Trellix MOVE AntiVirus 4.10.x Installation Guide

Contents

Multi-platform

Installation overview

Installation overview

The Multi-platform deployment removes the need to install an antivirus application on every VM, and it is the original agent-based deployment option.

The Multi-platform deployment option offloads all scanning to a dedicated VM — an SVM — that runs **Endpoint Security Threat Prevention** software. Guest VMs are no longer required to run antivirus software locally, which improves performance for antivirus scanning, and increases VM density per hypervisor.

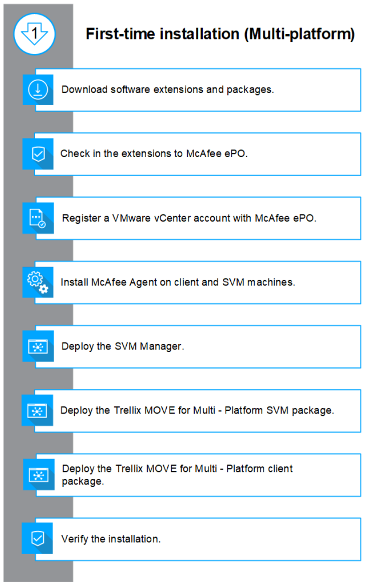
The Multi-platform deployment option:

- Uses **Trellix ePO - On-prem** to manage the **Trellix MOVE AntiVirus** configuration on the client systems, SVM, and SVM Manager.
- Uses the **Trellix Agent** for policy and event handling.
- Uses **Trellix ePO - On-prem** for reports on viruses that are discovered on the VMs.
- Uses **Trellix® Threat Intelligence Exchange (TIE)** and **Trellix Intelligent Sandbox** technologies to perform in-depth analysis of suspect files (using local, global, and enterprise-level caches), define threat reputation and take the required actions.

First-time installation workflow (Multi-platform)

To install and configure the **Trellix MOVE for Multi-Platform** environment, see the first-time installation high-level workflow diagram shown below:

First-time installation (Multi-platform) workflow diagram



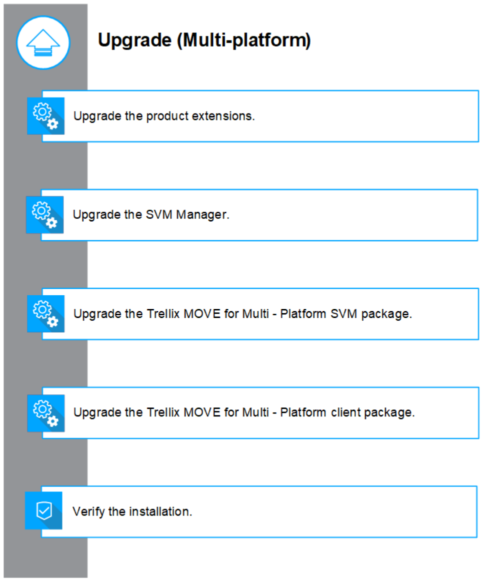
First-time installation (Multi-platform)

- Download software extensions and packages.
- Check in the extensions to McAfee ePO.
- Register a VMware vCenter account with McAfee ePO.
- Install McAfee Agent on client and SVM machines.
- Deploy the SVM Manager.
- Deploy the Trellix MOVE for Multi - Platform SVM package.
- Deploy the Trellix MOVE for Multi - Platform client package.
- Verify the installation.

Upgrade installation workflow (Multi-platform)

To upgrade the **Trellix MOVE for Multi-Platform** software and remain updated with the new features, see the **Upgrade (Multi-platform) workflow diagram** shown below:

Upgrade (Multi-platform) workflow diagram



Upgrade (Multi-platform)

- Upgrade the product extensions.
- Upgrade the SVM Manager.
- Upgrade the Trellix MOVE for Multi - Platform SVM package.
- Upgrade the Trellix MOVE for Multi - Platform client package.
- Verify the installation.

Planning your installation

System and hardware requirements

Make sure that each of your guest VMs is running a supported version of Microsoft Windows and confirms to these requirements

Hypervisor requirements

All hypervisors are supported, but only those listed were tested.

- VMware ESXi 6.0 or later
- Citrix XenServer 6.0 or later
- Microsoft 2012 R2 Hyper-V or later
- Nutanix AHV 20170830.395 or later

SVM requirements

The **SVM** requires a dedicated virtual machine with **McAfee® Endpoint Security Threat Prevention** November 2021 update or above installed.

Note

You need to first deploy **Trellix Agent**, followed by **Endpoint Security** software and then **MOVE SVM** package.

The virtual machine must meet these requirements:

Operating system	• Windows Server 2012 R2 (64-bit) • Windows Server 2016 • Windows Server 2019 • Windows Server 2022
Note: Make sure that the Windows security updates are up to date.	
CPU	CPU 4 vCPU, 2 GHz or higher
Memory	6-GB RAM or higher
Allotted space for MOVE AntiVirus deployment	8 GB or higher
IP address requirements	Static IP address (required for configuring policies with IP address)

Note: Trellix MOVE AntiVirus requires Microsoft Visual C++ 2019 Runtime and it is bundled with SVM package.	

SVM Manager requirements

Important

It is recommended to keep SVM on the same host where most of the clients are located, it improves the performance of the SVM.

CPU	2 vCPU
Memory	2-GB RAM or higher
Hard disk space for SVM Manager deployment	16 GB or higher
Note: SVM Manager is shipped as an OVF package (Linux, Ubuntu 18.04 (64-bit)) and comes preinstalled with the required software.	

Client system requirements

The **Trellix MOVE AntiVirus** client software requires a **Trellix Agent** for one of these operating **Trellix MOVE AntiVirus** systems:

Note

Trellix MOVE AntiVirus (Multi-platform) requires Microsoft Visual C++ 2019 Runtime and it is bundled with client package.

Supported Operating Systems
Windows 8.1 (32-bit and 64-bit)
Windows 10 (32-bit and 64-bit)

Supported Operating Systems
Windows Server 2008 R2 SP1
Windows Server 2012 R2
Windows Server 2016
Windows Server 2019
Windows 11
Windows Server 2022

Supported Trellix management platform and software

You must have specific versions of **Trellix** management platform and software installed.

Software	Versions
Trellix ePO - On-prem For details, see *T**Trellix ePO - On-prem** Installation Guide*.	5.10.0 Update 11 or later
vSphere Connector Extension	5.4.x or later
Trellix Agent	5.7.4 or later
McAfee® Endpoint Security Threat Prevention	ENS 10.7.0 November 2021 Update or later
McAfee® Endpoint Security for Linux Threat Prevention	10.7.1 (Part of SVM Manager package)
Trellix® Threat Intelligence Exchange (TIE)	3.0 or later
Trellix Intelligent Sandbox	3.6.1, 3.6.2, 3.8.0, or 4.0.0

Software	Versions
Virtual **Intelligent Sandbox** (vATD)	3.10
McAfee® Data Exchange Layer (DXL)	6.0.0 or later **Note:** Use the **McAfee® Data Exchange Layer (DXL)** version that is compliant with **Threat Intelligence Exchange**.

Ports for Multi-platform deployment

Following are the ports that are open and not reserved for other purposes:

System connections	Default ports
Trellix ePO - On-prem to vCenter communication	TCP 443
Communication between **Trellix Agent** and **Trellix ePO - On-prem**	TCP 8081
Communication between SVA Manager and the SVM	TCP 8443
Communication between SVA Manager and the client	TCP 8080
Communication between the client and the SVM	TCP 9053
GTI lookup - DNS	TCP 53

Note

If required, you can customize the default ports.

Installation prerequisites

Begin the installation once the environment meets the specified requirements.

Components	Requirements
All systems where you want to install the product	• Hardware components meet or exceed minimum requirements. • Supported Windows operating system is installed.
Managed systems only	Required **Trellix Agent** or software installed and communicating with the **Trellix ePO - On-prem** server.
Trellix ePO - On-prem server	Supported management platform is installed.

Pre-installation tasks

Pre-installation tasks

You can check-in the software and extensions on **Trellix ePO - On-prem** server in either ways:

- Manually download software extensions and packages and check-in to **Trellix ePO - On-prem** server
- Check-in the extensions and packages to **Trellix ePO - On-prem** using **Trellix ePO - On-prem** Software Catalog

Note

In the **Trellix ePO - On-prem** version 5.10.0 and above, the term Software Manager is identified as Software Catalog.

Download software extensions and packages

If not using Software Catalog, you can download these software extensions and product packages from the **Trellix** download site (https://www.trellix.com/en-us/downloads) and check in them to **Trellix ePO - On-prem** server.
The software package consists of **Trellix MOVE AntiVirus** extensions.

- MDCC_5.3.x.xx.zip
- VSPHEREDCEXTN_5.4.x.xx.zip
- DC__GS__4000_4.10.x.xx.zip
- DC__AM__4000_4.10.x.xx.zip
- MOVEAVLIC400_4.10.x.xx.zip

Note

Make sure that you download the required extensions and packages from the **Trellix** download site.

Check in the extensions and packages to Trellix ePO - On-prem manually

The **Trellix MOVE for Multi-Platform** extensions and **Endpoint Security** extensions must be installed on the **Trellix ePO - On-prem** server before you can manage **Trellix MOVE for Multi-Platform** on your virtual machines.

Before you begin

Make sure that the extension files are in an accessible location on the network.

Endpoint Security is only licensed for the SVM, not for other Windows systems in your environment.

(Optional) Install the **Endpoint Security for Linux** Threat Prevention extension to manage the **Endpoint Security for Linux** Threat Prevention policy on the SVM Manager. **Endpoint Security for Linux** Threat Prevention is only licensed for the SVM Manager, not for other Linux systems in your environment.

Note

Install the extensions **Trellix** Data Center Control, vSphere Connector Extension, and **Trellix MOVE AntiVirus** specific extensions (MOVE AntiVirus, MOVE AntiVirus Common) on the **Trellix ePO - On-prem** server manually. It also checks in the **Trellix MOVE AntiVirus** SVM and Client packages to the Main Repository.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **To check in the packages, select Menu → Software → Main Repository → Check In Package.**
3. **For File path, browse and select the individual packages as mentioned below, then click OK**

Package description	Package name
Endpoint Security Multi-platform client package	• **Endpoint_Security_Platform_10.7.x.xxxx.x_Client** • **Threat_Prevention_10.7.x.xxxx.x_Client**

4. **If you are using individual extensions instead of meta package, check in the extension and packages individually:**
   a. **Select Menu → Software → Extensions → Install Extension.**

      The Install Extension page opens.

   b. **Browse and select the extension files in the same order as mentioned below, then click Open → OK:**

Extension description	Extension name
Trellix MOVE AntiVirus extension	a. MDCC_5.3.x.xx.zip b. VSPHEREDCEXTN_5.4.x.xx.zip c. DC__GS__4000_4.10.x.xx.zip d. DC__AM__4000_4.10.x.xx.zip e. MOVEAVLIC400_4.10.x.xx.zip
Endpoint Security	• Endpoint_Security_Platform_10.7.x.xxx_Extension • Threat Prevention 10.7.x.xxx_Extension

c. Review the extension details and click OK.
d. To check in the packages, select Menu → Software → Main Repository → Check In Package.
e. For File path, browse and select the individual packages as mentioned below, then click OK:

Package description	Package name
Trellix MOVE for Multi-Platform package	• MOVE-AV_Offload_Scan_Server_4.10.x.xx.zip • MOVE-AV-MP_Client_Pkg_4.10.x.xx.zip
Endpoint Security Multi-platform client package	• Endpoint_Security_Platform_10.7.x.xxxx.x_Client • Threat_Prevention_10.7.x.xxxx.x_Client

Check in the extensions and packages to Trellix ePO - On-prem from Software Catalog

If you have Software Catalog, you can check in the software extensions and packages to the Main Repository without downloading them.

Task

1. Log on to Trellix ePO - On-prem as an administrator.
2. Select Menu → Software, then click Software Catalog.
3. From Software (by Label) → Endpoint Security, select these extensions, then click Check In.

Product	Component
Trellix MOVE AntiVirus 4.10.x	This main extension includes these extensions: • **Trellix MOVE AntiVirus** Common — Extension for product installation and deployment • **Trellix MOVE AntiVirus** — Extension for configuring and managing policies • **Trellix MOVE AntiVirus** License — License extension; upgrades evaluation extension to a fully licensed extension • vSphere Connector Extension — Data Center discovery software • **Trellix** Data Center Control — It is a dependency software for vSphere Connector Extension. • Multi-platform client package — It is a **Trellix MOVE AntiVirus** client package • Multi-platform SVM package — It is a **Trellix MOVE AntiVirus** SVM package • Multi-platform SVM Manager Debian package

Results

Note

All extensions and packages are checked in to the Main Repository from the Software Catalog.

You must download other **Trellix MOVE** Multi-Platform packages from the **Trellix** download site (http://www.trellix.com/us/downloads/).

Install Trellix MOVE AntiVirus

Register a VMware vCenter account with Trellix ePO - On-prem

To use **Trellix MOVE for Multi-Platform** to manage the security of the virtual machines in your data center, you must first add your VMware vCenter to the **Trellix ePO - On-prem** server.

Before you begin

Make sure that:

- You have configured your VMware vCenter server that manages the ESXi servers, which host the guest VMs.
- You have installed the **Trellix MOVE for Multi-Platform** software extension on the **Trellix ePO - On-prem** server.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**

2. **Select Menu → Configuration → Registered Cloud Accounts.**
3. **From the bottom-left click Actions → Add Cloud Account to open the Add Cloud Account dialog box.**
4. **From the Choose Cloud Provider drop-down list, select VMware vSphere and click OK.**
5. **On the vCenter Account Details page, configure these options.**

Note

You must have a vCenter Server user account with administrator rights to use the autoscale feature.

Option	Description
Account Name	A name for the VMware vCenter account in **Trellix ePO - On-prem**. Account names can include characters a–z, A–Z, 0–9, and [_.-], without space.
Server Address	(Required) IP address or the host name of the available VMware vCenter.
vCenter Username	(Required) User name of the available VMware vCenter account.
vCenter Password	(Required) Password of the available VMware vCenter account.
Sync Interval (In Minutes)	Specify the interval for running the next vCenter discovery (default value is 5 minutes).
Port	The port number required to establish the connection with the available VMware vCenter (default port is 443).
Tag	The administrator specifies this to identify the VMs. Tag name can include characters a–z, A–Z, 0–9, and [_.-], with space.

6. **Click Test Connection to validate VMware vCenter account details and verify the connection to the VMware vCenter, then click Next → Finish.**
7. **When prompted to confirm, click OK to register the vCenter account and wait for vCenter sync to complete.**

This action registers the VMware vCenter and imports all discovered virtual machines, which are unmanaged, into the System Tree. The instances are imported with the same organization as the VMware vCenter.

Note

The virtual machines that are already added and managed by **Trellix ePO - On-prem** are retained with the existing policy settings, but the virtualization properties for these systems are added.

Set up a general configuration for deployment

Before deploying **Trellix MOVE AntiVirus** SVM Manager, configure settings on the **Trellix ePO - On-prem** server, so that they are retrieved and used for every **Trellix MOVE AntiVirus** SVM Manager deployment.

Before you begin

Make sure that you have registered a VMware vCenter account with the **Trellix ePO - On-prem**.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Automation → MOVE AntiVirus Deployment.**
3. **In the Configuration tab, click General under General list.**

   The General Configuration page opens.
4. **Enter and confirm the password for Trellix ePO - On-prem Credentials section.**

   Trellix ePO - On-prem credentials

Options	Description
Password	Type the password of the **Trellix ePO - On-prem** console that the administrator has currently logged on
Confirm Password	Confirm the password

5. **Enter and confirm password for SVM (Agentless) and SVM Manager (Multi-Platform) Configuration section.**

Note

The **SVM (Agentless) and SVM Manager (Multi-Platform) Configuration** section shows a default password.

⚠ **Caution**

The password you enter is set to the SVM Manager and you can't update it once it is deployed. This password is not applicable to the SVM Manager, which is already deployed.

If required, change the password.

SVM (Agentless) and SVM Manager (Multi-platform) Configuration

Option	Description
Hostname Prefix (Agentless only)	Type a unique prefix that is added to the host name of the **Trellix MOVE AntiVirus** SVM Manager. The prefix can include characters a–z, A–Z, 0–9, and [-], without space
Password	Type a password to be used as the **Trellix MOVE AntiVirus** SVM Manager password during deployment. • The password must be at least 6 characters • The password must contain at least one uppercase letter (A-Z) and one numeral (0–9)
Confirm Password	Confirm the password

Note

The password configured for SVM (Agentless) and SVM Manager (Multi-platform) Configuration is assigned to SVM Manager which is deployed from SVM Manager Configuration page.

6. **Click Save to store these configurations, so that you can use them for every Trellix MOVE AntiVirus SVM Manager deployment.**

SVM assignment made easy

An SVM can generally be assigned to 150–300 endpoints, depending on the load of the endpoints.

Assigning policies to the SVM manually is a time-consuming task. The SVM Manager creates assignments based on IP address and tags where a range of endpoints are automatically assigned to a group of SVMs.

SVM autoscaling

The virtual environments are dynamic with the number of instances depending on time of the day and day of the week.

Provisioning your SVMs to accommodate this variation manually is not a scalable solution. You might end up running more SVMs than you require to accommodate peak load. Or, you might end up running fewer SVMs, resulting in endpoints not being protected.

The security administrator can define the number of backup SVMs that are ready to protect your client systems. Calculate the number of ready SVMs required for the maximum number of clients that need protection at any time of the day. The standby SVMs are automatically deployed based on the backup SVM value. For example, if you specify the backup SVM as 4, two standby SVMs are deployed automatically. The SVMs automatically scale up and down depending on the number of endpoints connected.

The SVM deployment automatically transitions between three modes:

- Standby — Standby SVMs are created and are ready to transition to the backup SVM mode. The standby SVMs are automatically deployed based on the backup SVM value. These SVMs are turned off.
- Ready — Backup SVMs that are ready for protecting your client systems. You need to calculate the number of ready SVMs required for the maximum number of clients that would need protection at any time of the day. These SVMs are turned on, but not protecting the client systems.
- Running — These SVMs are currently protecting the client systems.

Multi-platform deployment process using Trellix MOVE AntiVirus autoscaling with SVM Manager

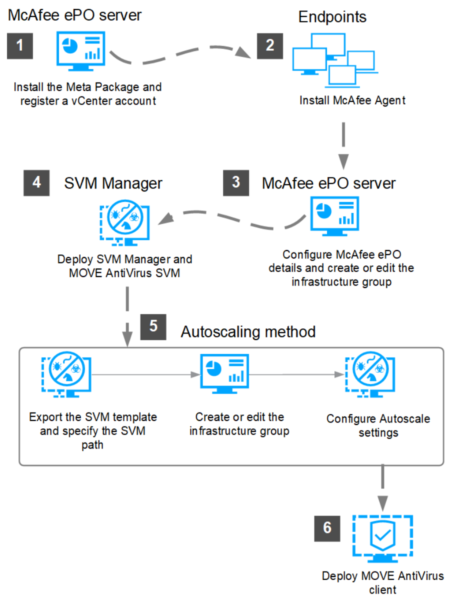
Using **Trellix MOVE AntiVirus** SVM autoscaling, the overall **Trellix MOVE AntiVirus** SVM deployment of the Multi-Platform option consists of the following tasks.

1. Install the extensions on **Trellix ePO - On-prem** and register a VMware vCenter account with **Trellix ePO - On-prem**
2. Install **Trellix Agent** on the endpoints
3. Configure **Trellix ePO - On-prem** details for deployment and create or edit the infrastructure group on **Trellix ePO - On-prem**
4. Deploy SVM Manager
    a. Deploy **Trellix MOVE AntiVirus** SVM
    b. Assign the SVM Manager to SVM
    c. Configure assignment rules in SVM Manager Settings policy
5. Export the SVM template and specify the **Trellix MOVE AntiVirus** SVM path in **Trellix ePO - On-prem**.

    Note

    This is required only when you are using autoscaling method.

    a. Create or edit the infrastructure group on **Trellix ePO - On-prem**
    b. Configure the SVM Autoscale Settings in SVM Manager Settings policy and assign it to SVM Manager
6. Deploy the **Trellix MOVE AntiVirus** Client using **Trellix ePO - On-prem**


McAfee ePO server
1
Install the Meta Package and register a vCenter account
Endpoints
2
Install McAfee Agent
3
McAfee ePO server
Configure McAfee ePO details and create or edit the infrastructure group
4
SVM Manager
Deploy SVM Manager and MOVE AntiVirus SVM
5
Autoscaling method
Export the SVM template and specify the SVM path
Create or edit the infrastructure group
Configure Autoscale settings
6
Deploy MOVE AntiVirus client

The SVM ready pool is now created based on the number of backup SVMs specified. The backup SVMs that you specified in **Trellix ePO - On-prem** are deployed automatically.

