init.d/ds_agent reset

To restart the Agent:

   /etc/init.d/ds_agent restart

Installing Agents on Other Operating Systems

For instructions on installing Agents on Solaris, HP-UX, or AIX, see "Installation Guide (Basic Components)" on the Trend Micro documentation page.
Deploying Deep Security Agents on your Azure Virtual Machines

The next step is to deploy Deep Security Agents to protect your Azure virtual machines. There are five ways that you can deploy Deep Security Agents:

- Generate a deployment script and run it to deploy a Deep Security Agent on an existing virtual machine.
- Add a custom script extension on the Azure portal on an existing virtual machine.
- Use a PowerShell script to install the Deep Security Extension on an existing virtual machine.

Each of these methods is described below.

Add Deep Security Extension

When you create an Azure virtual machine, in Extensions setting, you can add Trend Micro Deep Security Agent to your virtual machine. This installs the Deep Security Agent software and also registers the Agent with the Deep Security Manager.

1. Log in to the Azure portal, click the VM you want to protect with Deep Security in the Virtual Machines blade, and click All Settings.
3. Enter the required information for the extension and then click OK:
   - Manager Address: The DNS name of the Azure Marketplace Deep Security Manager.
   - Tenant Identifier: This is not applicable to Deep Security VM for Azure Marketplace, so type n/a here.
   - Tenant Activation Password: This is not applicable to Deep Security VM for Azure Marketplace, so type n/a here.
   - Security Policy Identifier (optional): The policy ID or name in your Deep Security Manager that you want to assign to this Azure VM. It is displayed in the deployment script generated by Deep Security Manager.

Generate a deployment script

To facilitate the creation of deployment scripts, Deep Security provides a wizard that generates a deployment script based on options that you choose. You can generate deployment scripts for use in deployment tools like RightScale, Chef, Puppet, and custom scripts to automate the protection of new VMs.

2. Select the platform to which you are deploying the software.
3. Select Activate Agent automatically after installation. (Deep Security 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 Azure VMs. Copy the script and save it into powershell (.ps1) or bash shell script (.sh) file.

Note: Do not copy <powershell> and </powershell> tags in the script for windows platform.

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-ExcecutionPolicy RemoteSigned
```
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.

Run the deployment script on an existing virtual machine

If you have a virtual machine that is already up and running, you can run the deployment script as a shell script or batch file on that VM.

For example, log into your Windows VM using Remote Desktop, open the PowerShell application, and right-click to paste the deployment script.

Add the custom script extension to existing virtual machine

If you have a virtual machine that is already up and running, this is another option available to deploy and activate the Deep Security Agent.

Navigate to your existing virtual machine in the Azure management portal. Use the steps below to upload and execute the deployment script on your Azure VM.

1. Log in to Azure portal, then switch to preview portal, click the virtual machine that you want to add custom script, and in the virtual machine blade, click All settings.
2. In the Settings blade, click Extensions, then in the Extensions blade, click +Add.
3. In the New resource blade, select Custom Script, then in the Custom Script blade, click Create.
4. In the Add Extension blade, in Script File (required) field, click the upload button to select the saved deployment script (in .ps1 format), then click OK.

Use PowerShell Script to install Deep Security Extension on an existing virtual machine

To automate the process of installing the Deep Security Agent, you can use the PowerShell script below, along with a customized JSON format config file to install the Agent on an existing virtual machine.

Note: The PowerShell scripts listed below are based on Azure cmdlets version 0.9.x. The command names may be different in another Azure cmdlets version.

1. Open Azure Powershell.
2. Ensure you have set up the proper authentication to your Azure subscription for the Powershell commands to work.
3. Copy the text below to a text file named "public.config":

   ```json
   {
   "DSMname": "<your Deep Security Manager URL in the Deep Security Manager VM blade>",
   "DSMport": "<4120 or your heartbeat port in the Deep Security Manager VM blade>",
   "policyNameorID": "<appropriate policy ID or policy name>"
   }
   ```

4. Customize the content of the public.config file if you want to choose a custom policy to deploy. Copy these Powershell commands into a text file on your local hard drive and save it with a .ps1 extension.
5. Copy the text below to a text file named "private.config":

   ```json
   {
   "tenantID": "NA",
   "tenantPassword": "NA"
   }
   ```
6. Customize the content of the `private.config` file with your TenantID and Tenant Password. Copy these Powershell commands into a text file on your local hard drive and save it with a .ps1 extension.

7. Copy the appropriate set of text below:

**Azure PowerShell script for installing Deep Security VM extension for classic (ASM) virtual machine (Windows):**