A **Trellix MOVE AntiVirus** SVM can generally be assigned to 150–300 endpoints, depending on the load of the endpoints. The security administrator can define the number of backup SVMs that are ready to protect your client systems. Calculate the number of ready SVMs required for the maximum number of clients that need protection at any time of the day.

The standby SVMs are automatically deployed based on the backup SVM value. For example, if you specify the backup SVM as 4, 2 standby SVMs are deployed automatically. The SVMs automatically scale up and down depending on the number of endpoints connected.

When a **Trellix MOVE AntiVirus** client system starts communicating with the SVM Manager, one SVM from the ready pool moves to the running pool and protects the client system. The transition from the ready pool to running pool occurs when no running SVMs exist or all running SVMs have reached their client limit. The ready pool is again replaced with one **Trellix MOVE AntiVirus** SVM from the standby pool.

One **Trellix MOVE AntiVirus** SVM is automatically deployed to the standby pool to retain the number of standby SVMs, which is specified in **Trellix ePO - On-prem**.

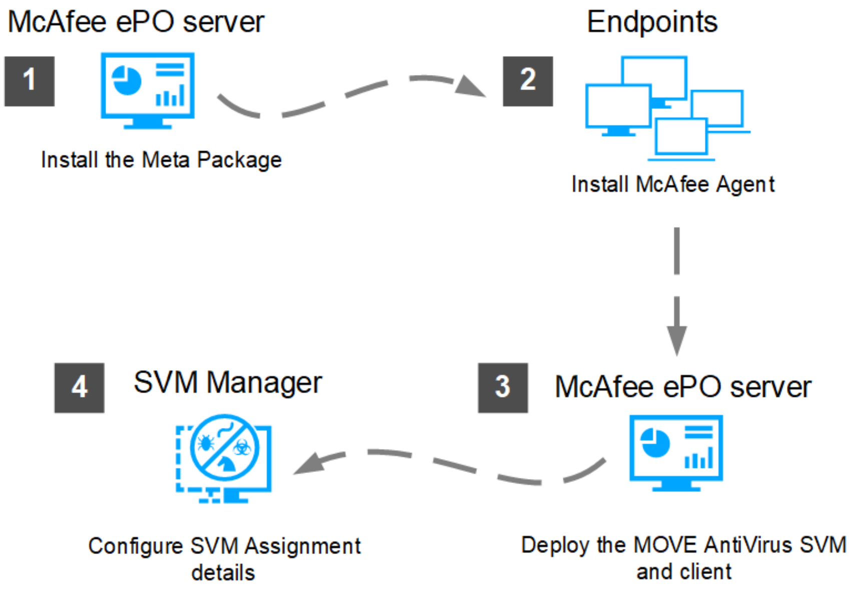
Configure Multi-platform product without SVM Manager

The overall **Trellix MOVE AntiVirus** Multi-platform SVM deployment consists of the following tasks.

1. Install the extensions on **Trellix ePO - On-prem**
2. Install **Trellix Agent** on the endpoints
3. Deploy the **Trellix MOVE AntiVirus** SVM
4. Deploy the **Trellix MOVE AntiVirus** client
5. Configure the **Trellix MOVE AntiVirus** SVM details in the **Options** policy

Note

Configuring the Multi-platform product without SVM Manager is recommended only if you are planning to have one SVM.



Create or edit an infrastructure group in Trellix ePO - On-prem for SVM Manager deployment

After registering your vCenter account, your default group is added to the **MOVE AntiVirus Deployment** wizard when you access the **Infrastructure Details** option under **General**. You can edit the details of the default infrastructure group, as needed.

Before you begin

- You installed the **Trellix MOVE AntiVirus** Meta Package extension on the **Trellix ePO - On-prem** server.
- You registered your VMware vCenter account with **Trellix ePO - On-prem**.

You can deploy the SVM Manager to any infrastructure group using **Trellix ePO - On-prem**. With the **Infrastructure Details** option, you can create or edit a hypervisor-based or cluster-based infrastructure group. You can then customize and select the infrastructure group for SVM Manager deployment.

You can include individual infrastructure groups for SVM Manager deployment.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Automation → MOVE AntiVirus Deployment.**
3. **On the Configuration tab, click Infrastructure Details.**
4. **Edit the default infrastructure group options, as needed.**

Option	Description
Group Name	The name of the infrastructure group. **Note:** The name of the default group can't be edited.
Cloud Account Name	The name of the registered vCenter account.
ESXi / Cluster	The IP address or name of the hypervisor or the cluster selected as part of the infrastructure group. **Note:** If you are selecting **Infrastructure Type** as **Cluster Based**, make sure that you configured a distribution switch for the hypervisors, which are under the selected cluster.
IP Pool Name	The name of the DHCP or IP Pool used in the infrastructure group. By default, DHCP is selected. **Note:** To configure **AD server**, Static IP Pool must be selected.
Provisioning Type	The provisioning type as **Thin** or **Thick**.
Network Name	The name of the management network used by the group.
Datastore Name	The name of the datastore used by the infrastructure group. By default, the datastore with the most free space is selected.
Action	• **Edit** — Click to edit the infrastructure group properties, as needed.

Option	Description
	- **Delete** — Click to delete any unused infrastructure groups. **Note:** You can't delete the **Default Group**.

5. **(Optional) Click Actions → Create and configure properties for the custom infrastructure group. You don't need to configure the custom group options when the default group is available.**

Option	Description
Group Name	Type a name for the infrastructure group.
Infrastructure Type	Select whether you want to create a group based on your hypervisor or cluster. **Note:** If you are selecting **Cluster Based**, make sure that you configured a distribution switch for the hypervisor, which are under the selected cluster.
Select Host / Select Cluster	Select the IP address of your host or cluster.
Hostname Prefix	Type a unique prefix that is added to the host name of the hypervisor or cluster. The prefix can include characters a–z, A–Z, 0–9, and [-], without space.
IP Pool	Configure the IP Pool as **Static** or **DHCP**.
AD Server	Select the registered Active Directory server, so that the deployed SVM is automatically added to the selected domain.
Provisioning Type	Select the provisioning type as **Thin** or **Thick.**

Option	Description
Network Name	Select the required management network.
Datastore Name	Select the configured datastore for the infrastructure.

6. **Click Save to store the infrastructure group details.**

Deploy the SVM Manager in VMware vCenter environment

Check in the SVM Manager OVF package using Trellix ePO - On-prem

Check in the SVM Manager OVF package to the **Trellix ePO - On-prem** server, so that **Trellix ePO - On-prem** can deploy it to your hypervisor.

Before you begin

Make sure that:

- You have installed the **Trellix MOVE AntiVirus** extension on the **Trellix ePO - On-prem** server.
- You have registered a VMware vCenter account with **Trellix ePO - On-prem**.
- You have set up a general configuration for deployment.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Automation → MOVE AntiVirus Deployment.**
3. **On the Configuration tab, click SVM Manager Configuration to open the SVM Manager OVF Details page with these SVM Manager options.**

Options	Description
SVM Manager OVF Name	Name of the SVM Manager OVF package checked in to the **Trellix ePO - On-prem** server.
SVM Manager OVF Version	Version of the SVM Manager OVF package checked in to the **Trellix ePO - On-prem** server.
Action	**Delete** — To remove a checked in SVM Manager OVF.

4. **Click Actions → Add SVM Manager to open the Check-in SVM Manager OVF (zip) File page.**
5. **Under SVM Manager OVF Check-in, configure these options:**

- **Select SVM Manager OVF (zip) file to check-in** — Browse to and select the SVM Manager OVF package (MOVE-AV-MP_SVM_Manager_OVF_ 4.9.0.195.zip).
- **Specify the location of Trellix ePO - On-prem system** — Specify the SVM Manager OVF package location on the **Trellix ePO - On-prem** server (for example, **C:\SVM Manager**). The package is taken from this location during deployment to the hypervisor.

Note

> Make sure that you first deploy **SVM Manager** version 4.9 using MOVE-AV-MP_SVM_Manager_OVF_ 4.9.0.195.zip and later upgrade the **SVM Manager** to version 4.10 using MOVE-AV-MP_SVM_Manager_OVF_ 4.10.0.547.zip. For more information on how to upgrade the SVM Manager see, Upgrade the SVM Manager topic in this document.

6. **Click OK to check in the package.**

Results

The SVM Manager OVF package appears in the specified folder on the **Trellix ePO - On-prem** server. Also, the SVM Manager details appear on the **SVM Manager OVF Details** page.

To deploy SVM Manager in a VMware vCenter environment, see

Deploy SVM Manger from Trellix MOVE AntiVirus deployment page

Using the **Trellix ePO - On-prem** console, deploy the SVM Manager to your hypervisors, so that it automatically assigns the SVM to a group of clients.

Before you begin

Note

> You need to have the vendor specific tool for conversion installed on your systems to deploy SVM Manager on **Citrix Xenserver** and **Microsoft Hyper-V** environments.

Make sure that:

- You have installed the **Trellix MOVE AntiVirus** extension on the **Trellix ePO - On-prem** server.
- You have registered your VMware vCenter account with **Trellix ePO - On-prem**.
- Your VMware vCenter account is synced successfully.
- You have configured your **Trellix ePO - On-prem** details about the **General** page under **Menu** → **Automation** → **MOVE AntiVirus Deployment** → **Configuration**.
- You configured your Infrastructure Group.
- You have checked in the SVM Manager OVF package to the **Trellix ePO - On-prem** server.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Automation → MOVE AntiVirus Deployment.**

The default password for the SVM Manager svaadmin account is `Svaadmin$1`

You can change the password from the **SVM Manager (Multi-Platform) Configuration** option under **Menu** → **Automation** → **MOVE AntiVirus Deployment** → **Configuration** → **General**.

3. **On the Configuration tab, click SVM Manager Configuration to open the SVM Manager OVF Details page.**
4. **Under Deployment Configuration, configure these options.**
   - **Infrastructure Group** — Select the **Default Group** or an infrastructure group you created. The SVM Manager is deployed on this infrastructure group.
   - **Checked-in OVF** — Select the SVM Manager OVF package that is checked in to the **Trellix ePO - On-prem** server.
   - **SVM Manager Settings policy** — Select the SVM Manager Settings policy, so that it is assigned to the SVM Manager.
5. **Click Deploy SVM Manager to open the Confirm SVM Manager Deployment dialog box.**
6. **Click OK to deploy the SVM Manager.**

Results

On a successful deployment, an **SVM-Manager** VM is created on the configured infrastructure group. Now, the SVM Manager service can communicate with **Trellix ePO - On-prem** through the **Trellix Agent**. Also, the selected SVM Manager Settings policy is applied to the SVM Manager.

Check the SVM Manager deployment status

After deploying the SVM Manager, you can view the deployment details on the **Deployment Status** tab under **MOVE AntiVirus Deployment** wizard on the **Trellix ePO - On-prem** server.

Before you begin

- You installed the **Trellix MOVE AntiVirus** extension on the **Trellix ePO - On-prem** server.
- You initiated the SVM Manager deployment using **Trellix ePO - On-prem**.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Automation → MOVE AntiVirus Deployment.**
3. **On the Deployment Status tab, view the SVM Manager deployment details.**
4. **Click any SVM Manager deployment job to view these Task Status Details.**

Deployment status

Item	Description
Hypervisors/Hostname	Specifies the name of the hypervisor.
vCenter Name/IP address	Specifies the name of the VMware vCenter account that is registered with **Trellix ePO - On-prem**.

Item	Description
Deployment Type	Displays the SVM Manager deployment type as **Deploy SVM Manager**.
Status	Specifies the deployment status such as **Started**, **In Progress**, **Completed**, and **Failed**.
Start Time	Indicates the date and time when the SVM Manager deployment started.
End Time	Indicates the date and time when the SVM Manager deployment ended.

Task status

Item	Description
Node Type	Specifies whether the node is an SVM Manager or a hypervisor, SVM, or a VM.
Task Type	Specifies the set of internal tasks in a deployment job. The task list for one job is displayed in sequence with **Start Time**, **End Time**, and **Failure Reasons**, if applicable.
Node Name	Displays the SVM Manager name, or hypervisor name, SVM, or the guest VM name.
Status	Specifies the task status: **Started**, **In Progress**, **Completed**, **Skipped**, and **Failed**.
Failure Reason	Specifies the reason for the failure of the task.
Start Time	Indicates the date and time when the task started.
End Time	Indicates the date and time when the task ended.

Task type and status details

These are the task types that specify the internal tasks of a deployment job. The task list for one job is displayed in sequence with **Start Time**, **End Time**, and **Failure Reasons**, if applicable.

During SVM Manager deployment

Task type	Description
Deploying SVM Manager	Indicates that the SVM Manager deployment is in progress.
Powering on SVM Manager	Specifies that the SVM Manager is turned on.
Registering SVM Manager with McAfee ePO	Registers the SVM Manager with **Trellix ePO - On-prem**.
Assigning SVM Manager Settings policy to the SVM Manager node	Assigns the SVM Manager Settings policy to the SVM Manager node.

During rollback

Task type	Description
Rollback: Returning Static IP to IP Pool	(If Static IP Pool is used) Rolls back the static IP to IP Pool, which was assigned to the deployed SVM Manager. (If DHCP is used) This task is skipped.
Rollback: Powering off SVM Manager	Rolls back the **Powering on SVM Manager** task.
Rollback: Remove SVM Manager	Rolls back the **Deploying SVM Manager** task.

SVM Manager in Hyper-V environment

To deploy the SVM Manager on Hyper-V, you must convert the **.vmdk** file, part of SVM Manager appliance, into a **.vhd** file.

Before you begin

Note

You need to have the vendor specific tool for conversion installed on your systems to deploy SVM Manager on **Citrix Xenserver** and **Microsoft Hyper-V** environments.

Make sure the **MOVE-AV-MP_SVM_Manager_OVF_4.10.x.x.zip** file is in accessible location.

Task

1. **Unzip the MOVE-AV-MP_SVM_Manager_OVF_4.10.x.x.zip file.**
2. **Using the Microsoft Virtual Machine Converter software, convert the .vmdk file into a .vhd file.**
3. **Attach the .vhd file as a hard disk to a new VM in Hyper-V.**

Setup SVM Manager on vCenter environment manually

You must set up and configure the SVM Manager before deploying the SVM and assigning it to a group of clients. You can use this method for all type of hypervisors.

Before you begin

- You must have administrator rights to perform this task.
- The SVM Manager OVF package is in an accessible location on the network.

Task

1. **Open the VMware vSphere client, then click File → Deploy OVF Template.**
2. **Browse to and select the SVM Manager OVF package (`MOVE-AV-MP_SVM_Manager_Pkg.4.10.x.x.zip`) on your computer, then click Next to start the installation wizard.**
3. **Complete the steps in the wizard, accepting the default values or entering different values as needed.**
4. **When finished, select Power On to turn on the virtual machine and open a Console window to configure the SVM Manager appliance.**
5. **At the prompt, log on with these credentials:**
   - User name: `svaadmin`
   - Password: `svaadmin`
6. **Configure the VM appliance with these details:**
   - Time zone
   - Network — DHCP or Static (Recommended: select a Static IP address for SVM Manager)
   - DNS servers
   - IP Address or Hostname of the **Trellix ePO - On-prem** server

     Note

     It is recommended to use **Trellix ePO - On-prem** IP, even if the hostname resolves from new SVA-manager box.
   - **Trellix ePO - On-prem** credentials Check for the correct format of the user name, for example: `domain\\user name`.
7. **Verify that these communication ports are open and reachable on the SVM Manager:**
   - **8080** — For communication between SVM Manager and the client
   - **8081** — For communication between **Trellix Agent** and **Trellix ePO - On-prem**

- **8443** — For communication between SVM Manager and the SVM

Tip

Best practice: By default, these ports are already opened through the firewall installed on the appliance. However, verify that the firewall settings in your environment are configured to allow communication on these ports.

8. **Use this command to manually run the configuration script:** `sudo /home/svaadmin/.sva-config`.

Results

Now, the SVM Manager service can communicate with **Trellix ePO - On-prem** through the **Trellix Agent**. You must now set the required policies in **Trellix ePO - On-prem**.

Deploy the Trellix MOVE AntiVirus SVM

Create a SVM deployment client task

Create an SVM deployment client task, so that you can assign that task to virtual machines.

Before you begin

Make sure that:

- You have installed the **Trellix MOVE AntiVirus** extension on the **Trellix ePO - On-prem** server.
- The **Trellix Agent** and **Endpoint Security** 10.x.x are installed on the target virtual system.

Note

Make sure that you check for AMCore Content (DAT) update before deploying the SVM.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Policy → Client Task Catalog.**
3. **Select Product Deployment in the Client Task Types menu, then select Actions → New Task.**
4. **Select Product Deployment from the list, then click OK to open the Client Task Builder wizard.**
5. **Type a name for the task you are creating, and add any descriptive information in the Description field.**
6. **Make sure that Windows is the only target platform selected.**
7. **For Products and components:**
   a. **For SVM, select Trellix MOVE AV [Multi-Paltform] SVM 4.10.x.x from the drop-down list.**
   b. **Set the action to Install, set the language to Language Neutral, and set the branch to Current.**
   c. **Leave the Command line setting blank.**
8. **Review the task settings, then click Save.**

Results

The task is added to the list of client tasks for the selected client task type.

Assign an SVM deployment client task

After creating the SVM deployment client task, you must assign that task to virtual machines.

Before you begin

The **Trellix Agent** must already be deployed to target virtual systems.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Policy → Client Task Assignments, then click the Assigned Client Tasks tab.**
3. **Click Actions → New Client Task Assignment.**
4. **Configure these settings, then click Next.**
   - **Product** — **Trellix Agent**
   - **Task Type** — Product Deployment
   - **Task Name** — The name of the task you used when you created the client task
5. **On the Schedule tab, specify the schedule for running the client task, then click Next.**
6. **Examine the settings on the Summary tab, then click Save to assign the task.**

Results

The **Trellix MOVE AntiVirus** SVM is deployed to systems in the selected group in the System Tree.

Assign the SVM Manager to an SVM

Configure the SVM Manager details in **Trellix MOVE AntiVirus Options** policy and assign it to the SVMs, so that the SVM Manager and SVMs can communicate to each other.

Before you begin

Make sure that:

- You have installed the **Trellix MOVE AntiVirus** extension on the **Trellix ePO - On-prem** server.
- You have deployed the **Trellix MOVE AntiVirus** SVM Manager.
- You have deployed the **Trellix MOVE AntiVirus** SVM package to the target virtual systems.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Click Menu → Policy → Policy Catalog, select MOVE AntiVirus 4.10.x from the Product drop-down list, then select Options from the Category drop-down list.**
3. **Click New Policy or click the name of an existing policy to edit it.**
4. **Type a name for the new policy (for example, `SVM Assignment Policy`), then click OK.**

5. **Under SVM Assignment on the policy settings page, select Assign SVM using SVM Manager and configure the SVM Manager details, then click Save.**
   - Enter the SVM Manager **IP address** or **FQDN** (domain name)
   - Enter the SVM Manager **Port**. Default is 8080.
6. **Assign the configured policy to your SVMs.**

Results

The SVM Manager and the SVMs communicate, so that the clients can request the SVM Manager when they require an SVM. SVM Manager serves them an SVM based on the filtering rules created in the **SVM Manager Settings** policy.

Configure an SVM assignment rule

Add or edit an SVM Manager assignment rule using IP address

Using their IP address range, assign a set of endpoints to a selected SVM or multiple SVMs, so that those endpoints are protected by the SVM Manager assignment rule.

Before you begin

Make sure that:

- You have installed the **Trellix MOVE AntiVirus** extension on the **Trellix ePO - On-prem** server.
- You have deployed the SVM Manager.
- You have deployed the **Trellix MOVE AntiVirus** SVM package to the target virtual systems.

Things to remember:

- You can define different rules to overwrite the autoscale settings. After defining the generic SVM autoscale requirements in **SVM Autoscale Settings**, you can also define rule-based autoscale settings.
- Rule-based autoscale settings can overwrite the regular **SVM Autoscale Settings**.
- You can separate IP addresses or ranges with a comma (,) or a new line.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Policy → Policy Catalog, select MOVE AntiVirus 4.10.x from the Product drop-down list, then select SVM Manager Settings from the Category drop-down list.**
3. **Click New Policy or click the name of an existing policy to edit it.**
4. **Type a name for the new policy (for example, `MOVE AV SVM Manager Policy`), then click OK.**
5. **On the Assignment Rules tab on the Policy Settings page, click Add to open the Add/Edit SVM IP Assignment Rule dialog box and configure these settings as needed.**

For this option...	Do this...
Rule name	Type a unique user-friendly name that can help you identify the rule.
Client IP Addresses	Type the IP address or a range of IP addresses of the endpoints, so that these endpoints can be protected by the SVM, which is specified in the **SVM IP Address** option.
SVM IP Addresses	Type the IP address of the SVM, so that this SVM can protect the endpoints, which are specified in the **Client IP Address** option.

If you are using the autoscale SVM feature, configure these settings.

For this option...	Do this...
Select and add to infrastructure groups	Select the **Default Group** or an infrastructure group you created using the **Menu** → **Automation** → **MOVE AntiVirus Deployment** → **Configuration** → **Infrastructure Details** option, so that SVM deployment can be done to a specific infrastructure group in your organization.
Customize SVM Settings	This is the SVM assignment rule specific to autoscale settings. Each rule can be assigned for individual SVM deployment settings. You can define different rules, which overwrite the common autoscale settings defined under **SVM Autoscale Settings**. • **Number of backup SVMs** — Type the number of ready SVMs required to protect your client systems. Calculate the number of ready SVMs required for the maximum number of clients that need protection at any time of the day. The standby SVMs are automatically deployed based on the backup SVM value. For example, if you

For this option...	Do this...
	specify the backup SVM as 4, two standby SVMs are deployed automatically. The **Trellix MOVE AntiVirus** SVMs automatically scale up and down depending on the number of endpoints connected.
Alarms	**Threshold for number of connected endpoints (per SVM)** — Specify the SVM capacity threshold level. A warning appears when the number of connected endpoints is more than this level.

Note

The **Assign SVM if no rule is defined for the above client** option is used to assign the SVM to endpoints, which are not defined in any of the rules. By default, this option is enabled.

6. **(Optional) Select Enable to get SVM preference from the same subnet to assign an SVM from the same subnet. For details, see *SVM preference*.**
7. **Click OK to save your changes.**

Add or edit an SVM Manager assignment rule using Trellix ePO - On-prem tag

Assign a set of endpoints to a selected SVM using their tag group, so that they are protected by the SVM Manager assignment rule.

Before you begin

Make sure that:

- You have installed the **Trellix MOVE AntiVirus** extension on the **Trellix ePO - On-prem** server.
- You have deployed the SVM Manager.
- You have deployed the **Trellix MOVE AntiVirus** SVM package to the target virtual systems.

Things to remember:

- You can define different rules to overwrite the autoscale settings. After defining the generic SVM autoscale requirements in **SVM Autoscale Settings**, you can also define rule-based autoscale settings
- Rule-based autoscale settings overwrite the regular **SVM Autoscale Settings**.
- Separate tag names with a comma (,)
- Tag-based assignment rules take priority over IP-based assignment rules

Task

1. **Log on to Trellix ePO - On-prem as an administrator**

2. **Select Menu → Policy → Policy Catalog, select MOVE AntiVirus 4.10.x from the Product drop-down list, then select SVM Manager Settings from the Category drop-down list**
3. **Click New Policy or click the name of an existing policy to edit it**
4. **Type a name for the new policy (for example, MOVE AV SVM Manager Policy), then click OK**
5. **In the Tag Assignment Rules tab on the Policy Settings page, click Add to open the Add/Edit SVM Tag Assignment Rule dialog box and configure these settings as needed**

For this option...	Do this...
Rule name	Type a unique user-friendly name that can help you identify the rule
Select and add to client tags	Select the **Trellix ePO - On-prem** tag names of the endpoints, so that these endpoints can be protected by the SVM, which is specified in the **Select and add to SVM tags** option
Select and add to SVM tags	Select the **Trellix ePO - On-prem** tag name of the SVM, so that this SVM can protect the endpoints, which are specified in the **Select and add to client tags** option

If you are using the autoscale SVM feature, configure these settings.

For this option...	Do this...
Select and add to infrastructure groups	Select the **Default Group** or an infrastructure group you created using the **Menu** → **Automation** → **MOVE AntiVirus Deployment** → **Configuration** → **Infrastructure Details** option, so that SVM deployment can be done to a specific infrastructure group in your organization
Customize SVM settings	This is the SVM assignment rule specific to autoscale settings. Each rule can be assigned for individual SVM deployment settings. You can define different rules, which overwrite the common autoscale settings defined under **SVM Autoscale Settings**.

For this option...	Do this...
	• **Number of backup SVMs** — Type the number of ready SVMs required for protecting your client systems. Calculate the number of ready SVMs required for the maximum number of clients that need protection at any time of the day. The standby SVMs are automatically deployed based on the backup SVM value. For example, if you specify the backup SVM as 4, two standby SVMs are deployed automatically
Alarms	**Threshold for number of connected endpoints (per SVM)** — Specify the SVM capacity threshold level. A warning appears when the number of connected endpoints is more than this level

Note

The **Assign SVM if no rule is defined for the above client** option is used to assign the SVM to endpoints, which are not defined in any of the rules. By default, this option is enabled.

6. **(Optional) Select Enable to get SVM preference from the same subnet to assign an SVM from the same subnet. For details, see *SVM preference***
7. **Click OK to save your changes**

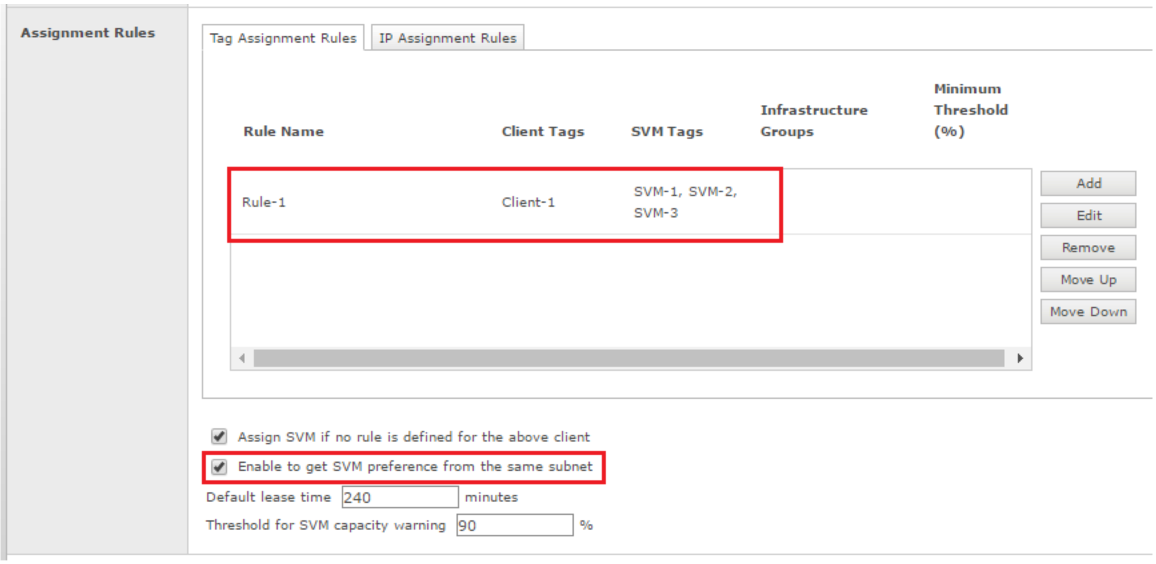
SVM preference

Selecting the **Enable to get SVM preference from the same subnet** option, you can assign an SVM to the clients from the same subnet when clients migrate from one hypervisor to another. You must define tag or IP-based rules specifying the SVM's IP address or tag of respective hypervisor/subnet.

For example, consider a scenario where:

- SVM-1, SVM-2, and SVM-3 are in ESXi-1, ESXi-2, and ESXi-3 servers respectively
- You have a client that keeps migrating from one hypervisor to another
- You want to protect the client by an SVM that belongs to the same subnet

With these assumptions, selecting the **Enable to get SVM preference from the same subnet** option, when the client migrates from one hypervisor to another, it is protected from an SVM that belongs to the same subnet.



Rule Name	Client Tags	SVM Tags	Infrastructure Groups	Minimum Threshold (%)
Rule-1	Client-1	SVM-1, SVM-2, SVM-3		

☑ Assign SVM if no rule is defined for the above client

☑ Enable to get SVM preference from the same subnet

Default lease time 240 minutes

Threshold for SVM capacity warning 90 %

Default rule vs custom rules (tag-based or IP-based)

After registering your vCenter account, your default infrastructure group is added to the **MOVE AntiVirus Deployment** wizard when you access the **Infrastructure Details** option under **Multi-Platform**.

When you enable the autoscale SVM feature based on the specified SVMs value under **Customize SVM Settings**, a default SVM pool is created, then Ready and Standby SVMs are deployed to the default infrastructure group for the default SVM assignment rule.

When you create SVM assignment rules (tag-based or IP-based), you can specify the number of backup SVMs for the rule, then new SVMs are deployed to the selected infrastructure group. The infrastructure group can be default group or user-defined group.

The clients that are not under a tag-based or IP-based rule are protected by the default SVM pool corresponding to the default SVM assignment rule.

- If you bring up the client system that is not part of the SVM assignment rules (tag-based or IP-based), the client system is protected by the SVM pool that is created for the default SVM assignment rule.
- If you bring up the client system that is part of the SVM assignment rules (tag-based or IP-based), the client system is protected by the SVM pool that is created for the custom SVM assignment rule.

Creating more rules consumes more computing resources for deploying SVMs. For example, if you create 10 SVM assignment rules (tag-based or IP-based) specifying backup SVMs as 2, then 2 Ready and 1 Standby SVMs are deployed for each rule.

How autoscale SVM works

A default infrastructure group is added to the **MOVE AntiVirus Deployment** wizard when you access the **Infrastructure Details** option under **Multi-Platform**.

When you enable the autoscale SVM feature, based on the specified SVM's value under **Customize SVM Settings**, a default SVM pool is created then Ready and Standby SVMs are deployed to the default infrastructure group for the default SVM assignment rule (The SVM assignment rule is created by default for the clients that are not part of user-defined SVM assignment rules. The default SVM assignment rule does not appear on the **Trellix ePO - On-prem** page).

For user-defined SVM assignment rule, the number of backup SVMs can be specified on the **Add/Edit SVM Tag Assignment Rule** or **Add/Edit SVM IP Assignment Rule** dialog box under **Customize SVM Settings**.

Example 1

Consider a scenario where:

- The number of clients — X
- The number of Ready SVMs specified in **Trellix ePO - On-prem** — Y
- The number of Standby SVMs — Z

Depending on the value Y, the time it takes to start protecting the X number of clients varies. If the value of Y is less (considering each SVM protects 250 clients), then for the first time, it takes more time to protect the X clients because that number of required SVMs must be deployed. But eventually all X clients are protected.

You can also bring all these X clients to the **Trellix MOVE AntiVirus** environment in different batches. For example, if you have 10000 clients in your environment, you can bring them in 2 batches (5000 clients in each batch), so that there is no gap in protecting the clients by SVMs.

Example 2

Consider a scenario where:

- The total number of client systems — 15000
- The number of static client systems (All time turned on) — 6000
- The number of dynamic clients (Keep turned on and off when needed) — 9000 These 9000 clients are part of 3 SVM assignment rules (a default, one tag-based, and one IP-based rule) — 3000 client systems per each rule
- The number of client systems with a tag-based SVM assignment rule — 3000
- The number of client systems with an IP-based SVM assignment rule — 3000
- The number of client systems with a default SVM assignment rule — 9000 (3000 dynamic and 6000 static)

These 9000 dynamic client systems need immediate protection when they are up and running. These 9000 dynamic client systems can be protected by using the autoscale SVM feature.

You configured the number of Ready SVMs as 4 and the number of Standby SVMs as 2 for each SVM assignment rule (default, tag-based, and IP-based) to protect these 9000 dynamic client systems.

With these 4 Ready and 2 Standby SVMs, dynamic and static client systems must be protected.

Protecting dynamic client systems

- During the peak time, say 9000 client systems are up and running, then first 3000 clients (1000 clients per each rule) are protected immediately [As the 12 Ready SVMs (4 Ready SVMs of each rule) would immediately transition to Running state and protect the first 3000 clients]. But for next 6000 dynamic clients, the new Ready SVMs need to be deployed and they keep transitioning from **Standby** → **Ready** → **Running** state depending on the client load. It takes some time to protect these 6000 dynamic client systems. So to keep protecting the total 9000 dynamic clients, 36 Running SVMs (12 SVMs per each rule) are required.

- When clients systems are turned off, the corresponding Running SVMs are transitioned to Standby state so that the computing resources are saved.

Protecting static client systems

These 6000 static clients are protected by the respective SVM pool that is created for the corresponding SVM assignment rule (default, tag-based, and IP-based).

- To protect 6000 static client systems, 24 Running SVMs (6000/250 = 24 Running SVMs) are required.
- These initial 24 Running SVMs creation takes some time, as this is an initial setup and fresh Ready and Standby SVMs need to be deployed. The transition from **Standby** → **Ready** → **Running** happens in phase by phase manner. But eventually all X clients are protected.

To protect 12,000 static clients at once, you can also bring all these 12,000 clients to the **Trellix MOVE AntiVirus** environment in different batches, for example, you can bring them in 12 batches (1000 clients per batch) so that there is no gap in protecting the clients by SVMs.

Configuring an SVM OVF template for autoscaling

An SVM OVF template is a primary image of a virtual machine that can be used to create and deploy many SVMs.

When you export an SVM, you create a copy of the entire virtual machine, including its settings, installed software, and other configuration settings. Exporting the SVM saves time when you are deploying many SVMs. You can create and configure a single SVM, then deploy it multiple times, rather than creating and configuring each SVM individually.

When you deploy an SVM from OVF template, the resulting SVM is independent of the original SVM or template. Changes to the original SVM or template are not reflected in the deployed SVM, and changes to the deployed SVM are not reflected in the original SVM or template.

Note

Exporting an SVM OVF template is required only when you are using autoscaling method.

You can configure an SVM OVF template using one of these options:

- **Export an existing SVM or create and export from a VM** — You can export a template from an SVM system or can create an SVM and export it to make a primary image of the SVM, from which you can deploy many SVMs.
- **Specify the SVM OVF location available on the McAfee ePO system** — You can export an SVM OVF template using the export utility, then copy the exported SVM OVF template to the **Trellix ePO - On-prem** server. Then specify the location of the SVM OVF template that is available on the **Trellix ePO - On-prem** server, so that **Trellix MOVE AntiVirus** can deploy SVMs, as needed.

Export an SVM OVF template

Using the **Export an existing SVM or create and export from a VM** option, you can export a template from an SVM system or can create an SVM system, then export it to make a primary image of an SVM, from which you can deploy many SVMs. When you use this option, **Trellix MOVE AntiVirus** installs **Endpoint Security** and the SVM package (if they are not installed) on the VM, then exports it to the **Trellix ePO - On-prem** server.

Before you begin

Make sure that:

- You have installed the **Trellix MOVE AntiVirus** 4.10.x extensions on the **Trellix ePO - On-prem** server.
- Your VMware vCenter account is synced successfully.
- (If you are creating and exporting from a VM) You have a VM with one of these Plain Vanilla Windows Server platforms: 2008 R2 SP1 (64-bit), 2012 R2 (64-bit), 2016, or 2019.
- (If you are exporting from an existing SVM) Make sure that the SVM package is upgraded to 4.10.x.
- The latest VMware Tools are installed on the VM.
- The VM is managed by **Trellix ePO - On-prem**.
- The VM has no snapshots.
- The VM has only one hard disk.
- The VM is turned on.
- (If your environment includes more than one domain) Make sure that the VM is not part of any domain, so that the exported SVM template is a generic one and can be deployed to any domain.
- Do not configure the SVM Manager IP details under **SVM Manager Assignment** in **Options** policy until you create and export the SVM template.

Note

To use autoscale SVM feature, the minimum supported **Endpoint Security** version is 10.7.0 or later.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Automation → MOVE AntiVirus Deployment.**
3. **On the Configuration tab, under Multi-Platform, click SVM Configuration to open the SVM OVF Details page with these SVM OVF details and actions.**

Options	Description
SVM OVF Name	Name of the **Trellix MOVE AntiVirus** SVM OVF template checked in to **Trellix ePO - On-prem**.
SVM OVF Version	Version of the **Trellix MOVE AntiVirus** SVM OVF template checked in to **Trellix ePO - On-prem**.

Options	Description
SVM OVF Use Count	Specifies the number of SVMs that are deployed for SVM autoscaling
Action	**Delete** — To remove an existing **Trellix MOVE AntiVirus** SVM OVF when it is not deployed to any hypervisor. You can delete the SVM OVF only when the **SVM OVF Use Count** is 0.

4. **Click Actions → Add SVM to open the Configure SVM OVF page.**
5. **Under Configure SVM OVF template, select Export an existing SVM or create and export from a VM and configure these options.**

Options	Description
Registered Cloud Account	Select a VMware vCenter account where the VM is present
VM Name	Type the name of the VM
Username	Type the user name of the VM
Password	Type the password of the VM
Confirm Password	Retype the password
SVM Location on McAfee ePO	Specify the location on the **Trellix ePO - On-prem** server. This location is used to store the exported SVM OVF template
SVM OVF Version	Type a version for the SVM OVF template, for example, `4.10.x`
SVM OVF Name	Type a name for the SVM OVF template, for example, `ESVM 4.10.x`

Options	Description
Description	(Optional) Type details about the SVM OVF template, to help identify the SVM OVF template

6. **Click Export to open the Export SVM OVF Confirmation dialog box.**
7. **Click OK to create an SVM system and export it to make an SVM OVF template.**

Results

The SVM OVF template files (**.ovf and **.vmdk) are created on the **Trellix ePO - On-prem** server. Also, the exported SVM

OVF template details are available on the **SVM OVF Repository** page under **MOVE AntiVirus Deployment** → **Configuration** → **Multi-Platform** → **SVM Configuration**.

Check the SVM export status

After exporting an SVM, you can view the export details on the **Deployment Status** tab under **MOVE AntiVirus Deployment** wizard on the **Trellix ePO - On-prem** server.

Before you begin

Make sure that you initiate an SVM export using **Trellix ePO - On-prem**.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Automation → MOVE AntiVirus Deployment.**
3. **On the Deployment Status tab, view the SVM export details.**
4. **Click any Export SVM OVF template job to view these Task Status Details.**

Deployment status

Item	Description
Hypervisors/Hostname	Specifies the host name of the SVM
vCenter Name/IP address	Specifies the name of the VMware vCenter account that is registered with **Trellix ePO - On-prem**
Deployment Type	Displays the deployment type as **Export SVM OVF template**

Item	Description
Status	Specifies the deployment status such as **Started**, **In Progress**, **Completed**, and **Failed**
Start Time	Indicates the date and time when the SVM export job started
End Time	Indicates the date and time when the SVM export job ended

Task status

Item	Description
Node Type	Specifies whether the node is an SVM or endpoint
Task Type	Specifies the set of internal tasks in an SVM export job. The task list for one job is displayed in sequence with **Start Time**, **End Time**, and **Failure Reasons**, if applicable
Node Name	Displays the name of the VM
Status	Specifies the task status: **Started**, **In Progress**, **Completed**, **Skipped**, and **Failed**
Failure Reason	Specifies the reason for the failure of the task
Start Time	Indicates the date and time when the task started
End Time	Indicates the date and time when the task ended

Create or edit an infrastructure group in Trellix ePO - On-prem for SVM autoscaling

After registering your vCenter account, your default group is added to the **MOVE AntiVirus Deployment** wizard when you access the **Infrastructure Details** option under **Multi-Platform.** You can edit the details of the default infrastructure group, as needed.

Before you begin

You registered your VMware vCenter account with **Trellix ePO - On-prem**.

You can deploy the SVM to any infrastructure group by configuring the SVM Manager and autoscale settings in **Trellix ePO - On-prem**. By default, an infrastructure group is added to the **MOVE AntiVirus Deployment** wizard when you access the **Infrastructure Details** option under **Multi-Platform**.