```powershell
$jsonPrivate=Get-Content -Raw -Path "private.config"
$jsonPublic=Get-Content -Raw -Path "public.config"
$dsaExtName="TrendMicroDSA"
$nameSpace="TrendMicro.DeepSecurity"
Switch-AzureMode AzureServiceManagement
$dsaExtVersion =(Get-AzureVMAvailableExtension -ExtensionName $dsaExtName –Publisher $nameSpace ).Version
$vmname="<your VM name>"
$servicename="<your cloud service name without the '.cloudapp.net' suffix>"
$vm=Get-AzureVM -ServiceName $servicename -Name $vmname
Set-AzureVMExtension -VM $vm.VM -Version $dsaExtVersion -ExtensionName $dsaExtName `-Publisher $nameSpace ` -PrivateConfiguration $jsonPrivate `-PublicConfiguration $jsonPublic
Update-AzureVM -ServiceName $servicename -Name $vmname -VM $vm.VM
```

**Azure PowerShell script for installing Deep Security VM extension for classic (ASM) virtual machine (Linux):**

```powershell
$jsonPrivate=Get-Content -Raw -Path "private.config"
$jsonPublic=Get-Content -Raw -Path "public.config"
$dsaExtName="TrendMicroDSALinux"
$nameSpace="TrendMicro.DeepSecurity"
Switch-AzureMode AzureServiceManagement
$dsaExtVersion =(Get-AzureVMAvailableExtension -ExtensionName $dsaExtName –Publisher $nameSpace ).Version
$vmname="<your VM name>"
$servicename="<your cloud service name without the '.cloudapp.net' suffix>"
$vm=Get-AzureVM -ServiceName $servicename -Name $vmname
Set-AzureVMExtension -VM $vm.VM -Version $dsaExtVersion -ExtensionName $dsaExtName `-Publisher $nameSpace ` -PrivateConfiguration $jsonPrivate `-PublicConfiguration $jsonPublic
Update-AzureVM -ServiceName $servicename -Name $vmname -VM $vm.VM
```

**Azure PowerShell script for installing Deep Security VM extension for Resource Manager (ARM) virtual machine (Windows):**

```powershell
$jsonPrivate=Get-Content -Raw -Path "private.config"
$jsonPublic=Get-Content -Raw -Path "public.config"
$dsaExtName="TrendMicroDSA"
Switch-AzureMode AzureServiceManagement
$dsaExtVersion =(Get-AzureVMAvailableExtension -ExtensionName $dsaExtName –Publisher $nameSpace ).Version
Switch-AzureMode AzureResourceManager
$resourceGroup="<resource group name>"
$vmname="<your VM name>"
$location="<vm location>"
$nameSpace="TrendMicro.DeepSecurity"
Set-AzureVMExtension -ResourceGroupName $resourceGroup -VMName $vmname `-Location $location `-TypeHandlerVersion $dsaExtVersion `-ExtensionType $dsaExtName `-NAME $dsaExtName `-Publisher $nameSpace `-ProtectedSettingString $jsonPrivate `-SettingString $jsonPublic
```

**Azure PowerShell script for installing Deep Security VM extension for Resource Manager (ARM) virtual machine (Linux):**