Using the **Infrastructure Details** option, you can create a hypervisor-based or cluster-based infrastructure group. You can then customize and select the infrastructure group for SVM deployment.

You can customize the **SVM Manager Settings** policy for creating and assigning IP-based or tag-based assignment rules for SVM deployment. You can select and include individual infrastructure groups for SVM deployment.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Automation → MOVE AntiVirus Deployment.**
3. **On the Configuration tab, click Infrastructure Details to open the Infrastructure Details page with the default infrastructure group details.**

Option	Description
Group Name	Specifies the name of the infrastructure group. **Note:** The name of the default group can't be edited.
Cloud Account Name	Specifies the account name of the registered vCenter account.
ESXi/Cluster	Specifies the IP address or name of the hypervisor or the cluster selected as part of the infrastructure group. **Note:** If you are selecting **Infrastructure Type** as **Cluster Based**, make sure that you configured a distribution switch for the hypervisors, which are under the selected cluster.

Option	Description
IP Pool Name	Specifies the name of the DHCP or IP Pool used in the infrastructure group. By default, DHCP is selected. **Note:** To configure **AD server**, Static IP Pool must be selected.
Provisioning	Specifies the provisioning type as **Thin** or **Thick**.
Network Name	Specifies the name of the management network used by the group.
Datastore Name	Specifies the name of the datastore used by the infrastructure group. By default, the datastore with the most free space is selected.
Action	• **Edit** — Click to edit the infrastructure group properties, as needed. • **Delete** — Click to delete any unused infrastructure groups. **Note:** You can't delete the **Default Group**.

4. **Click Actions → Create and configure these properties for the custom infrastructure group details. You don't need to configure the custom group details when the default group is available.**

Option	Description
Group Name	Type a name for the infrastructure group.
Infrastructure Type	Select whether you want to create a group based your hypervisor or cluster.

Option	Description
	Note: If you are selecting **Cluster Based**, make sure that you configured a distribution switch for the hypervisor, which are under the selected cluster.
Select Host (Cluster)	Select the IP address of your host or cluster.
Hostname Prefix	Type a unique prefix that is added to the host name of the hypervisor or cluster. The prefix can include characters a–z, A–Z, 0–9, and [-], without space.
IP Pool	Configure the IP Pool as **Static** or **DHCP**.
AD Server	Select the registered Active Directory server, so that the deployed SVM is automatically added to the selected domain.
Provisioning Type	Select the provisioning type as **Thin** or **Thick.**
Network Name	Select the required management network.
Datastore Name	Select the configured datastore for the infrastructure.

5. **Click Save to store the infrastructure details.**

Enable and configure SVM autoscale settings

Create and assign a policy that specifies which SVM an infrastructure group uses.

Before you begin

Make sure that:

- You define the autoscale settings for the **Trellix MOVE AntiVirus** SVM so that its deployment starts automatically, depending on the number of clients connecting to it for protection.
- You installed the **Trellix MOVE AntiVirus** extension on the **Trellix ePO - On-prem** server
- You configured your **Trellix ePO - On-prem** details about the **General** page under **Automation** → **MOVE AntiVirus Deployment** → **Configuration**

- You deployed the SVM Manager
- You exported an SVM OVF template
- (If you exported an SVM OVF using export utility tool) You specified the **Trellix MOVE AntiVirus** SVM OVF template path in **Trellix ePO - On-prem**
- You configured the SVM Manager IP details under **SVM Manager Assignment** in **Options** policy

You can track the status of the SVM deployment on the **Deployment Status** page on the **Trellix ePO - On-prem** server.

Note

You can deploy only one SVM manager if you enable the autoscaling feature.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Policy → Policy Catalog, select MOVE AntiVirus 4.10.x from the Product drop-down list, then select SVM Manager Settings from the Category drop-down list.**
3. **Click New Policy or click the name of an existing policy to edit it.**
4. **Type a name for the new policy (for example, `MOVE AV Server Policy`), then click OK.**
5. **Under SVM Manager Configuration, configure these settings as needed, then click Save.**
    - **SVM Port** — Specify the port for the SVM to communicate to SVM Manager. Default is 8443.
    - **Client Port** — Specify the port for the client system to communicate to SVM Manager. Default is 8080.
6. **From SVM Autoscale Settings, select Enable auto scaling of SVMs.**

    Important

    Enabling the **Enable auto scaling of SVMs** option deletes all manually deployed SVMs after the new SVMs are deployed. The new SVMs are ready to protect the client systems. Disabling the **Enable auto scaling of SVMs** option deletes all ready and standby SVMs, but the running SVMs continue to protect the client systems.

7. **Under SVM Autoscale Settings, configure these options:**
    - **Number of backup SVMs** — Type the number of ready SVMs required to protect your client systems. Calculate the number of ready SVMs required for the maximum number of clients that need protection at any time of the day. The standby SVMs are automatically deployed based on the backup SVM value. For example, if you specify the backup SVM as 4, 2 standby SVMs are deployed automatically.

        Important

        The ready SVMs are not protecting your clients, but running SVMs are. The backup SVMs are the ready SVMs, which enable faster protection for new client systems that might be added during peak hours or during a cloud burst.

- **Threshold for number of connected endpoints (per SVM)** — Specify the SVM capacity threshold level. A warning appears when the number of connected endpoints is more than this level.

  Note

  When the SVM reaches minimum threshold for the number of connected endpoints, the running SVMs move to the standby SVM pool.

8. **Click Show Advanced and configure the Assignment Rules options as needed, then click Save.**

Autoscale SVM details

When you define the autoscale SVM settings, the SVM deployment starts automatically depending on the number of clients connecting to the **Trellix MOVE AntiVirus** SVM for protection.

You can view the SVM deployment mode, its status, and the purging details on the **Autoscale SVM Details** page.

Option	Description
Preset	You can select an option to filter and display the deployed SVM modes: • **All** — Filters and displays all SVMs deployed using the autoscale deployment. • **Standby** — Filters and displays all standby SVMs. • **Ready** — Filters and displays all ready SVMs. • **Running** — Filters and displays all running SVMs.
Hostname	Host name of the deployed **Trellix MOVE AntiVirus** SVM.
Assignment Rule	Specifies the name of assignment rule, which assigns a set of endpoints to a selected SVM or multiple SVMs, so that those clients are protected by the SVM Manager assignment rule.
Infrastructure Group	Specifies whether it is a hypervisor-based or cluster-based infrastructure group.
Version	Specifies the version of the SVM.
SVM Mode	Specifies the mode of the deployed SVM:

Option	Description
	• **Standby** — Standby SVMs are created and ready to transition to the backup SVM mode. The standby SVMs are automatically deployed based on the backup SVM value. These SVMs are turned off. • **Ready** — Backup SVMs that are ready to protect your client systems. Calculate the number of ready SVMs required for the maximum number of clients that need protection at any time of the day. These SVMs are powered on, but are not protecting the client systems. • **Running**— These SVMs are currently protecting the client systems.
SVM Status	Specifies whether the SVMs are running.
Action	• **Delete** — Deletes the selected SVMs. • **Upgrade Standby SVMs** — Removes the existing standby SVMs and deploys the new standby SVMs with the latest OVF template.

Deploy the Trellix MOVE AntiVirus client

Deploy the client package to virtual machines using **Trellix ePO - On-prem**, so that **Trellix ePO - On-prem** can manage the **Trellix MOVE AntiVirus** configuration on client systems.

Before you begin

Make sure that:

- The **Trellix Agent** must already be deployed to target virtual systems.
- You installed the **Trellix MOVE AntiVirus** extension on the **Trellix ePO - On-prem** server.
- Make sure that your VMware vCenter account is synced successfully.
- You deployed the SVM Manager using **Trellix ePO - On-prem**.
- (If you are using autoscale SVM) You exported an SVM OVF template and configured SVM autoscale settings.
- (If you are not using autoscale SVM) You deployed the **Trellix MOVE AntiVirus** SVM package to target virtual systems.
- Make sure that the SVMs are communicating with the SVM Manager and are ready to protect new clients.
- Make sure that your virtual machines are turned on where you want to deploy **Trellix MOVE AntiVirus** client.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Systems → System Tree.**

3. **In the System Tree, select the virtual machines where you want to deploy the client package.**
4. **From Actions, select MOVE → Deploy Client [Multi-Platform] to open the Client Deployment Configuration page.**
5. **Under Client Configuration for Client Package, select Trellix MOVE AV [Multi-Platform] Client 4.10.x..**

   You can view all SVM Assignment Rules, if the selected client systems are part of the assignment rules.
6. **Click Proceed to open the Deployment Confirmation dialog box.**

   A message shows the number of systems that are compatible and non-compatible for the client deployment.
7. **Review the message, then click OK to deploy the client package to the compatible client systems.**

   A deployment task is created for all selected systems. Go to **Deployment Status** tab under the **MOVE AntiVirus Deployment** wizard to view the **Passed** or **Failed** tasks with their details.

   If you click **Cancel**, the deployment task is created only for the non-compatible client systems, and the failure reasons can be viewed on the **Deployment Status** tab under the **MOVE AntiVirus Deployment** wizard.

   Note

   Reboot the system after installing **Trellix MOVE** client software.

Results

For compatible client systems, the SVM Manager IP address is updated in the respective **Options** policy, then the SVM Manager assigns an SVM for the clients to protect them.

Note

When the **Trellix MOVE AntiVirus** client is present, disable **Endpoint Security** Threat Protection. Deploying two AntiVirus solutions on the same system results in performance impact.

Check the Trellix MOVE AntiVirus client deployment status

After deploying **Trellix MOVE AntiVirus** client, you can view the deployment details on the **Deployment Status** tab under **MOVE AntiVirus Deployment** wizard on the **Trellix ePO - On-prem** server.

Before you begin

Make sure that:

- You have installed the **Trellix MOVE AntiVirus** package extension on the **Trellix ePO - On-prem** server.
- You have initiated the **Trellix MOVE AntiVirus** client deployment using **Trellix ePO - On-prem**.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Automation → MOVE AntiVirus Deployment.**
3. **On the Deployment Status tab, you can view the Trellix MOVE AntiVirus client deployment details.**
4. **Click any of the Deploy client and enable protection jobs to view these Task Status Details.**

Job status

Item	Description
Start Time	Indicates the date and time when the **Trellix MOVE AntiVirus** client deployment started
End Time	Indicates the date and time when the **Trellix MOVE AntiVirus** client deployment ended
Deployment Type	Displays the **Trellix MOVE AntiVirus** client deployment type as **Deploy client and enable protection**
Status	Specifies the deployment status such as **Started**, **In Progress**, **Completed**, and **Failed**
vCenter Name/IP address	Specifies the IP address of the **Trellix MOVE AntiVirus** client system
Hypervisors/Hostname	Specifies the host name of the **Trellix MOVE AntiVirus** client system

"Task status details" \ Guest Tab

Item	Description
Node Type	Specifies the node type as **Endpoint**
Task Type	Specifies the set of internal tasks that happen in a deployment job. The task list for one job is displayed in sequence with **Start Time**, **End Time**, and **Failure Reasons**, if applicable
Node Name	Displays the host name of the **Trellix MOVE AntiVirus** client system.

Item	Description
Status	Specifies the task status such as **Started**, **In Progress**, **Completed**, **Skipped**, and **Failed**
Failure Reason	Specifies the reason for the failure of the task
Start Time	Indicates the date and time when the task started
End Time	Indicates the date and time when the task ended

During Trellix MOVE AntiVirus client deployment

Task type	Description
Updating Options policy	Updates the IP address of the SVM Manager in the respective Options policies that are assigned to the clients.
Deploying client	Indicates that the **Trellix MOVE AntiVirus** client deployment is in progress.
Connecting to SVM Manager	Specifies that the **Trellix MOVE AntiVirus** client is communicating to the SVM Manager.
Assigning SVM to endpoint	Assigns the **Trellix MOVE AntiVirus** SVM to the client system.
Connecting to SVM	Specifies that the client is communicating to the **Trellix MOVE AntiVirus** SVM.
Testing EICAR	Tests EICAR on the **Trellix MOVE AntiVirus** client system on which the **Trellix MOVE AntiVirus** client deployment is successful.

Deploy client in a Virtual Desktop Infrastructure environment

When operating in a Virtual Desktop Infrastructure (VDI) environment, follow these steps to create a primary image of a client system and clone the virtual machines.

Before you begin

Make sure that:

- The **Trellix Agent** is installed on the primary image.
- The **Trellix MOVE AntiVirus** client is in the Main Repository.

Task

1. **Deploy the Trellix MOVE AntiVirus client to the primary image.**
2. **Configure and apply Trellix MOVE AntiVirus policies to the primary image.**
3. **Run the targeted on-demand scan on the primary image to build up the cache.**
   Building up the cache on the primary image improves the performance of the VDI when you clone the virtual machines.
4. **In the primary image, delete the registry key `AgentGUID` from the location determined by your Windows operating system.**
   - **32-bit — HKEY_LOCAL_MACHINE\SOFTWARE\Network Associates\ePolicy Orchestrator\Agent (32-bit)**
   - **64-bit — HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Network Associates\ePolicy Orchestrator\Agent (64-bit)**
5. **In the primary image, under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mvagtdrv\Parameters, delete the data for ServerAddress1, ServerAddress2, and ODSUniqueId.**
6. **Shut down the primary image and clone the virtual machines from the primary image.**

Results

When cloned virtual machines are turned on, new agent GUID values are automatically generated. The virtual machines are now managed by the **Trellix ePO - On-prem** server.

Deploy the Trellix MOVE AntiVirus Multi-Platform client 4.10 with Endpoint Security Threat Prevention

Deploy the client package to virtual machines using **Trellix ePO - On-prem**, so that **Trellix ePO - On-prem** can manage the **Trellix MOVE AntiVirus** configuration on client systems. The co-existence of **Trellix MOVE AntiVirus** and **Endpoint Security Threat Prevention** is a replacement for **MOVE** + HIPS configuration because of the HIPS EOL announcement.

Before you begin

Make sure that:

- The **Trellix Agent** must already be deployed to target virtual systems.
- You installed the **Trellix MOVE AntiVirus** extension on the **Trellix ePO - On-prem** server.
- Make sure that your VMware vCenter account is synced successfully.
- You deployed the SVM Manager using **Trellix ePO - On-prem**.
- (If you are using autoscale SVM) You exported an SVM OVF template and configured SVM autoscale settings.
- (If you are not using autoscale SVM) You deployed the **Trellix MOVE AntiVirus** SVM package to target virtual systems.

- Make sure that the SVMs are communicating with the SVM Manager and are ready to protect new clients.
- Make sure that your virtual machines are turned on where you want to deploy **Trellix MOVE AntiVirus** client.
- The client machine has ENS 10.7.0 installed with June 2021 Update or later.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Systems → System Tree.**
3. **In the System Tree, select the virtual machines where you want to deploy the client package.**
4. **From Actions, select Agent → Run Client Task Now to open the Run Client Task Now page.**
5. **In the Run Client Task Now:**
   a. **For Product, select Trellix Agent.**
   b. **For Task Type, select Product Deployment.**
   c. **For Task Name, select Create New Task.**
   d. **Check if Target Platforms is Windows only.**
   e. **For Products and components, select Trellix Move AV [Multi-Platform] Client 4.10.x or later Trellix MOVE AntiVirus client version and in the Command Line, enter `KEEPENS=1`.**
   f. **In the bottom right corner, click Run Task Now.**

   You can see the status of the installation in the **Running Client Task Status** page.
6. **Reboot the system after installing Trellix MOVE client software.**

Results

If you see the **Status** as **Completed** on the **Running Client Task Status** page, the **MOVE AntiVirus** installation on your client machine is finished.

Note

This solution is only for **MOVE** + **Endpoint Security** exploit prevention function only. All other **Endpoint Security Threat Prevention** functions such as: On Access scan, On Demand Scan and Access Protection aren't supported.

Configuring Policies and Settings for MOVE Multi Platform

Create policies and settings on Trellix ePO - On-prem

Policies and setting need to be created and configured for **Trellix MOVE AntiVirus** 4.10.x.x. This can be done under the **Policy Catalog** in **Trellix ePO - On-prem**. The Multi Platform client assigned with the created policies and settings will be protected based on the set configuration.

Create an On Access Scan policy

After you deploy the **Trellix MOVE M-Platform** to the clients from the **Trellix ePO - On-prem** server, you need to create an **On Access Scan** policy. This policy is used to Enable/Disable On Access Scan, Enable/Disable Deferred Scan, File types to Scan, Path Exclusion, Process Exclusion, and Publisher Exclusion.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Policy → Policy Catalog.**
3. **Select MOVE AntiVirus 4.10.x from the Product drop-down list, then click New Policy.**

   The **Create a new policy** dialog box appears on the screen.
4. **In the Create a new policy, select On Access Scan from the Category drop-down list.**
5. **Select My Default from the Create a policy based on this existing policy drop-down list.**
6. **Enter the name of your policy in Policy Name.**
7. **Click OK to save the policy.**

Results

The new **On Access Scan** policy page appears on the screen with all the parameters and their values. As per your requirements, edit the values of the parameters and click **Save** otherwise click **Cancel**.

Create an On-Demand scan policy

After you deploy the **MOVE** Multi Platform AntiVirus to the clients from the **Trellix ePO - On-prem** server, you need to create an On-Demand Scan policy. Use this policy to enable or disable On Access Scan, Deferred Scan, File types to Scan, and Path Exclusion.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Policy → PolicyCatalog.**
3. **Select MOVE AntiVirus 4.10.x from the Product drop-down list, then click New Policy.**

   The **Create a new policy** dialog box appears on the screen.
4. **In Create a new policy, select On Demand Scan from the Category drop down list.**
5. **Select My Default from the Create a policy based on this existing policy drop down list**
6. **Enter the name of your policy in Policy Name.**
7. **Click OK to save the policy**

   The new **On Demand Scan** policy page appears on the screen with all the parameters and their values.

   As per your requirements, edit the values of the parameters and click **Save** otherwise click **Cancel.**

Create an On-Demand scan task on individual folder

After you deploy the **Trellix MOVE AntiVirus** Multi Platform to the clients from the **Trellix ePO - On-prem** server, you can run on-demand scan at individual folder level.

Task

1. **Log on to the Trellix ePO - On-prem server as an administrator.**
2. **Select Menu → Policy → Client Task Catalog.**
3. **From Client Task Types, select MOVE AntiVirus 4.10.x → Targeted On-Demand Scan [Multi-Platform].**
4. **Click the name of an existing client task or click New Task, then confirm the task type.**

5. **Configure the Task Name and Description on each tab. Also provide Folder Path (Optional), then click Save**
6. **Configure Task Name and Description on each tab, then click Save.**

   Note

   Specify the path in **Folder Path (Optional)** to run on-demand scan on individual folders.

7. **Click Assign, specify the servers where you want to assign the task, then click OK.**
8. **Click Schedule to schedule the task.**

Create an Options policy

After you deploy the **MOVE** Multi Platform AntiVirus to the clients from the **Trellix ePO - On-prem** server, you need to create an Options policy. Using this policy, you can assign SVM manager or SVM to Multi-Platform clients.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Policy → PolicyCatalog.**
3. **Select MOVE AntiVirus 4.10.x from the Product drop-down list, then click New Policy.**

   The **Create a new policy** dialog box appears on the screen.
4. **In Create a new policy, select Options from the Category drop-down list.**
5. **Select My Default from the Create a policy based on this existing policy drop-down list.**
6. **Enter the name of your policy in Policy Name.**
7. **Click OK to save the policy**

   The new **Options** policy page appears on the screen with all the parameters and their values.

8. **On the policy settings page, click Show Advanced to see all the settings**
9. **Under SVM Assignment (Multi-Platform only) on the policy settings page:**
   a. **Click on Assign SVM using SVM Manager and provide the IP address/host name and the port (If SVM Manager need to be assigned) OR**
   b. **Click on Assign SVM manually and provide the IP address/host name and the port for SVM-1 and SVM-2 (If SVM need to be assigned instead of SVM Manager)**
   c. **Click Save to save the new settings to your Options policy**

   As per your requirements, edit the values of the parameters and click **Save** otherwise click **Cancel.**

Create SVM settings policy

After you deploy the **MOVE** Multi Platform AntiVirus to the clients from the **Trellix ePO - On-prem** server, you need to create a policy for SVM settings policy. Using this policy, you can configure the ODS scheduler, Scanning options and other options.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Policy → PolicyCatalog.**
3. **Select MOVE AntiVirus 4.10.x from the Product drop-down list, then click New Policy.**

The **Create a new policy** dialog box appears on the screen.

4. **In Create a new policy, select SVM Settings from the Category drop-down list.**
5. **Select My Default from the Create a policy based on this existing policy drop-down list**
6. **Enter the name of your policy in Policy Name.**
7. **Click OK to save the policy**

   The new **SVM Settings** policy page appears on the screen with all the parameters and their values.

   As per your requirements, edit the values of the parameters and click **Save** otherwise click **Cancel.**

Create a Certificates policy

After you deploy the **Trellix MOVE for Multi-Platform** AntiVirus to the clients from the **Trellix ePO - On-prem** server, you need to create a Certificate policy. Using this policy, you can add the trusted certificates.

The Certificates policy option allows you to add certificates in the policy. Once you add the certificate, all files that are signed by the listed certificates are excluded from on-access and on-demand scanning.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Policy → PolicyCatalog.**
3. **Select MOVE AntiVirus 4.10.x from the Product drop-down list, navigate to Certificates (Multi-Platform only) policy.**
4. **In Create a new policy, select SVM Manager Settings from the Category drop-down list.**
5. **Select My Default and edit the My Default policy.**
   As per your requirements, edit the values of the parameters and click **Save** otherwise click **Cancel.**

Create a Shared Cloud Solutions policy

After you deploy the **Trellix MOVE for Multi-Platform** AntiVirus to the clients from the **Trellix ePO - On-prem** server, you can create a Shared Cloud Solutions policy. Using this policy, you can configure **Threat Intelligence Exchange** and **Intelligent Sandbox** settings.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Policy → PolicyCatalog.**
3. **Select MOVE AntiVirus 4.10.x from the Product drop-down list, then click New Policy.**
   The **Create a new policy** dialog box appears on the screen.
4. **In Create a new policy, select Shared Cloud Solutions from the Category drop-down list.**
5. **Select My Default from the Create a policy based on this existing policy drop-down list**
6. **Enter the name of your policy in Policy Name.**
7. **Click OK to save the policy**

   The new **Shared Cloud Solutions** policy page appears on the screen with all the parameters and their values.

   As per your requirements, edit the values of the parameters and click **Save** otherwise click **Cancel.**

Create a SVM Manager settings policy

After you deploy the **Trellix MOVE for Multi-Platform** AntiVirus to the clients from the **Trellix ePO - On-prem** server, you need to create a policy for SVM Manager settings policy. Using this policy, you can configure the ODS scheduler, Scanning options and other options.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Policy → PolicyCatalog.**
3. **Select MOVE AntiVirus 4.10.x from the Product drop-down list, then click New Policy.**
   The **Create a new policy** dialog box appears on the screen.
4. **In Create a new policy, select SVM Manager Settings from the Category drop-down list.**
5. **Select My Default from the Create a policy based on this existing policy drop-down list**
6. **Enter the name of your policy in Policy Name.**
7. **Click OK to save the policy**

   The new **SVM Manager Settings** policy page appears on the screen with all the parameters and their values.

   As per your requirements, edit the values of the parameters and click **Save** otherwise click **Cancel.**

Upgrade Trellix MOVE AntiVirus

Upgrade from Trellix MOVE AntiVirus 4.9.x

If a supported version of **Trellix MOVE AntiVirus** is installed in your environment, you can upgrade to **Trellix MOVE AntiVirus** 4.10.x.

The **Trellix MOVE AntiVirus** 4.10.x upgrade these components:

- **Trellix MOVE AntiVirus** extensions.
- **Trellix MOVE AntiVirus** SVM Manager.
- **Trellix MOVE AntiVirus** SVM.
- **Trellix MOVE AntiVirus** Client.

Upgrade the extension

Version 4.10.x of the **Trellix MOVE AntiVirus** extension upgrades the 4.9.x extension on the **Trellix ePO - On-prem** server.

Before you begin

Make sure the extension file in an accessible location on the network.

All policies created in version 4.9.x exist after you upgrade to version 4.10.x.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Software → Extensions.**

3. **Click Install Extension.**
4. **Browse to and select the extension file, then click OK.**
5. **After a confirmation message, click OK.**

Upgrade the SVM Manager

In-place upgrade from version 4.9.x to 4.10.x is supported, the version 4.10.x of the SVM Manager upgrades over the 4.9.x SVM Manager on your hypervisor. Once the new 4.10.x SVM Manager is up and running, the existing 4.9.x SVM Manager is turned off.

Before you begin

Make sure that:

- The VMware vCenter account is synced successfully.
- You have configured the Infrastructure Group. For details, see *Create or edit an infrastructure group in **Trellix ePO - On-prem** for SVM Manager deployment*.
- The SVM Manager package (**MOVE-AV-MP_SVM_Manager_Pkg.4.10.x.zip**) is in an accessible location on the network.
- You have not removed the existing SVM Manager IP address in respective options policy.

Note

The **MOVE** SVM Manager upgrade from older versions to 4.10.x using Debian package is not supported.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Systems → System Tree.**
3. **In the System Tree, select the virtual machines where you want to deploy the SVM Manager package.**
4. **Click Actions → Agent → Run Client Task Now to open the Run Client Task Now page.**
5. **Perform these tasks to run the client task:**
   a. **In the Product drop-down list, select Trellix Agent.**
   b. **In the Task Type, select Product Deployment.**
   c. **In the Task Name, click Create New Task to create the new task.**

   The **Run Client Task Now** window opens on the screen.
6. **Perform these steps to create a task in the Run Client Task Now window:**
   a. **From the Target Platforms checkboxes, select Linux only.**
   b. **In the Products and components dropdown list, select Trellix MOVE AV [Multi-Platform] SVM Manager 4.10.x.xx.**
7. **Click Run Task Now to deploy the SVM Manager.**

Results

You can see the status of the installation in the Running Client Task Status page. If you see the **Status** as **Completed** on the **Running Client Task Status** page, the **Trellix MOVE AntiVirus** SVM Manager 4.10.x upgraded on your virtual machine.

Upgrade the SVM with Trellix ePO - On-prem (without autoscale SVM)

Create an SVM deployment client task for upgrade

Create an SVM deployment client task, so that you can assign that task to SVMs.

Before you begin

Make sure that:

- The **Trellix MOVE AntiVirus**extensions upgrade are successful.
- The SVM Manager upgrade is successful.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Policy → Client Task Catalog.**
3. **Select Product Deployment in the Client Task Types menu, then select Actions → New Task.**
4. **Select Product Deployment from the list, then click OK to open the Client Task Builder wizard.**
5. **Type a name for the task you are creating, and add any descriptive information in the Description field.**
6. **Make sure that Windows is the only target platform selected.**
7. **For Products and components:**
   a. **For SVM, select Trellix MOVE AV [Multi-Platform] SVM 4.10.x from the drop-down list.**
   b. **Set the action to Install, set the language to Language Neutral, and set the branch to Current.**
   c. **Leave the Command line setting blank.**
8. **Review the task settings, then click Save.**

Results

The task is added to the list of client tasks for the selected client task type.

Assign an SVM deployment client task for upgrade

After creating the SVM deployment client task, you must assign that task to the SVMs.

Before you begin

Make sure that the **Trellix Agent** and **Endpoint Security** is already deployed to target virtual systems.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Policy → Client Task Assignments, then click the Assigned Client Tasks tab.**
3. **Click Actions → New Client Task Assignment.**
4. **Configure these settings, then click Next.**
   - **Product — Trellix Agent**
   - **Task Type — Product Deployment**
   - **Task Name** — The name of the task you used when you created the client task
5. **On the Schedule tab, specify the schedule for running the client task, then click Next.**
6. **Examine the settings on the Summary tab, then click Save to assign the task.**

Results

The **Trellix MOVE AntiVirus** SVM is deployed to systems in the selected group in the System Tree.

Upgrade the SVM with Trellix ePO - On-prem (with autoscale SVM)

You must export an SVM OVF template with 4.10.x SVM installed on it, so that your primary image of the SVM has latest version.

Before you begin

- Make sure that your SVM Manager upgrade is successful.
- You exported your latest SVM OVF template and checked in to the **Trellix ePO - On-prem** server and the SVM OVF details appear on the **SVM Configuration** page under **MOVE AntiVirus Deployment** wizard. For details, see *Configuring an SVM OVF template for autoscaling*.
- You configured your Infrastructure Group. For details, see *Create or edit an infrastructure group in **Trellix ePO - On-prem** for SVM autoscaling*.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Policy → Policy Catalog, then select Trellix MOVE AntiVirus 4.10.x from the Product list.**
3. **From the Category list, select SVM Manager Settings.**
4. **Click the name of the policy that you are currently using for SVM autoscaling.**
5. **From SVM Autoscale Settings, deselect Enable auto scaling of SVMs.**

Note

Disabling this option disappears all running, ready, and standby SVMs from the **Autoscale SVM Details** page under **MOVE AntiVirus Deployment** wizard. Also, delete all ready and standby SVMs, but the running SVMs continue to protect the client systems.

6. **Select Menu → Systems → System Tree.**
7. **Identify the VM or SVM that you used to export SVM OVF template, then delete it.**
8. **From SVM Autoscale Settings, again select Enable auto scaling of SVMs.**

Results

The new ready and standby SVMs are deployed. Once the new ready and standby SVMs are up, the existing running SVMs are deleted.

Upgrade the Trellix MOVE AntiVirus client

Version 4.10.x of the **Trellix MOVE AntiVirus** client upgrades the 4.9.x clients.

Before you begin

Make sure that:

- The VMware vCenter account is synced successfully.
- The client systems are turned on where you want to deploy **Trellix MOVE AntiVirus** client.

- The SVM Manager upgrade is successful.
- The SVM upgrade is successful.

Note

You can also upgrade clients by creating an upgrade client task and assigning that task to virtual machines.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Systems → System Tree.**
3. **In the System Tree, select the virtual machines where you want to deploy the client package.**
4. **From Actions, select MOVE → Deploy Client [Multi-Platform] to open the Client Deployment Configuration page.**
5. **Under Client Configuration for Client Package, select Trellix MOVE AV [Multi-Platform] Client 4.10.x.**

   You can view all SVM Assignment Rules, if the selected client systems are part of the assignment rules.
6. **Click Proceed to open the Deployment Confirmation dialog box.**

   A message shows the number of systems that are compatible and non-compatible for the client deployment.
7. **Review the message, then click OK to deploy the client package to the compatible client systems.**

   A deployment task is created for all selected systems. Go to **Deployment Status** tab under the **MOVE AntiVirus Deployment** wizard to view the **Passed** or **Failed** tasks with their details.

   If you click **Cancel**, the deployment task is created only for the non-compatible client systems, and the failure reasons can be viewed on the **Deployment Status** tab under the **MOVE AntiVirus Deployment** wizard.

   Note

   After upgrading the **Trellix MOVE AntiVirus** software, reboot the system.

   For the compatible client systems, if the SVM Manager IP address is updated in the respective **Options** policy, then the SVM Manager assigns an SVM for the clients to protect them.

Job status

Item	Description
Start Time	Indicates the date and time when the **Trellix MOVE AntiVirus** client deployment started
End Time	Indicates the date and time when the **Trellix MOVE AntiVirus** client deployment ended

Item	Description
Deployment Type	Displays the **Trellix MOVE AntiVirus** client deployment type as **Deploy client and enable protection**
Status	Specifies the deployment status such as **Started**, **In Progress**, **Completed**, and **Failed**
vCenter Name/IP address	Specifies the IP address of the **Trellix MOVE AntiVirus** client system
Hypervisors/Hostname	Specifies the host name of the **Trellix MOVE AntiVirus** client system

Task status details

Item	Description
Node Type	Specifies the node type as **Endpoint**
Task Type	Specifies the set of internal tasks that happen in a deployment job. The task list for one job is displayed in sequence with **Start Time**, **End Time**, and **Failure Reasons**, if applicable
Node Name	Displays the host name of the **Trellix MOVE AntiVirus** client system.
Status	Specifies the task status such as **Started**, **In Progress**, **Completed**, **Skipped**, and **Failed**
Failure Reason	Specifies the reason for the failure of the task
Start Time	Indicates the date and time when the task started
End Time	Indicates the date and time when the task ended

During Trellix MOVE AntiVirus client deployment

Task type	Description
Updating Options policy	Updates the IP address of the SVM Manager in the respective Options policies that are assigned to the clients.
Deploying client	Indicates that the **Trellix MOVE AntiVirus** client deployment is in progress.
Connecting to SVM Manager	Specifies that the **Trellix MOVE AntiVirus** client is communicating to the SVM Manager.
Assigning SVM to endpoint	Assigns the **Trellix MOVE AntiVirus** SVM to the client system.
Connecting to SVM	Specifies that the client is communicating to the **Trellix MOVE AntiVirus** SVM.
Testing EICAR	Tests EICAR on the **Trellix MOVE AntiVirus** client system on which the **Trellix MOVE AntiVirus** client deployment is successful.

Upgrade persistent virtual machines

Upgrading persistent virtual machines provides nearly seamless virus protection, but requires the overhead of duplicate SVMs during the upgrade process.

We recommend this method for environments made up primarily of persistent virtual machines, where the clients require support from the SVM during the client migration process.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Check in and install the Trellix MOVE AntiVirus 4.10.x extension in Trellix ePO - On-prem.**
3. **Create a new virtual server and install Endpoint Security 10.7.x or later on that server.**
4. **Install SVM version 4.10.x on the virtual server.**
5. **Create a new Trellix MOVE AntiVirus 4.10.x policy that references the SVM you created, and assign it to the virtual machines being upgraded.**
6. **Create a Trellix ePO - On-prem client task to upgrade the Trellix MOVE AntiVirus clients to version 4.10.x.**
   As the upgrade task is executed on virtual machines, the VMs begin to use the 4.10.x SVM for file scanning.

7. **After all clients are upgraded to version 4.10.x, shut down the older versions of the SVM.**

Note

> After upgrading the **Trellix MOVE AntiVirus** software, reboot the system.

Upgrade non-persistent virtual machines

Upgrading non-persistent virtual machines does not require creating additional SVMs, although it might result in a window of time when virtual machines are unprotected.

We recommend that you perform this upgrade during scheduled downtime.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Install the Trellix MOVE AntiVirus 4.10.x client package and Trellix MOVE AntiVirus 4.10.x SVM packages and upgrade the extensions in Trellix ePO - On-prem.**
3. **Create a new 4.10.x client policy definition that references existing SVM systems.**
4. **From the Trellix ePO - On-prem console, upgrade all SVMs to version 4.10.x.**

Caution

> Virtual machines serviced by upgraded SVMs do not have anti-virus protection until after this task is completed.

5. **Change the primary image by deploying version 4.10.x of the Trellix MOVE AntiVirus client from Trellix ePO - On-prem, or by manually upgrading the client directly on the primary image.**

Note

> After upgrading the **Trellix MOVE AntiVirus** software, reboot the system.

Upgrade the Trellix MOVE AntiVirus client with Endpoint Security on Trellix ePO - On-prem

Version 4.10.x of the **Trellix MOVE AntiVirus** client upgrades the 4.9.x clients which have **MOVE** + **Endpoint Security Threat Prevention** combination using **Trellix ePO - On-prem**.

Before you begin

Make sure that:

- The client systems are turned on where you want to deploy **Trellix MOVE AntiVirus** client.
- The client machine has **Endpoint Security** 10.7.0 and MOVE 4.9.x installed.

Note

You can also upgrade clients by creating an upgrade client task and assigning that task to virtual machines.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Systems → System Tree.**
3. **In the System Tree, select the virtual machines where you want to deploy the client package.**
4. **From Actions, select Agent → Run Client Task Now to open the Run Client Task Now page.**
5. **In the Run Client Task Now:**
    a. **For Product, select Trellix Agent.**
    b. **For Task Type, select Product Deployment.**
    c. **For Task Name, select Create New Task.**
    d. **Check if Target Platforms is Windows only.**
    e. **For Products and components, select Trellix Move AV [Multi-Platform] Client 4.10.x or later Trellix MOVE AntiVirus client version and in the Command Line, enter `KEEPENS=1`.**
    f. **In the bottom right corner, click Run Task Now.**

    You can see the status of the installation in the **Running Client Task Status** page.
6. **Reboot the system after installing Trellix MOVE client software.**

Results

If you see the **Status** as **Completed** on the **Running Client Task Status** page, the **Trellix MOVE AntiVirus** upgrade on your client machine is finished.

Post-installation tasks

Update the standby SVMs (Autoscale SVMs)

When the latest SVM OVF template is configured in **Trellix ePO - On-prem**, you can deploy it from **Trellix ePO - On-prem** to all standby SVMs. This is only true for standby SVMs, not for ready and running SVMs.

Before you begin

Make sure that you have created your latest SVM OVF template.

When you click **Update Standby SVMs**, the existing standby SVMs are purged and new standby SVMs are deployed.

When you define the autoscale settings, the **Trellix MOVE AntiVirus** SVM deployment starts automatically depending on the number of clients connecting to the **Trellix MOVE AntiVirus** SVM for protection. You can view SVM deployment mode, its status, and the purging details about the **Autoscale SVM Details** page.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Automation → MOVE AntiVirus Deployment.**
3. **On the Configuration tab, click Autoscale SVM Details to open the Autoscale SVM Details page with the autoscale SVM deployment details.**

4. **Click Actions → Update Standby SVMs.**

Results

This action removes the existing standby SVMs and deploys the new standby SVMs with the latest SVM OVF template.

Generate certificates for Trellix MOVE AntiVirus

If there is a connectivity issue with the SVM Manager, you must generate the certificates for **Trellix MOVE AntiVirus**, so that the SVM and SVM Manager communicate and authenticate each other properly.

Before you begin

Make sure that:

Trellix MOVE AntiVirus uses secure https protocol for communication between **Trellix MOVE AntiVirus** SVM and SVM Manager. For secure https protocol, you must generate the **Trellix MOVE AntiVirus** certificates when the **Trellix ePO - On-prem** certificate is changed, so that the change is reflected in the **Trellix MOVE AntiVirus** policies.

- You have installed the **Trellix MOVE AntiVirus** extension on the **Trellix ePO - On-prem** server.
- You have deployed the SVM Manager.
- You have deployed the **Trellix MOVE AntiVirus** SVM package to the target virtual systems.
- You have deployed the **Trellix MOVE AntiVirus** client package to client systems.
- You have configured your **Trellix ePO - On-prem** details about the **General** page under **Automation** → **MOVE AntiVirus Deployment** → **Configuration**.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Automation → Server Tasks to open Server Tasks page.**
3. **Select MOVE AntiVirus : Generate Certificates query and click Run to generate the Trellix MOVE AntiVirus certificates.**
4. **Select Menu → Systems → System Tree.**
5. **In the System Tree, select the group containing the virtual machines where you want to apply the Trellix MOVE AntiVirus 4.10.x policies.**
6. **To apply the policy immediately, send an agent wake-up call to the client system.**
7. **Log on to the client system as an administrator.**
8. **Run an EICAR test.**
9. **Verify that the SVM sends threat details as threat events to Trellix ePO - On-prem.**

Results

Trellix MOVE AntiVirus certificates are generated successfully and **Trellix MOVE AntiVirus** SVM and SVM Manager are communicating properly.

Integrating TIE and Intelligent Sandbox

TIE provides context-aware adaptive security for your virtual environment. It quickly analyzes files and content from the SVM in your environment and makes informed security decisions.

These decisions are based on a file's security reputation and your own criteria set in the **Shared Cloud Solutions** policy of **Trellix MOVE AntiVirus**.

The Multi-platform deployment, with **TIE** and **Intelligent Sandbox** integration, becomes a multi-layered solution that involves various techniques to scan and detect the malware. It includes:

- Pattern matching
- Global reputation
- Program emulation
- Static analysis
- Dynamic analysis

All these layers are seamlessly integrated and provide a single point of control for easy configuration and management.

TIE and Intelligent Sandbox integration process

The overall **TIE** and **Intelligent Sandbox** integration process of the Multi-platform consists of the following tasks.

1. Install the **TIE** server appliance.
2. Deploy the Data Exchange Layer client to **Trellix MOVE AntiVirus** SVM.
3. Verify the **TIE** server installation.
4. Create a new registered server in **Trellix ePO - On-prem**.
5. Enable **TIE** and **Intelligent Sandbox** protection for **Trellix MOVE AntiVirus**.
6. Verify the **TIE** server integration.
7. Verify the **Intelligent Sandbox** integration.