```powershell
$jsonPrivate=Get-Content -Raw -Path "private.config"
$jsonPublic=Get-Content -Raw -Path "public.config"
$dsaExtName="TrendMicroDSALinux"
Switch-AzureMode AzureServiceManagement
$dsaExtVersion =(Get-AzureVMAvailableExtension -ExtensionName $dsaExtName –Publisher $nameSpace ).Version
Switch-AzureMode AzureResourceManager
```
Use Azure Command-Line Interface (CLI) to install Deep Security Extension on an existing virtual machine

To automate the process of installing the Deep Security Agent, you can use the Azure Command-Line (CLI) below, along with a customized JSON format config file to install the Agent on an existing virtual machine.

**Note:** The Azure Command-Line (CLI) listed below are based on Azure cmdlets version 0.9.x. The command names may be different in another Azure cmdlets version.

**Note:** For more details about how to install Azure Command-Line, please refer to Install the Azure CLI.

2. Ensure you have set up the proper authentication to your Azure subscription for the CLI commands to work.
3. Copy the text below to a text file named "public.config":

   ```
   {
   "DSMname": "<your Deep Security Manager URL in the Deep Security Manager VM blade>",
   "DSMport": "<4120 or your heartbeat port in the Deep Security Manager VM blade>",
   "policyNameorID": "<appropriate policy ID or policy name>",
   }
   ```

4. Customize the content of the private.config file with your TenantID and Tenant Password.
5. Copy the text below to a text file named "private.config":

   ```
   {
   "tenantID": "NA",
   "tenantPassword": "NA"
   }
   ```

6. Customize the content of the private.config file with your TenantID and Tenant Password. Copy these Powershell commands into a text file on your local hard drive and save it with a .ps1 extension.
7. Use the appropriate set of commands (below) to add the Deep Security VM extension. There are separate instructions for ASM and ARM VMs.

**Azure Command-Line for installing Deep Security VM extension for classic (ASM) virtual machine:**

1. Log in to Azure account:
   ```command
   azure login -u < azure log in account > -p < azure log in password>
   ```
2. Set subscription ID:
   ```command
   azure account set <subscription id>
   ```
3. Set mode of classic (v1) operation:
azure config mode arm

4. Get extension version:

5. Add extension:

| Note: | <Extension Version> is formatted as major.minor, for example, 9.6 |

### Azure Command-Line for installing Deep Security VM extension for Resource Manager (ARM) virtual machine:

1. Log in to Azure account:
   azure login -u < azure log in account > -p < azure log in password>

2. Set subscription ID:
   azure account set <subscription id>

3. Set mode of Resource Manager (ARM) operation:
   azure config mode arm

4. Get extension version:

5. Add extension:

| Note: | <Extension Version> is formatted as major.minor, for example, 9.6 |

### Iptables on Linux

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

### Activating the Agent

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

**To activate the newly installed Agent:**

1. In the Deep Security Manager, go to the Computers page and click New > New Computer... to display the New Computer Wizard.
2. Enter the hostname or IP address of the computer. If you want to use the Agent to provide protection for the host computer as well as function as a Relay, select a Deep Security Policy from the **Policy** menu. Otherwise leave **Policy** set to "None".

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

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

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

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

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

To enable Relay functionality:

1. In the Deep Security Manager, go to the Computers page, double-click the computer with the newly-activated Agent to display its Details editor window.

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

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

Considerations for Windows 2012 Server Core

There are a few things you should keep in mind when running a Deep Security Agent with Windows 2012 Server Core:

- Deep Security does not support switching the Windows 2012 server mode between Server Core and Full (GUI) modes after the Deep Security Agent is installed.

- If you are using Server Core mode in a Hyper-V environment, you will need to use Hyper-V Manager to remotely manage the Server Core computer from another computer. When the Server Core computer has the Deep Security Agent installed and Firewall enabled, the Firewall will block the remote management connection. To manage the Server Core computer remotely, turn off the Firewall module.

- Hyper-V provides a migration function used to move a guest VM from one Hyper-V server to another. The Deep Security Firewall module will block the connection between Hyper-V servers, so you will need to turn off the Firewall module to use the migration function.
Appendices