Deploy the Data Exchange Layer client to Trellix MOVE AntiVirus SVM

You must deploy the **DXL** client to all your **Trellix MOVE AntiVirus** SVMs for **TIE** integration.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Software → Product Deployment, then click New Deployment.**
3. **Complete the new deployment information, then start the deployment.**
4. **Verify that the DXL Connection Status on Trellix ePO - On-prem is Connected.**

Important

> Restart the **Trellix MOVE AntiVirus** SVM service if you deploy the **DXL** Client after deploying the **Trellix MOVE AntiVirus** SVM.

For details about deploying software from **Trellix ePO - On-prem**, see the product documentation for your version of **Trellix ePO - On-prem**.

Verify the TIE server installation

After installing the **Threat Intelligence Exchange** and **Data Exchange Layer** components, verify the installation.

Before you begin

Make sure that you have installed the **TIE** server appliance. For installing and setting-up **TIE**, see the installation guide for your version of **TIE**.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **In the System Tree, click the TIE server name, then click Products. Verify that the following components are listed with the corresponding version for the installation process.**
    - **Trellix DXL** Broker
    - **Trellix DXL** Client
    - **Trellix Threat Intelligence Exchange** Server
3. **In the System Tree, verify that the TIESERVER and DXLBROKER tags were applied to the system.**
4. **Select Menu → Configuration → Server Settings, click DXL ePO Client, then verify that the Connection State is Connected.**
5. **In the System Tree, select the TIE server, then from the Actions menu, select DXL | Lookup in DXL.**
6. **Verify that the Connection State is Connected.**
7. **Log on to the Trellix MOVE AntiVirus SVM system.**
8. **From the system tray, click 🛡 and select About to open the Trellix About window.**
9. **Under McAfee Data Exchange Layer, verify that the DXL Connected Status is Connected.**

Results

The **DXL** broker and **DXL** client communication is now up and running. From **Trellix ePO - On-prem**, you can select **Menu → Systems Section → TIE Reputations** to verify that you can search for files and certificates. It might take some time for reputation information to update the database.

Create a new registered server

To view **TIE** information in **Trellix ePO - On-prem** reports and dashboards, create a new registered server in **Trellix ePO - On-prem**.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Configuration → Registered Servers, then click New Server.**
3. **In the Server type drop-down list, select Database Server.**
4. **Enter a Name, for example, `TIE Server`, then click Next.**
5. **On the Details page:**
    - Select **Make this the default database for the selected database type**. This option is automatically selected when you create the first registered server. If you have more than one **TIE** database, select this option only for the database that you want as the default.

- In the **Database Vendor** field, select **TieServerPostgres**.
- In the **Host name or IP address** field, enter the IP address of the **TIE** server.
- Leave the **Database server instance** and **Database server port** fields blank (if they appear).
- For the **Database** name, enter `tie`.
- In the **User name** and **password** fields, enter the read-only postgress user name and password that you specified on the PosgresSQL page during the server installation.

6. **Click Test Connection.**
7. **Click Save.**

Results

Trellix ePO - On-prem communicates with the server and retrieves data for the reports and dashboards.

Enable TIE and Intelligent Sandbox protection for Trellix MOVE AntiVirus

Files and certificates have threat reputations based on their content and properties. The **Shared Cloud Solutions** policy determines whether files and certificates are blocked or allowed on systems in your environment based on reputation levels.

Before you begin

Make sure that:

- You have installed **TIE** and **Intelligent Sandbox** to integrate them with **Trellix MOVE AntiVirus**.
- You have installed the **Trellix MOVE AntiVirus** extension on the **Trellix ePO - On-prem** server.

File and certificate reputation is determined when a file tries to run on a managed system. For details about how to install and set up the **TIE** requirements, see the product documentation for your version of **TIE**.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Policy → Policy Catalog, select MOVE AntiVirus 4.10.x from the Product drop-down list, then select Shared Cloud Solutions from the Category drop-down list.**
3. **From Enable TIE, select Enabled to determine file and certificate reputation when a Portable Executable (PE) file is accessed on a managed endpoint.**
   PE file includes these formats: .cpl, .exe, .dll, .ocx, .sys, .scr, .drv, .efi, .fon
4. **From TIE Non-PE Lookup, select Enabled to determine file and certificate reputation when a non-PE file is accessed on a managed endpoint.**

   Note

   To enable **TIE Non-PE Lookup**, make sure that you selected **Enable TIE** option.

5. **Under Threat Intelligence Exchange (TIE), configure these reputation settings for files and certificates.**

Select this...	To do this...
Known malicious	Perform scan action for **Known malicious**, **Most likely malicious**, **Might be malicious**, **Unknown**, **Might be trusted**, and **Most likely trusted** files based on threat detection response specified in **On Access Scan** or **On Demand Scan** policies
Most likely malicious	• Perform threat detection response actions specified in **On Access Scan** or **On Demand Scan** policies for files **Known malicious** based on their TIE reputation score • Perform scan action for **Most likely malicious**, **Might be malicious**, **Unknown**, **Might be trusted**, and **Most likely trusted** files based on threat detection response specified in **On Access Scan** or **On Demand Scan** policies
Might be malicious	• Perform threat detection response actions specified in **On Access Scan** or **On Demand Scan** policies for files **Known malicious** and **Most likely malicious** based on their TIE reputation score • Perform scan action for **Might be malicious**, **Unknown**, **Might be trusted**, and **Most likely trusted** files based on threat detection response specified in **On Access Scan** or **On Demand Scan** policies
Unknown	• Perform threat detection response actions specified in **On Access Scan** or **On Demand Scan** policies for files **Known malicious**, **Most likely malicious**, and **Might be malicious** based on their TIE reputation score • Perform scan action for **Unknown**, **Might be trusted**, and **Most likely trusted** files based on threat detection response specified in **On Access Scan** or **On Demand Scan** policies

Select this...	To do this...
Might be trusted	• Perform threat detection response actions specified in **On Access Scan** or **On Demand Scan** policies for files **Known malicious**, **Most likely malicious**, **Might be malicious**, and **Unknown** based on their TIE reputation score • Perform scan action for **Might be trusted** and **Most likely trusted** files based on threat detection response specified in **On Access Scan** or **On Demand Scan** policies
Most likely trusted	• Perform threat detection response actions specified in **On Access Scan** or **On Demand Scan** policies for files **Known malicious**, **Most likely malicious**, **Might be malicious**, **Unknown**, and **Might be trusted** based on their TIE reputation score • Perform scan action for **Most likely trusted** files based on threat detection response specified in **On Access Scan** or **On Demand Scan** policies

Based on the file **TIE** reputation score, the SVM performs threat detection responses specified in the **On Access Scan** or **On Demand Scan** policies for files the TIE reputation score is higher than the threshold defined in OAS/ODS policy. The SVM performs the scan action for selected files based on the threat detection response specified in OAS/ODS policies.

6. **From Advanced Threat Defense (ATD), select Submit files to ATD at and below to send files with these reputation scores to Intelligent Sandbox for further analysis.**

    - Most likely malicious
    - Unknown
    - Most likely trusted

    For example, if the file hash is not found in the **TIE** server, the **TIE** server queries **Trellix GTI** for the file hash reputation. **Trellix GTI** sends the information that is available, for example "unknown reputation." The **TIE** server stores that information and sends the same to SVM.

    If **Submit files to ATD at and below** is enabled and the file is determined as an **Intelligent Sandbox** candidate by **TIE** server, SVM sends the file to **Intelligent Sandbox** through the **TIE** server for analyzing.

Verify the TIE server integration

Verify the **TIE** integration before configuring and using the scan policies to detect malware.

Before you begin

Make sure that you have installed the **TIE** server and configured **Threat Intelligence Exchange (TIE)** option under the **Shared Cloud Solutions** policy on the **Trellix ePO - On-prem** server.

Task

1. **Log on to the Trellix MOVE AntiVirus client system as an administrator.**
2. **Run an EICAR test.**
3. **Log on to Trellix ePO - On-prem as an administrator.**
4. **Select Menu → Reporting → Threat Event Log.**
5. **Under Threat Type, verify that Virus detected using TIE appears.**

Verify the Intelligent Sandbox integration

Verify the **Intelligent Sandbox** integration before configuring and using the scan policies to detect malware.

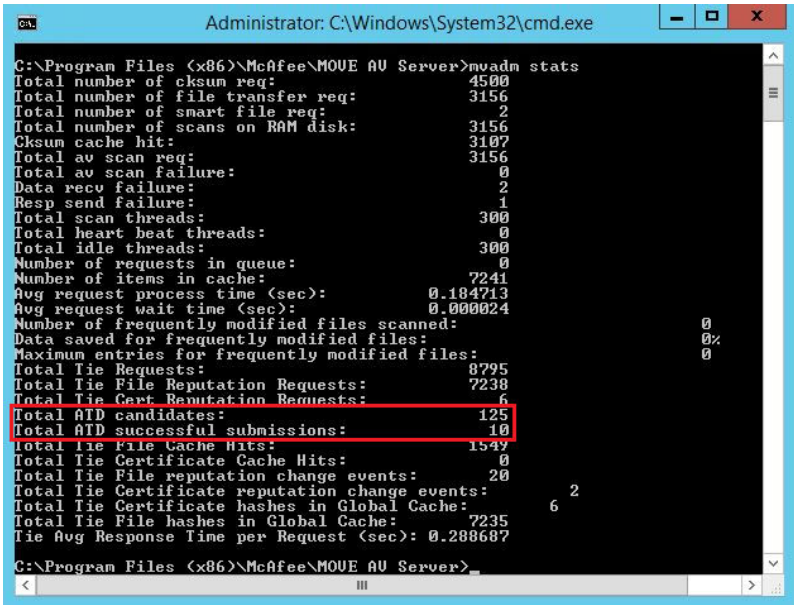
Before you begin

Make sure that you have installed **Intelligent Sandbox** and configured the **Advanced Threat Defense (ATD)** option under the **Shared Cloud Solutions** policy on the **Trellix ePO - On-prem** server.

Task

1. **Log on to the Trellix MOVE AntiVirus SVM.**
2. **Run this command:**

   `mvadm stats`
3. **Verify that `Total ATD candidates` and `Total ATD successful submissions` values appear.**



```
C:\Program Files (x86)\McAfee\MOVE AV Server>mvadm stats
Total number of cksum req:                   4500
Total number of file transfer req:           3156
Total number of smart file req:                 2
Total number of scans on RAM disk:           3156
Cksum cache hit:                             3107
Total av scan req:                           3156
Total av scan failure:                          0
Data recv failure:                              2
Resp send failure:                              1
Total scan threads:                           300
Total heart beat threads:                       0
Total idle threads:                           300
Number of requests in queue:                    0
Number of items in cache:                    7241
Avg request process time (sec):          0.184713
Avg request wait time (sec):             0.000024
Number of frequently modified files scanned:                        0
Data saved for frequently modified files:                           0%
Maximum entries for frequently modified files:                      0
Total Tie Requests:                          8795
Total Tie File Reputation Requests:          7238
Total Tie Cert Reputation Requests:             6
Total ATD candidates:                         125
Total ATD successful submissions:              10
Total Tie File Cache Hits:                   1549
Total Tie Certificate Cache Hits:               0
Total Tie File reputation change events:       20
Total Tie Certificate reputation change events:        2
Total Tie Certificate hashes in Global Cache:        6
Total Tie File hashes in Global Cache:       7235
Tie Avg Response Time per Request (sec): 0.288687

C:\Program Files (x86)\McAfee\MOVE AV Server>_
```

4. **Log on to Trellix ePO - On-prem as an administrator.**

5. Select Menu → Systems → TIE Reputations.
6. From the File Search tab, under ATD Reputation, verify the Intelligent Sandbox reputation details for the files those were submitted to Intelligent Sandbox.

Uninstall Trellix MOVE AntiVirus

Uninstall the client and SVM

Task

1. Log on to Trellix ePO - On-prem as an administrator.
2. Select Menu → Policy → Client Task Catalog.
3. In the left column under Trellix Agent , select Product Deployment.
4. Click Actions → New Task, select Product Deployment, then click OK.
5. Type the name of the task, like `Uninstall MOVE AV client on VM client`, and an optional description.
6. Make sure that Windows is the only target platform selected.
7. For Products and components, select the following, then click Next.
   a. Select Trellix MOVE AV [Multi-Platform] client 4.10.x or Trellix MOVE AV [Multi-Platform] SVM 4.10.x from the first drop-down list.
   b. Set the action to Remove, set the language to Language Neutral, and set the branch to Current.
   c. Leave the Command Line setting blank.
8. Select the remaining options according to your environment's best practices, then click Save.

Results

The newly created task appears in the **Client Task Catalog**.

Assign the uninstallation task to virtual systems

The uninstallation task for the client and **Trellix MOVE AntiVirus** SVM must be assigned to virtual systems to take effect.

Before you begin

Make sure that the **Trellix MOVE AntiVirus** client and SVM are added to the **Main Repository** and your virtual systems are added to the System Tree.

Task

1. Log on to Trellix ePO - On-prem as an administrator.
2. Select a group in the System Tree.
3. Select Menu → Policy → Client Task Assignments, then click the Assigned Client Tasks tab.
4. Click Actions → New Client Task Assignment.
5. Configure these settings, then click Next.
   - **Product** — Trellix Agent
   - **Task Type** — Product Deployment
   - **Task Name** — The name of the task you created earlier

6. **On the Schedule tab next to Schedule type, select Run Immediately from the drop-down list, set the options as appropriate, then click Next.**
7. **Examine the settings displayed on the Summary tab, then click Save to assign the task.**

Results

The **Trellix MOVE AntiVirus** client is removed from every system in the selected group in the System Tree.

Remove the client or SVM package from Trellix ePO - On-prem

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Software → Main Repository.**
3. **Select MOVE AV [Multi-Platform] client 4.10.x or MOVE AV [Multi-Platform] SVM 4.10.x, then click Delete.**

Remove the SVM Manager

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Automation → MOVE AntiVirus Deployment.**
3. **On the Configuration tab, click SVM Manager Configuration to open the SVM Manager OVF Details page.**
4. **Under Deployment Configuration, click Delete SVM Manager.**

Note

> The **Delete SVM Manager** button is enabled only when the version 4.10.0 of SVM Manager is checked in to the **Trellix ePO - On-prem** server

You can check the deletion status on the **Deployment Status** tab under **MOVE AntiVirus Deployment** wizard on the **Trellix ePO - On-prem** server.

Uninstall the extensions

Uninstall the **Trellix MOVE AntiVirus** extensions from **Trellix ePO - On-prem**.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Software → Extensions.**
3. **From the Extensions tab under McAfee group, select Data Center Security.**
4. **Click Remove next to each extension in this order.**
   - MOVE AntiVirus
   - MOVE AntiVirus Common
   - vSphere Connector Extension
   - MDCC

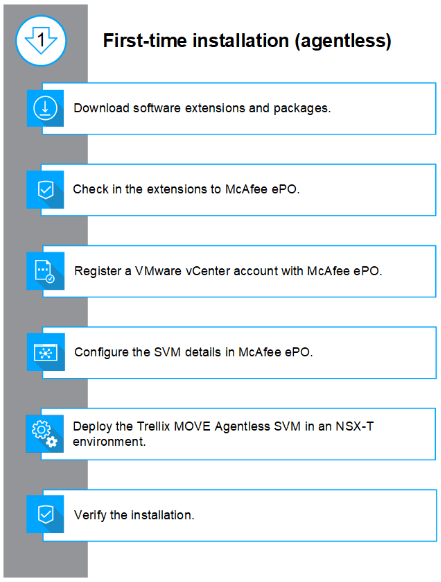
Agentless

Installation overview

The agentless solution integrates with VMware NSX-T Data Center. It addresses the challenges of protecting your VMware virtual machines and keeping it free of malware without a **Trellix** footprint on the client. The agentless deployment provides virus protection for virtual machines on the ESXi hypervisor.

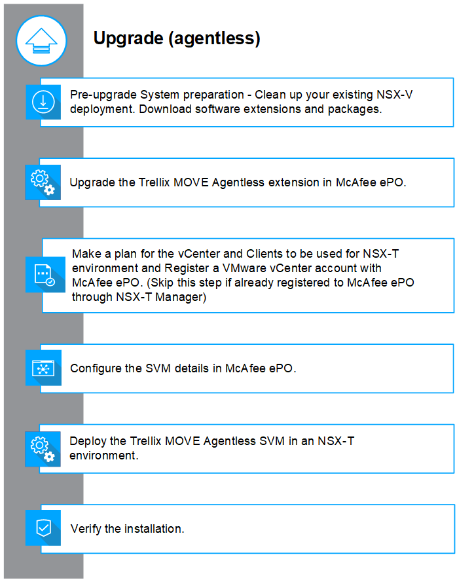
First-time installation workflow (Agentless)

To install and configure the **Trellix MOVE Agentless** environment, refer the first-time installation high-level workflow diagram shown below:


1
First-time installation (agentless)
Download software extensions and packages.
Check in the extensions to McAfee ePO.
Register a VMware vCenter account with McAfee ePO.
Configure the SVM details in McAfee ePO.
Deploy the Trellix MOVE Agentless SVM in an NSX-T environment.
Verify the installation.

Upgrade installation workflow (Agentless)

To upgrade the **Trellix MOVE Agentless** software and remain updated with the new features, see the Upgrade Trellix MOVE Agentless topic and Upgrade Agentless) high-level workflow diagram shown below:



Upgrade (agentless)

Pre-upgrade System preparation - Clean up your existing NSX-V deployment. Download software extensions and packages.

Upgrade the Trellix MOVE Agentless extension in McAfee ePO.

Make a plan for the vCenter and Clients to be used for NSX-T environment and Register a VMware vCenter account with McAfee ePO. (Skip this step if already registered to McAfee ePO through NSX-T Manager)

Configure the SVM details in McAfee ePO.

Deploy the Trellix MOVE Agentless SVM in an NSX-T environment.

Verify the installation.

Planning your Installation

Supported Trellix management platform and software

The **Trellix Agent** and **McAfee® Endpoint Security for Linux** Threat Prevention are preinstalled in SVM Open Virtualization Format (OVF). If required you can update to current version according to Point Product Compatibility Testing (PPCT). You must have specific versions of **Trellix** management platform and software installed as shown below:

Software	Version (Agentless)
Trellix ePO - On-prem For details, see the ***Trellix ePO - On-prem*** *Installation Guide*.	5.10.0 Update 11 or above
vSphere Connector Extension	5.4.0
Trellix Agent	5.7.4 (Part of SVM package)
McAfee® Endpoint Security for Linux Threat Prevention	10.7.0 (Part of SVM package)

SVM OVF requirements (Agentless)

- You must use the virtual machine we provide for Agentless SVM. This system is a dedicated virtual appliance with **Endpoint Security for Linux** Threat Prevention installed, which protects the SVM and **Trellix Agent**, to communicate with the **Trellix ePO - On-prem**.
- The OVF is a secure image, so it doesn't require any more hardening.
- The hardware and software specifications of the SVM OVF are:

CPU	4 vCPU, 1.6 GHz or higher
Memory	4-GB RAM or higher
Hard disk space for SVM deployment	32 GB or higher
Operating system	Linux, Ubuntu 18.04 (64-bit)
Software (pre-installed)	**Trellix Agent** **Endpoint Security for Linux** Threat Prevention **Trellix MOVE Agentless**

Note

The supported hypervisor is of VMware only.

Supported operating systems

Make sure that the guest virtual machine has a supported version of windows installed. The following windows operating systems are supported for the NSX Guest Introspection:

Windows supported operating system (Agentless)
Windows 10
Windows Server 2016
Windows Server 2019
Windows 2012 R2

Make sure that the guest virtual machine has a following supported version of Linux installed:

Linux supported operating system (Agentless)
Centos 7.5 - 7.6
RHEL 8.0 - 8.3
Ubuntu 18.04

Supported VMware management platform and software

You must install a supported version of VMware software.

Trellix ePO - On-prem	VMware NSX-T Manager	VMware vSphere
5.10.0 Update 11 or later	3.2, 3.2.0.1, 3.2.1	7.0 or later

For a complete list of supported **Trellix MOVE AntiVirus** environment, see **Trellix** KB article 74865 and for vSphere Connector Extension see **Trellix** KB article 96090.

For information about the Guest VM operating systems that are supported for NSX-T Data Center Manager, see *VMware NSX-T Data Center* Installation Guide.

Note

One **Trellix ePO - On-prem** supports only one NSX-T Datacenter. We support multiple vCenter through this managed NSX-T Datacenter.

Permissions required for SVM deployment

The VMware vCenter account credentials specified in the **Registered Cloud Account** page of **Trellix ePO - On-prem** for discovering the virtual instances must have these permissions.

Preparing the ESX host

This is the first step in deploying the SVM. In this phase, a kernel driver is loaded onto the ESX host, and a separate vSwitch is configured to facilitate internal connectivity for the SVM.

Configuration location	Permission description
Host → Configuration → Change Settings	Permissions required to query modules on ESX.

Configuration location	Permission description
Host → Configuration → Network Configuration	Permissions required to add details such as new virtual switch, port group, virtual NIC.
Host → Configuration → Advanced Settings	Permissions required to set up networking for filter communication on ESX.
Host → Configuration → Query Patch	Permissions required to install Filter Driver.
Host → Configuration → Security profile and firewall	Permissions to reconfigure outgoing firewall connections to allow retrieval of Filter Driver package from DSM.
Global → Licenses	To check which licenses are installed, so that you can add or remove licenses.
Sessions → Validate session	To verify the session validity.

Note

Make the MTU byte to 1600 and add 2 minimum NIC adapters.

Deploying the Virtual Appliance

This is the second step in SVM deployment, during which the virtual appliance itself is deployed from an OVF file.

Configuration location	Permission description
vApp → Import	Permissions to deploy SVM from OVF file.
Datastore → Allocate Space	Permissions required to allocate space for SVM on datastore.
Network → Assign Network	Permissions to assign SVM to networks.
Virtual Machine → Change Configuration → Add new disk	Permissions to add disks to SVM.

Configuration location	Permission description
Virtual Machine → Interaction → Power On	Permissions to turn on SVM.
Virtual Machine → Interaction → Power Off	Permissions to turn off SVM.
Virtual Machine → Change Configuration → Rename	Permissions to rename a virtual machine or change the associated notes of a virtual machine.

Activating the Virtual Machine

In this step, the SVM is activated.

Configuration location	Permission description
Virtual Machine → Change Configuration → Advanced	Permissions to reconfigure virtual machine for dvfilter

Enabling vShield Driver

This step involves enabling vShield driver on endpoints.

Configuration location	Permission description
Virtual Machine → Interaction → Install VMware Tools	To mount and unmount the VMware Tools CD installer as a CD for the guest operating system.
Virtual Machine → Guest Operations → Guest Operation Program Execution	For execution of virtual machine operation programs.
Virtual Machine → Guest Operations → Guest Operation Modifications	For changes of virtual machine operation.

Remove Operations

In this step, the SVM is removed.

Configuration location	Permission description
Virtual Machine → Edit Inventory → Remove	To delete a virtual machine and to remove its underlying files from disk. **Note:** To have permission to perform this operation, you must have this privilege assigned to both the object and its parent object.

Adding vCenter in NSX-T Compute Manager

This step involves adding vCenter as compute manager in NSX-T

Configuration location	Permission description
Extensions → Register extension	To register the extension
Extensions → Unregister extension	To unregister the extension
Extensions → Update extension	To update the extension

Setting up ESX Agent

This step involves setting up ESX Agent.

Configuration location	Permission description
ESX Agent Manager → Config	To configure the ESX Agent Manager
ESX Agent Manager → Modify	To modify the ESX Agent Manager
ESX Agent Manager → View	To view the ESX Agent Manager

Ports for Agentless deployment

Following are the ports that are open and not reserved for other purposes:

System connections	Default ports
ePO to vCenter communication	TCP 443
NSX-T to ePO communication	TCP 8443
ePO to NSX-T communication	TCP 443
SVM(MA) to ePO communication	TCP 80 and 8443
ePO to SVM (MA) communication	TCP 8081
SVM to MOVE Quarantine Share	TCP 445
GTI lookup - DNS	TCP 53

Note

If required, you can customize the default ports.

Pre-installation tasks

Register vCenter with NSX-T Data Center Manager Console

NSX-T Data Center Manager has a virtual appliance console. The vCenter registration and operational processes are carried out on this console from MOVE 4.10.x.

Before you begin

Make sure that:

- You have a vCenter user account with administrative access to synchronize NSX-T Manager with the vCenter.
- If your vCenter password has non-ASCII characters, change it before synchronizing the NSX-T Manager with the vCenter.

Task

1. **Log on to the NSX-T manager console using the IP address, for example: https://<NSXT-Manager-IP>**
2. **In the NSX-T Data Center Manager homepage, click System.**
3. **On the left pane, click Fabric → Compute Managers.**
4. **Click +Add Compute Managers and add Name, FQDN or IP address, Username, and Password. Use the default option for other fields.**

Note

If you are opting FQDN option, provide same domain name in **FQDN or IP address** in the **New Compute Manager** dialog box and in **Server Address** in the Registered Cloud Accounts page in the **Trellix ePO - On-prem**. The domain names are case-sensitive.

5. **After filling in all the details, click Add to complete the Compute Manager setup.**
6. **Verify that the vCenter Registration Status is Registered, and its Connection is UP.**

Configure a Transport Zone with NSX-T Manager console

A transport zone is a container that defines the potential reach of transport nodes. Transport nodes are hypervisor hosts and NSX Edges. The Transport Zone creation on the NSX-T Manager Console is given below for MOVE Agentless integration with NSX-T.

Task

1. **Log on to the NSX-T manager console using the IP address, for example: https://<NSXT-Manager-IP>**
2. **Navigate to System → Fabric → Transport Zones.**
3. **Click +Add Zone to create a transport zone.**
4. **In New Transport Zone, enter a name for the transport zone and optionally a description.**
5. **Select the traffic type as Overlay or VLAN.**
6. **After you add the transport zone, go to the Transport Zones page, and view the newly added transport zone.**

Configure a Service Profile with NSX-T Manager

A service profile is an instance of a partner vendor template. Administrators can customize attributes of a vendor template to create and configure an instance of the template.

Task

1. **Log on to the NSX-T manager console using the IP address, for example: https://<NSXT-Manager-IP>**
2. **In the NSX-T Data Center Manager homepage, click System.**
3. **On the left pane, click Fabric → Profiles.**
4. **Click Transport Node Profiles and then click +Add Profile.**
5. **In Add Transport Node Profile, enter a name to identify the transport node profile. You can optionally add the description about the transport node profile.**
6. **In the + Add Switch section, add details of the new switch.**
7. **Before you continue, decide which type of host switch you want to configure on nodes of a cluster.**
8. **In the New Node Switch section, if you select N-VDS as the host switch type, continue to enter details for the fields like described in this picture:**

Options	Values
Mode	Select **Standard**.

Options	Values
Name	Enter the name.
Transport Zone	Select the transport zone that you have created.
NIOC Profile	Select **nsx-default-nloc-hostswitch-profile**.
Uplink Profile	Select **nsx-default-nloc-uplink-hostswitch-profile**.
LLDP Profile	Select **LLDP [Send Packet Disabled**.
IP Assignment (TEP)	Select **Use DHCP**.
uplink-1	Enter physical NIC information like `vmnic1`.
uplink-2	Enter physical NIC information like `vmnic2`.

Note

For IP Assignment, you can also select **Use Static** but configure your IP address pool under **Networking** → **IP Address Pools**.

9. **In the Teaming Policy Uplink Mapping section, under Physical NICs, enter the ESXi physical NIC configuration as per your environment for uplink-1 and uplink-2.**
10. **Click Add to complete the configuration.**

Configure a NSX-T Data Center Manager Console

The NSX-T Data Center Manager virtual appliance console allows you to configure a vCenter with the existing Nodes, vCenters and Profiles.

Task

1. **Log on to the NSX-T manager console using the IP address, for example: https://<NSXT-Manager-IP>**
2. **Prepare the host in NSX-T Data Center Manager, click Fabric → Nodes, and in the main pane, click Host Transport Nodes.**
3. **From the Managed by drop-down list, select the vCenter that is added previously.**
4. **Select a cluster that contains the VMs that you want to protect.**
5. **Click CONFIGURE NSX and select Transport Node Profile from the drop-down list.**

   Now wait until NSX-T Data Center configuration becomes Success.

Download and check in software extensions and packages

Download and check in software extensions

You can download these extensions and packages either from:

- The **Trellix ePO - On-prem** server, Software Catalog. For more information see, *Check in the software extensions and download packages from Software Catalog in the **Trellix ePO - On-prem***.
- The **Trellix** download site. Check in the extensions to **Trellix ePO - On-prem**.

Note

Make sure to download the required extensions and packages from the **Trellix** download site.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Check in the extension and packages individually:**
   a. **Select Menu → Software → Extensions → Install Extension.**
   The Install Extension page opens.
   b. **Browse and select the extension files in the same order as mentioned below, and then click Open → OK:**

Extension description	Extension name
Trellix MOVE AntiVirus Agentless extension	i. MDCC_5.3.x.xx.zip ii. VSPHEREDCEXTN_5.4.x.xx.zip iii. DC__GS__4000_4.10.x.xx.zip iv. DC__AM__4000_4.10.x.xx.zip v. MOVEAVLIC400_4.10.x.xx.zip
Agentless SVM OVF package. For more information see, *Check in the **Trellix MOVE AntiVirus** SVM package to **Trellix ePO - On-prem***.	MOVE-AV-AL_SVM_OVF_4.10.X.zip

   c. **Review the extension details and click OK.**
   d. **To check in the packages, select Menu → Software → Main Repository → Check In Package.**
   e. **For File path, browse and select the individual packages as mentioned below, and then click OK:**

Package description	Package name
Trellix MOVE AntiVirus Agentless package	MOVE‑AV‑AL_SVM_OVF_4.10.X.XX.zip

Note

> **MOVE AL 4.10.x** extension supports version 4.10.x or above and incompatible with version 4.9.x or lower policies.

Check in the software extensions and download packages from Software Catalog in the Trellix ePO - On-prem

If you have Software Catalog, you can check in the software extensions from there.

Before you begin

Make sure to download the required packages from the software catalog.

Note

> In the **Trellix ePO - On-prem** version 5.10.0 and above, the term Software Manager is identified as Software Catalog.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Software, then click Software Catalog.**
3. **In the Product Categories pane, enter Move in the search bar.**
4. **Select the version of the Trellix MOVE AntiVirus 4.x and click Check In.**

Install Trellix MOVE AntiVirus (Agentless) for the first time

Register a VMware vCenter account with Trellix ePO - On-prem (Agentless)

To use **Trellix MOVE AntiVirus** to manage the security of the virtual machines in your data center, you must first add your VMware vCenter to the **Trellix ePO - On-prem** server.

Before you begin

Make sure that:

- You have configured your VMware vCenter server that manages the ESXi servers, which host the guest VMs.
- You have registered the VMware vCenter Server with VMware NSX-T Manager. In case of multiple VMware vCenter environment each of your vCenter Servers are registered with a single VMware NSX-T Manager.
- You have installed the **Trellix MOVE AntiVirus** software extension on the **Trellix ePO - On-prem** server.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Configuration → Registered Cloud Accounts.**
3. **From the bottom-left click Actions → Add Cloud Account to open the Add Cloud Account dialog box.**
4. **From the Choose Cloud Provider drop-down list, select VMware vSphere and click OK.**
5. **On the vCenter Account Details page, configure these options.**

Note

You must have a vCenter Server user account with administrator rights to use the autoscale feature.

Option	Description
Account Name	A name for the VMware vCenter account in **Trellix ePO - On-prem**. Account names can include characters a–z, A–Z, 0–9, and [_.-], without space.
Server Address	(Required) IP address or the host name of the available VMware vCenter.
vCenter Username	(Required) User name of the available VMware vCenter account.
vCenter Password	(Required) Password of the available VMware vCenter account.
Sync Interval (In Minutes)	Specify the interval for running the next vCenter discovery (default value is 5 minutes).
Port	The port number required to establish the connection with the available VMware vCenter (default port is 443).
Tag	The administrator specifies this to identify the VMs. Tag name can include characters a–z, A–Z, 0–9, and [_.-], with space.

6. **Click Test Connection to validate VMware vCenter account details and verify the connection to the VMware vCenter, then click Next → Finish.**
7. **When prompted to confirm, click OK to register the vCenter account and wait for vCenter sync to complete.**
   This action registers the VMware vCenter and imports all discovered virtual machines, which are unmanaged, into the System Tree. The instances are imported with the same organization as the VMware vCenter.

Note

The virtual machines that are already added and managed by **Trellix ePO - On-prem** are retained with the existing policy settings, but the virtualization properties for these systems are added.

Set up a general configuration for deployment (Agentless)

Before deploying **Trellix MOVE AntiVirus** SVM, configure settings on the **Trellix ePO - On-prem** server, so that they are retrieved and used for every **Trellix MOVE AntiVirus** SVM deployment.

Before you begin

Make sure that you have registered a VMware vCenter account with the **Trellix ePO - On-prem**.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Automation → MOVE AntiVirus Deployment.**
3. **In the Configuration tab, click General under General list.**

   The General Configuration page opens.
4. **Enter and confirm the password for Trellix ePO - On-prem Credentials section.**

   Trellix ePO - On-prem credentials

Options	Description
Password	Type the password of the **Trellix ePO - On-prem** console that the administrator has currently logged on
Confirm Password	Confirm the password

5. **Enter and confirm password for SVM (Agentless) and SVM Manager (Multi-Platform) Configuration section.**

   Note

   The **SVM (Agentless) and SVM Manager (Multi-Platform) Configuration** section shows a default password.

   Caution

   The password you enter is set to the SVM and you can't update it once the SVM is deployed. This password is not applicable to the SVM, which is already deployed.

   If required, change the password.

   SVM (Agentless) and SVM Manager (Multi-platform) Configuration

Option	Description
Hostname Prefix (Agentless only)	Type a unique prefix that is added to the host name of the **Trellix MOVE AntiVirus** SVM. The

Option	Description
	prefix can include characters a–z, A–Z, 0–9, and [-], without space
Password	Type a password to be used as the **Trellix MOVE AntiVirus** SVM password during deployment. • The password must be at least 6 characters • The password must contain at least one uppercase letter (A-Z) and one numeral (0–9)
Confirm Password	Confirm the password

6. **Click Save to store these configurations, so that you can use them for every Trellix MOVE AntiVirus SVM deployment.**

Validate your NSX-T Data Center Manager using Trellix ePO - On-prem

The vSphere Connector extension automatically detects once vCenter sync is successful in RCA page and then it shows the details of your NSX-T Manager accounts in the **Trellix ePO - On-prem**. You must now register these NSX-T Manager servers with **Trellix ePO - On-prem**.

Before you begin

Make sure that you have set up a common configuration for **Trellix ePO - On-prem** and SVA.

Using this configuration available on the **Trellix ePO - On-prem**, you can edit the details and validate the credentials of your NSX-T Manager.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Automation → MOVE AntiVirus Deployment.**
3. **In the Configuration tab, click NSX Manager under Agentless.**
   The **NSX Manager: Registration** page displays these options:

Option	Description
vCenter Account	Displays the name of the registered vCenter account
NSX-T Manager Name	Displays the name of your NSX-T Manager

Option	Description
Configuration Status	Specifies whether the NSX-T Manager is configured
Action	**Edit** — Click to edit and validate the credentials and other details of the NSX-T Manager accounts, which are automatically detected and sent to **Trellix ePO - On-prem**

4. **Click Edit under Action to open the Edit NSX Manager Details dialog box and edit these NSX-T Manager account options.**

Note

Make sure that your NSX-T Manager account and its details are ready.

Option	Description
vCenter Account	Specifies the name of the registered vCenter account **Note:** This option is predefined.
NSX Manager Name	Specifies the name of the available NSX-T Manager **Note:** Do not include spaces.
NSX Manager Address	Specifies the IP address or the host name of the available NSX Manager **Note:** This option is predefined.
NSX Manager Port	Specifies the port number of NSX-T Manager

Option	Description
NSX Manager Username	Specifies the user name of the available NSX-T Manager
NSX Manager Password	Specifies the password of the available NSX-T Manager

5. **Click Validate Credentials to verify the credentials of the NSX-T Manager and verify that the connection to the NSX-T Manager works.**
6. **Click Save to store the NSX-T Manager account details.**

What to do next

Note

MOVE AntiVirus can only register with a single VMware NSX-T manager. In a multiple VMware vCenter environment, each VMware vCenter must be configured to share the same NSX-T manager.

Check in the Trellix MOVE AntiVirus SVM package to Trellix ePO - On-prem

Check in the **Trellix MOVE AntiVirus** SVM package to **Trellix ePO - On-prem**, so that it is available with VMware NSX Manager to deploy it to the cluster. You can view and delete the **Trellix MOVE AntiVirus** SVM package using **Trellix ePO - On-prem**.

Before you begin

Make sure that you have installed the **Trellix MOVE AntiVirus** extension on the **Trellix ePO - On-prem** server.

Important

For a successful check-in, do not change the file name of the **Trellix MOVE AntiVirus** SVM package.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Automation → MOVE AntiVirus Deployment.**
3. **On the Configuration tab under Agentless, click SVM Repository to open the SVM OVF Details page with these Trellix MOVE AntiVirus SVM OVF options:**

Options	Description
SVM OVF Name	Name of the **Trellix MOVE AntiVirus** SVM package checked in to **Trellix ePO - On-prem**.

Options	Description
SVM OVF Version	Version of the **Trellix MOVE AntiVirus** SVM package checked in to **Trellix ePO - On-prem**.
SVM OVF Use Count	Specifies the number of hypervisors that are using this **Trellix MOVE AntiVirus** SVM.
Action	• **Delete** — To remove an existing **Trellix MOVE AntiVirus** SVM when it is not registered with any NSX Manager.

4. **Click Actions → Add SVM to open the Check-in SVM OVF (zip) file page.**
5. **Click Choose File to select the Trellix MOVE AntiVirus SVM package, then click Open → OK.**

   Note

   You can check in up to three versions of **Trellix MOVE AntiVirus** SVM starting from 4.x.x.

   The package to **Trellix ePO - On-prem** is checked in.
6. **(Optional) On the Configuration tab under Agentless, click Server Settings to enable NSX Unprotected Tag.**

Register the Trellix MOVE AntiVirus service with NSX-T Manager using Trellix ePO - On-prem

After registering your vCenter account details on NSX-T Manager and **Trellix ePO - On-prem**, use **Trellix ePO - On-prem** to enable the registration of **Trellix MOVE AntiVirus** (Agentless) as a service in NSX-T Manager.

The details of the registered vCenter, SVM OVF Version, and NSX-T Manager are automatically retrieved and displayed on the **Trellix ePO - On-prem** server. But you must register the **Trellix MOVE AntiVirus** service with the vCenter account. This registration permits the deployment of the service to the ESXi servers.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Automation → MOVE AntiVirus Deployment.**
3. **On the Service tab, click NSX Manager to open the MOVE Service Registration page with these options.**

Option	Description
NSX Manager Name	Displays the name of the registered NSX-T Manager.

Option	Description
NSX Manager Address	Displays the IP address of your NSX-T Manager.
vCenter Account	Displays the name of the vCenter account that is registered with NSX-T Manager and **Trellix ePO - On-prem**.
Registered SVM Version	Displays the version of the **Trellix MOVE AntiVirus** SVM package checked in to **Trellix ePO - On-prem**.
Service Registration Status	Displays registration status values **Registered**, **Not Registered**, and **Registration Failed**.
Actions	• **Register** — Click to select the latest **Trellix MOVE AntiVirus** SVM and register it to the vCenter that is added to your NSX-T Manager. • **Unregister** — Click to unregister the **Trellix MOVE AntiVirus** service and to remove it from the vCenter. • **Upgrade** — Click to upgrade the **Trellix MOVE AntiVirus** service. ⚠ **Caution:** Make sure that you checked in the latest **Trellix MOVE AntiVirus** SVM required for the upgrade. Otherwise, the existing **Trellix MOVE AntiVirus** service is deployed to the ESXi servers.

4. **Click Register under Actions to open the MOVE Service Registration dialog box.**
5. **Select the latest Trellix MOVE AntiVirus SVM and click OK.**

   The **Trellix MOVE AntiVirus** service is now registered with the vCenter account that is registered with your NSX-T Manager.
6. **On the NSX-T Data Center console, verify that the Trellix MOVE AntiVirus service is now available under System → Service Deployments → Catalog.**

Deploy the Trellix MOVE AntiVirus SVM

To provide **Trellix MOVE AntiVirus** (Agentless) protection to the virtual machines on your ESXi servers, you must install the **Trellix MOVE AntiVirus** service (**Trellix MOVE AntiVirus** SVM) on your ESXi servers.