System Requirements

Deep Security Manager

Deep Security Manager is available as an Azure Marketplace Linux virtual machine.

- **Web Browser:** Firefox 38+, Internet Explorer 9.x, Internet Explorer 10.x, Internet Explorer 11.x, Chrome 43+, Safari 6+. (Cookies enabled.)
  - **Monitor:** 1024 x 768 resolution at 256 colors or higher

Database

Deep Security Manager requires a database. Azure Marketplace will create an Azure SQL database virtual machine. For additional information, see *Database Considerations (page 11).*

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) - Full Server or Server Core with latest service pack or patch
  - Windows 8.1 (32-bit and 64-bit) with latest service pack or patch
  - Windows 8 (32-bit and 64-bit) with latest service pack or patch
  - Windows 7 (32-bit and 64-bit) with latest service pack or patch
  - Windows Server 2008 (32-bit and 64-bit), Windows Server 2008 R2 (64-bit) with latest service pack or patch
  - Windows Vista (32-bit and 64-bit) with latest service pack or patch
  - Windows Server 2003 SP2 (32-bit and 64-bit) with latest service pack or patch
  - Windows Server 2003 R2 SP2 (32-bit and 64-bit) with latest service pack or patch
  - Windows XP (32-bit and 64-bit) with latest service pack or patch
  - **With Relay functionality enabled:** All 64-bit Windows versions above

- **Linux:**
  - Red Hat 5 (32-bit and 64-bit)
  - Red Hat 6 (32-bit and 64-bit)
  - Red Hat 7 (64-bit)
  - Oracle Linux 5 (32-bit and 64-bit)
- Oracle Linux 6 (32-bit and 64-bit)
- Oracle Linux 7 (64-bit)
- CentOS 5 (32-bit and 64-bit)
- CentOS 6 (32-bit and 64-bit)
- Debian 6 (64-bit)
- Debian 7 (64-bit)
- SUSE 10 SP3 and SP4 (32-bit and 64-bit)
- SUSE 11 SP1, SP2, and SP3 (32-bit and 64-bit)
- SUSE 12 (64-bit)
- CloudLinux 5 (32-bit and 64-bit)
- CloudLinux 6 (32-bit and 64-bit)
- CloudLinux 7 (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 9.6 SP1 Supported Features and Platforms. For a list of specific Linux kernels supported for each platform, see the document titled Deep Security 9.6 SP1 Supported Linux Kernels.

### Deep Security Notifier System Requirements

- **Windows:**
  - Windows Server 2012 R2 (64-bit) with latest service pack or patch
  - Windows Server 2012 (64-bit) with latest service pack or patch
  - Windows 8.1 (32-bit and 64-bit) with latest service pack or patch
  - Windows 8 (32-bit and 64-bit) with latest service pack or patch
  - Windows 7 (32-bit and 64-bit) with latest service pack or patch
  - Windows Server 2008 R2 (64-bit) with latest service pack or patch
  - Windows Server 2008 (32-bit and 64-bit) with latest service pack or patch
  - Windows Vista (32-bit and 64-bit) with latest service pack or patch
  - Windows Server 2003 SP2 (32-bit and 64-bit) with latest service pack or patch
  - Windows Server 2003 R2 (32-bit and 64-bit) with latest service pack or patch
  - Windows XP (32-bit and 64-bit) with latest service pack or patch
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 authentication certificate in a Linux environment:**

1. Go to the Deep Security Manager installation directory (for the purpose of these instructions, we will assume it's "opt/dsm") and create a new folder called Backupkeystore
2. Copy .keystore and configuration.properties to the newly created folder Backupkeystore
3. From a command prompt, go to the following location: opt/dsm/jre/bin
4. Run the following command, which will create a self-signed certificate:
   ```bash
   opt/dsm/jre/bin# keytool -genkey -alias tomcat -keyalg RSA -dname cn=dsmserver
   ```
   **Note:** 
   - `dname` is the common name of the certificate your CA will sign. Some CAs require a specific name to sign the Certificate Signing Request (CSR). Please consult your CA Admin to see if you have that particular requirement.
5. When prompted, enter a password.
6. There is a new .keystore file created under the user home directory. If you are logged in as "Administrator", You will see the .keystore file under "/root/
   
   If the file is hidden, use the following command: `find -type f -iname ".keystore" -ls`
7. View the newly generated certificate using the following command:
   ```bash
   opt/dsm/jre/bin# keytool -list -v
   ```
8. Run the following command to create a CSR for your CA to sign:
   ```bash
   opt/dsm/jre/bin# keytool -certreq -keyalg RSA -alias tomcat -file certrequest.csr
   ```
   If you see "Keytool unrecognized option "-keyalg"", use `sigalg` instead.
9. Send the certrequest.csr to your CA to sign. In return you will get two files. One is a "certificate reply" and the second is the CA certificate itself.
10. Run the following command to import the CA cert into the Java trusted keystore:
    ```bash
        /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:
    ```bash
        /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:
    ```bash
        /opt/dsm/jre/bin/keytool -import -alias tomcat -file certreply.txt
    ```
13. Run the following command to view the certificate chain in you keystore:

```bash
opt/dsm/jre/bin# keytool -list -v
```

14. Copy the .keystore file from your home directory to `/opt/dsm/`

```bash
cp $HOME/.keystore /opt/dsm/.keystore
```

15. Open the `opt/dsm/configuration.properties` file. It will look something like:

```properties
keystoreFile= opt/dsm/.keystore
port=443
keystorePass=xxxx
installed=true
serviceName= Trend Micro Deep Security Manager
```

16. Replace the password in the following string:

```properties
keystorePass=xxxx
```

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

17. Save and close the file.


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

---

**Note:** You will need to log in to your virtual machine, using trend as the userid and the SSH key associated with the virtual machine.
Connecting to your virtual machine via SSH

The Azure Marketplace version of Deep Security Manager is installed on CentOS.

Note that the username for the Deep Security Manager virtual machine is created by Azure during the launching of Azure Marketplace.
Managing trusted certificates

Importing trusted certificates

You can import trusted certificates for code signing and SSL connections other than Amazon Web Services into the system using the Deep Security Manager.

If you are importing a trusted certificate to establish trust with an Amazon Web Services region, you must use the dsm_c command-line tool.

To import a trusted certificate using the Deep Security Manager:
1. In the Deep Security Manager, go to Administration > System Settings > Security.
2. Under Trusted Certificates, click View Certificate List to view a list of all security certificates accepted by Deep Security Manager.
3. Click Import From File... to start the Import Certificate wizard.

To import a trusted certificate using dsm_c:
1. On the Deep Security Manager server, run the following command:
   
   ```
   dsm_c -action addcert -purpose PURPOSE -cert CERTFILE
   ```
   
   where the parameters are:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Sample value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PURPOSE</td>
<td>What type of connections the certificate will be used for. This value must be selected from one of the sample values listed on the right.</td>
<td>AWS - Amazon Web Services, DSA - code signing, SSL - SSL connections</td>
</tr>
<tr>
<td>CERTFILE</td>
<td>The (user-defined) name of the file containing the certificate you want to import.</td>
<td>/path/to/cacert.pem</td>
</tr>
</tbody>
</table>

   Note: If you are running the Deep Security Manager in a Linux environment, you will need to run the dsm_c command as the root user.

Viewing trusted certificates

You can view trusted certificates for code signing and SSL connections other than Amazon Web Services using the Deep Security Manager.

To view trusted certificates for Amazon Web Services connections, you must use the dsm_c command-line tool.

To view trusted certificates using the Deep Security Manager:
1. In the Deep Security Manager, go to Administration > System Settings > Security.
2. Under Trusted Certificates, click View Certificate List.

To view trusted certificates using dsm_c:
1. On the Deep Security Manager server, run the following command:
   
   ```
   dsm_c -action listcerts [-purpose PURPOSE]
   ```
   
   The -purpose PURPOSE parameter is optional and can be omitted to see a list of all certificates. If you specify a value for PURPOSE, then only the certificates used for that purpose will be shown.
Removing trusted certificates

You can remove trusted certificates for code signing and SSL connections other than Amazon Web Services using the Deep Security Manager.

To remove trusted certificates for Amazon Web Services connections, you must use the dsm_c command-line tool.

To remove a trusted certificate using the Deep Security Manager:

1. In the Deep Security Manager, go to Administration > System Settings > Security.
2. Under Trusted Certificates, click View Certificate List.
3. Select the certificate you want to remove and click Delete.

To remove a trusted certificate using dsm_c:

2. Run the following command:

   ```
   dsm_c -action listcerts [-purpose PURPOSE]
   ```

   The `-purpose` `PURPOSE` parameter is optional and can be omitted to see a list of all certificates. If you specify a value for `PURPOSE`, then only the certificates used for that purpose will be shown.

3. Find the `ID` value for the certificate you want to remove in the list.
4. Run the following command:

   ```
   dsm_c -action removecert -id ID
   ```

   The `ID` parameter value is required.

Note: If you are running the Deep Security Manager in a Linux environment, you will need to run the `dsm_c` commands as the root user.
Uninstalling Deep Security

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

To uninstall the Relay-enabled Agent

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

To uninstall the Relay-enabled Agent (Windows)

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

**To uninstall from the command line:**

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

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

To uninstall the Relay-enabled Agent (Linux)

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

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

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

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

To uninstall the Deep Security Agent

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

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

To uninstall from the command line:

msiexec /x <package name including extension>

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

To uninstall the Deep Security Agent (Linux)

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

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

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

For Ubuntu:

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

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

Enter the following:

```
pkgrm ds-agent
```

(Note that uninstall may require a reboot.)

To uninstall the Deep Security Agent (Solaris 11)

Enter the following:

```
pkg uninstall ds-agent
```

(Note that uninstall may require a reboot.)

To uninstall the Deep Security Agent (AIX)

Enter the following:

```
installp -u ds_agent
```

To uninstall the Deep Security Agent (HP-UX)

Enter the following:

```
swremove ds_agent
```
To uninstall the Deep Security Notifier

To uninstall the Deep Security Notifier (Windows)

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

To uninstall from the command line:

msiexec /x <package name including extension>

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

To uninstall the Deep Security Manager

To uninstall the Deep Security Manager (Windows)

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

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

<installation folder>\Uninstall.exe

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

<installation folder>\Uninstall.exe -q

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

To uninstall the Deep Security Manager (Linux)

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

Uninstall

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

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

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

rm -rf <installation location>

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