Before you begin

Make sure that:

- The host, where you are deploying the SVM using NSX-T Manager, is part of a cluster
- The datacenter is using a vSphere distributed switch
- The Guest Introspection service is installed on all ESXi servers
- The virtual machines have the latest VMware Tools installed and have the Guest Introspection Thin Agent enabled for both Windows and Linux VMs.
- You have appropriate permission to perform the SVM deployment using **Trellix ePO - On-prem**. You can enable this permission by navigating through **Menu** → **Users** → **Permission Sets** → **MOVE AV [Agentless] SVM Deployment** → **Edit**.

Deploy the **Trellix MOVE AntiVirus** services on a set of clusters. Manage service deployments here by adding new services or deleting existing ones.

This deployment automatically provides virus protection for virtual machines on a new hypervisor from the moment the hypervisor is added to the clusters. When a new cluster is added, deploy the **Trellix MOVE AntiVirus** SVM again.

Task

1. **Log on to the NSX-T Data Center manager as an administrator.**
2. **In the NSX-T Data Center manager console, navigate to System and then in the left pane, click Service Deployment.**
3. **Select Partner service from the drop-down list and then click Deploy Service.**
4. **To configure the service deployment:**
   a. **Enter the name under Service Deployment Name.**
   b. **Select your desired Compute Manager, Cluster, and Data Store.**
   c. **Click Edit Details.**
      A Networks dialog box appears on your screen.
   d. **Choose your Management NIC and their Network, Network Type as per your environment and click Save.**
5. **In the NSX-T Data Center manager, select System → Service Deployment, click Save. The service deployment starts and after successful Service deployment SVA is installed vCenter.**

Results

Service Status	ID	Description
UNKNOWN	3	Specifies that the **Trellix MOVE AntiVirus** service status is unknown
UP	N/A	Not applicable
DOWN	1	Specifies that the **Trellix MOVE AntiVirus** service is stopped

The **Trellix MOVE AntiVirus** service is now deployed to the cluster when the **Installation Status** is **Successful** and the **Service Status** is **UP**.

On-access scan policy export to NSX-T

After you register the **Trellix MOVE AntiVirus** service on the **Trellix ePO - On-prem** server, the **On Access Scan** policies for **Trellix MOVE AntiVirus** are exported from **Trellix ePO - On-prem** to NSX-T in real time.

The exported policies are available in NSX-T console under **Security** → **Endpoint Protection Rules** → **Service Profiles** with a Service Profile Name, Service Profile Description, Vendor Template, Vendor Template Key, Tags and Status.

ⓘ **Important**

Only the **On Access Scan** policies are exported from **Trellix ePO - On-prem** to NSX-T Manager. If you need to assign the **On Demand Scan** policies, assign them manually on **Trellix ePO - On-prem**.

When you create a new or duplicate **On Access Scan** policy in **Trellix ePO - On-prem**, it is immediately exported to **Service Profiles** in NSX-T Manager. This real-time policy export helps the VMware NSX-T administrator understand the different sets of policies created and changed by the administrator.

Note

Once an **On Access Scan** policy is exported to NSX-T Manager, changes to an **On Access Scan** policy names in **Trellix ePO - On-prem** will not update in NSX-T Manager. You must manually update the name changes in the NSX-T Manager.

If you want to delete an **On Access Scan** policy from **Trellix ePO - On-prem**, the best practice is to delete the same policy from the NSX-T Manager.

Tip

Best practice: Verify the security policy in NSX-T before deleting any **On Access Scan** policy from **Trellix ePO - On-prem**.

You can't delete the exported **On Access Scan** policy in NSX-T Manager when it is included in any NSX-T security policy. You must remove all configurations referring to this policy before deleting it.

Configure the security group and security policy in NSX-T Manager

You must create the security policy and apply it to the security group of VMs that you want to protect.

The security policies for **Trellix MOVE AntiVirus** are automatically exported from **Trellix ePO - On-prem** after you register the **Trellix MOVE AntiVirus** service on **Trellix ePO - On-prem**. This configuration is a one-time initial activity for a vCenter. But you must repeat this configuration when a new datacenter is added.

Create an NSX-T service profile

Create an NSX-T service profile with **Trellix MOVE AntiVirus** (Agentless).

Before you begin

Make sure that:

- The **Trellix MOVE AntiVirus** service is registered with **Trellix ePO - On-prem**.
- You deploy the **Trellix MOVE AntiVirus** SVM.

Task

1. **Log on to the NSX-T manager console as an administrator.**
2. **Select Security → Endpoint Protection → Endpoint Protection Rules, then click the Security Profiles tab.**
3. **In the Service Profiles page, click Add Service Profile.**
4. **Complete the details of the service profile:**
    a. **In the Service Profile Name, enter the name of the service profile.**
    b. **In the Service Profile Description, enter a description for the profile (optional).**
    c. **In the Vendor Template, select the policy configured in the Trellix ePO - On-prem.**
5. **Click Save. The status of the Service Profile changes to Success on successful configuration.**

Results

You have created your NSX-T service profile for the **Trellix MOVE AntiVirus** (Agentless).

Create an NSX-T security policy and rule

Create an NSX-T security policy with **Trellix MOVE AntiVirus** (Agentless) enabled as a Guest Introspection Service.

Before you begin

Make sure that:

- The **Trellix MOVE AntiVirus** service is registered with **Trellix ePO - On-prem**.
- You deploy the **Trellix MOVE AntiVirus** SVM.

Task

1. **Log on to the NSX-T manager console as an administrator.**
2. **Select Security → Endpoint Protection → Endpoint Protection Rules, then click the Rules tab.**
3. **In the Rules page, click +Add Policy.**

   The policy gets listed in the list of available policies.
4. **In the list of policies, click the desired policy and click +Add Rule.**
5. **In the new rule, rename the rule name and click the Edit icon under the Groups column.**

   The **Set Groups** dialog box appears on the screen.
6. **Select a group in the list and click Apply.**

   The selected group appears in the list.
7. **Click the Edit icon under the Service Profiles column.**

   The **Set Service Profile** dialog box appears on the screen.

8. **Select a service profile in the list and click Save.**

   The selected service profile appears in the list.
9. **Click Publish to change the status from Uninitialized to Success.**

Results

You have created your NSX-T security policy for deploying **Trellix MOVE AntiVirus** (Agentless).

Create an NSX-T Security Group

Select the required Clusters or Virtual Machines from the available vCenter and configure them as a security group. This configuration allows you to assign the security policy to the group and protect its VMs.

Before you begin

Make sure that:

- VMware vSphere is installed and added to the cluster.
- The **Trellix MOVE AntiVirus** service is registered with NSX-T Data Center Manager using **Trellix ePO - On-prem**.
- You deploy the **Trellix MOVE AntiVirus** SVM

Task

1. **Log on to the NSX-T manager console as an administrator.**
2. **Select Security → Endpoint Protection → Endpoint Protection Rules, then click the Rules tab.**
3. **In the list of policies, click the desired policy and click +Add Rule.**
4. **In the new rule, rename the rule name and click the Edit icon under the Groups column.**

   The **Set Groups** dialog box appears on the screen.
5. **In the Set Groups dialog box, click +Add Group.**
6. **Enter the name in the Group Name field.**
7. **Click Set Members under the Compute Members column.**

   The **Select Members** dialog box appears on the screen.
8. **Under Membership Criteria, click +Add Criteria to add multiple criteria. Maximum number of allowed criteria are five.**
9. **In the Criteria row, select the desired values from the dropdown lists and enter the field values, then click Apply.**
10. **Click Save and click View Members to check the effective list of virtual machines in the group.**

Results

Your security group is added and contains the virtual machines to be protected from the selected cluster.

Verify the SVM deployment on Trellix ePO - On-prem

To verify the Managed State of the deployed SVM.

Before you begin

Make sure that:

- The **Trellix MOVE AntiVirus** service is registered with **Trellix ePO - On-prem**.
- You deploy the **Trellix MOVE AntiVirus** SVM.
- The **Installation Status** appear as **Succeeded** and **Service Status** as **Up** in NSX-T console.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → System Tree → Systems.**
3. **Under Managed State column, verify the SVM state as Managed.**

Note

The SVM name is in the format of **<NSX Manager Name>-<Hostname prefix>-host-xx** .

Configuring Policies and Settings in Multiple vCenter environment

Create Policies and Settings on Trellix ePO - On-prem

If you want to support multi vCenter environment with **Trellix MOVE AntiVirus** (Agentless), then you need to create individual policy and settings to each multi vCenter environment. The policy catalog on the **Trellix ePO - On-prem** of the **Trellix MOVE AntiVirus** contains the policies and settings required for each vCenter.

Create a On Access Scan policy

After you register the **Trellix MOVE AntiVirus** on the **Trellix ePO - On-prem** server, you need to create a **On Access Scan** policy each for every vCenter that you want to protect with **Trellix MOVE AntiVirus**.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Policy → Policy Catalog.**
3. **Select MOVE AntiVirus 4.x.x from the Product drop-down list, then click New Policy.**

   The **Create a new policy** dialog box appears on the screen.
4. **In the Create a new policy, select On Access Scan from the Category drop-down list.**
5. **Select My Default from the Create a policy based on this existing policy drop-down list.**
6. **Enter the name of your policy in Policy Name.**
7. **Click OK to save the policy.**

Results

The new **On Access Scan** policy page appears on the screen with all parameters and their values.

What to do next

According to your requirements, edit the values of the parameters and click **Save** otherwise click **Cancel**.

Create an On Demand Scan policy

After you register the **Trellix MOVE AntiVirus** on the **Trellix ePO - On-prem** server, you need to create a **On Demand Scan** policy each for every vCenter that you want to protect with **Trellix MOVE AntiVirus**.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Policy → Policy Catalog.**
3. **Select MOVE AntiVirus 4.x.x from the Product drop-down list, then click New Policy.**

   The **Create a new policy** dialog box appears on the screen.
4. **In the Create a new policy, select On Demand Scan from the Category dropdown list.**
5. **Select My Default from the Create a policy based on this existing policy dropdown list.**
6. **Enter the name of your policy in Policy Name.**
7. **Click OK to save the policy.**

Results

The new **On Demand Scan** policy page appears on the screen with all the parameters and their values.

What to do next

As per your requirements, edit the values of the parameters and click **Save** otherwise click **Cancel**.

Create a SVM Settings policy

After you register the **Trellix MOVE AntiVirus** on the **Trellix ePO - On-prem** server, you need to create a **SVM Settings** policy each for every vCenter that you want to protect with **Trellix MOVE AntiVirus**.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Policy → Policy Catalog.**
3. **Select MOVE AntiVirus 4.x.x from the Product drop-down list, then click New Policy.**

   The **Create a new policy** dialog box appears on the screen.
4. **In the Create a new policy, select SVM Settings from the Category drop-down list.**
5. **Select My Default from the Create a policy based on this existing policy drop-down list.**
6. **Enter the name of your policy in Policy Name.**
7. **Click OK to save the policy.**

   The new **On Access Scan** policy page appears on the screen with all the parameters and their values.
8. **Under SVM Configuration → Agentless on the policy settings page, configure these settings as needed, then click Save.**

   - **Hypervisor/vCenter Server** — Enter the valid IP address of either the hypervisor that the SVM resides on or the vCenter server (vCenter details are recommended to provide here).
   - **Protocol** — Select **https** or **http**, depending on the protocol the server uses to receive client requests.
   - **vCenter/ESXi Port** — Specify the port number of the SVM. The default port is 443.
   - **Username** — Enter the user name credentials to connect with the server.

Note

> The user account requires at least read access to the vCenter server or the ESXi host. Domain-based credentials are supported only when the vCenter server or the ESXi host has been configured to support domain-based authentication.

- **Password** — Enter the password associated with the user.

Note

> After you save and reopen the **SVM Settings** policy, the vCenter **Password** field appears blank. Though it appears blank, the password is encrypted and saved in the policy settings. Confirm the password to test connection settings.

- **Confirm password** — confirm the password.
- **SVM Time Zone** — Select your local time zone from the drop-down list.
- **NTP Servers(s)** — Select **Use Default** servers or **Use following Servers**. If **Use following Servers** is selected, enter the NTP server details.

9. **Click Test connection settings to test the connection to the hypervisor/vCenter Server and then click Save to save the new settings to your SVM Settings policy.**

Create a Options policy

After you register the **Trellix MOVE AntiVirus** on the **Trellix ePO - On-prem** server, you need to create a **Options** policy each for every vCenter that you want to protect with **Trellix MOVE AntiVirus**.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Policy → Policy Catalog.**
3. **Select MOVE AntiVirus 4.x.x from the Product drop-down list, then click New Policy.**
   The **Create a new policy** dialog box appears on the screen.
4. **In the Create a new policy, select Options from the Category dropdown list.**
5. **Select My Default from the Create a policy based on this existing policy dropdown list.**
6. **Enter the name of your policy in Policy Name.**
7. **Click OK to save the policy.**
   The new **Options** policy page appears on the screen with all the parameters and their values.
8. **On the policy settings page, click Show Advanced to see all the settings.**
9. **Under Quarantine Manager → Agentless only on the policy settings page:**
   a. Enter the network share under **Quarantine network share**.
   b. Enter the network domain and username under **Network domain and username**.
   c. Enter the network domain password under **Network Password** and **Confirm Password**.
10. **Click Save to save the new settings to your Options policy.**

Create a SVM Manager settings policy

After you deploy the **Trellix MOVE for Multi-Platform** AntiVirus to the clients from the **Trellix ePO - On-prem** server, you need to create a policy for SVM Manager settings policy. Using this policy, you can configure the ODS scheduler, Scanning options and other options.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Policy → PolicyCatalog.**
3. **Select MOVE AntiVirus 4.10.x from the Product drop-down list, then click New Policy.**
   The **Create a new policy** dialog box appears on the screen.
4. **In Create a new policy, select SVM Manager Settings from the Category drop-down list.**
5. **Select My Default from the Create a policy based on this existing policy drop-down list**
6. **Enter the name of your policy in Policy Name.**
7. **Click OK to save the policy**

   The new **SVM Manager Settings** policy page appears on the screen with all the parameters and their values.

   As per your requirements, edit the values of the parameters and click **Save** otherwise click **Cancel.**

Create a Shared Cloud Solutions policy

After you deploy the **Trellix MOVE for Multi-Platform** AntiVirus to the clients from the **Trellix ePO - On-prem** server, you can create a Shared Cloud Solutions policy. Using this policy, you can configure **Threat Intelligence Exchange** and **Intelligent Sandbox** settings.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Policy → PolicyCatalog.**
3. **Select MOVE AntiVirus 4.10.x from the Product drop-down list, then click New Policy.**
   The **Create a new policy** dialog box appears on the screen.
4. **In Create a new policy, select Shared Cloud Solutions from the Category drop-down list.**
5. **Select My Default from the Create a policy based on this existing policy drop-down list**
6. **Enter the name of your policy in Policy Name.**
7. **Click OK to save the policy**

   The new **Shared Cloud Solutions** policy page appears on the screen with all the parameters and their values.

   As per your requirements, edit the values of the parameters and click **Save** otherwise click **Cancel.**

Group SVM and client systems under vSphere

The **Trellix MOVE AntiVirus** service deployment to the client systems and their status are visible in their respective vCenter. In multiple vCenters scenarios, after deploying the virtual machines with **Trellix MOVE AntiVirus** Agentless, each client system and SVM is shown under their respective vCenter.

The vCenter dashboard shows the **Trellix MOVE AntiVirus** Agentless deployment and functional status. When you register all your VMware vSphere accounts under Registered Cloud Accounts, the same systems and SVMs must appear under their respective groups in the ePO under **System Tree** > **My Organization** > **vSphere**.

Lost and Found

For example, if you manage two vCenter accounts, those two accounts reflect as groups under vSphere. There are some scenarios where the systems and SVMs might not appear under their respective groups and their SVM might appear in the **Lost and Found** section.

Verify the SVA and Client System are grouped properly

The SVA and client system must present in the same group in the **Trellix ePO - On-prem** which are named after the vCenters. The sync process must be verified between VMware vSphere vCenters and **Trellix ePO - On-prem**.

Before you begin

Make sure that multiple VMware vCenter servers that manage the ESXi servers, which host the guest VMs are configured properly.

Make sure that all vCenter Servers are configured on the NSX-T Manager Console.

Make sure that the VMware vCenter account with the **Trellix ePO - On-prem** under Registered Cloud Account.

'Make sure the SVM deployment is completed successfully from the NSX-T console

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Navigate to System Tree and expand My Organization → vSphere.**

   The account groups appear with their respective client systems and SVAs.
3. **Select each account and check whether SVA and client system IP addresses match with your respective vSphere vCenter client system and SVA IP addresses.**

What to do next

If the account groups systems and SVAs are not grouped properly as expected, then delete all the client systems and SVAs from the vSphere and **Lost and Found** groups. After that make sure to delete the Group.

Delete the groups and systems

In some scenarios, the groups under **My Organization** → **vSphere** don't have the SVAs and Client systems are not organized as per vSphere vCenters. You must delete all the groups and systems that are grouped under different accounts and **Lost and Found**.

Before you begin

Make sure that multiple VMware vCenter servers that manage the ESXi servers, which host the guest VMs are configured properly.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Navigate to System Tree and expand My Organization > vSphere.**

   The account groups appear with their respective client systems and SVAs.
3. **Select each account, under Systems tab, select the checkbox to select all the systems.**
4. **Select Delete under Actions → Directory Management on the Wake Up Agents toolbar.**

   The **Delete** dialog box appears on the screen.
5. **Click Ok on the Delete dialog box.**

   All the systems are deleted under the group with a message **Deleted Systems** at the bottom right corner.
6. **Repeat the above two steps to delete all the systems under each group and Lost and Found.**
7. **Under System Tree, select each group account and click System Tree Actions → Delete Group.**

   The **Delete Group** dialog box appears on the screen.
8. **Click Ok on the Delete Group dialog box.**

   The group is deleted with a message **Group deleted successfully** at the bottom right corner.

What to do next

Make sure that all the systems and groups are deleted, even delete the systems under **Lost and Found**. Now sync your vSphere accounts on the **Registered Cloud Accounts** page.

Sync all vSphere accounts in Trellix ePO - On-prem

After cleaning up the group accounts and systems associated to each configured vSphere account, check the vSphere accounts registered under **Registered Cloud Accounts**.

Before you begin

Make sure that the VMware vCenter account with the **Trellix ePO - On-prem** under **Registered Cloud Account**.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Configuration → Registered Cloud Account**
3. **In the list of VMware vSphere accounts, under Actions, click Sync for every account.**

Results

This syncs the VMware vSphere accounts and groups these as accounts with their SVAs and Client Systems.

Assign On-access scan, On-demand scan, options, and svm settings to the Groups in System Tree

The vCenters are created as a group account with their corresponding SVAs and client systems. The assigned policies are the default policies assigned to the group and their systems for the deployed **Trellix MOVE AntiVirus** software.

Before you begin

Make sure to provide the NSX-T manager details for only one vCenter account in the **Trellix ePO - On-prem** and registered it to the NSX-T Manager. This validates your NSX-T Data Center Manager for all vCenters.

Make sure to deploy the **Trellix MOVE AntiVirus** SVM on all vCenters from NSX-T manager console.

The newly created policies specifically for the vSphere groups are applied as follows:

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Navigate to System Tree → My Organization → vSphere, select a vSphere account and, click the Assigned Polices tab.**
3. **Select MOVE AntiVirus 4.10.0 from the Product drop-down list.**

   All default policies assigned to the vCenter appear in this list.
4. **For each policy, click Edit Assignment under Actions.**

   The policy assignment page appears for the selected policy.
5. **Under Assignment page, edit the options as:**
   a. **Choose Inherit from as Break inheritance and assign the policy and settings below.**
   b. **Select your policy from the Assigned Policy drop-down list.**
   c. **Choose Lock policy inheritance as Unlocked.**
6. **Click Save and click OK in the dialog box to save your changes.**

Results

Now the client systems under each vSphere account are assigned with created policies.

What to do next

Repeat the same for assigning the created policies for **On Access Scan**, **On Demand Scan**, **SVM settings** and **Options**.

Post-installation tasks

Configure the vCenter details in SVM Settings policy in Trellix ePO - On-prem

You must specify these details under **SVM Configuration** in the **Trellix MOVE AntiVirus SVM Settings** policy in **Trellix ePO - On-prem**.

Note

If you failed to provide the vCenter details:

- The IP address for the threat events generated for client will not appear.
- The Security tags will not work.
- The **Agentless Anti-Malware Protection Status** for the clients will not appear.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Policy → Policy Catalog.**
3. **Select MOVE AntiVirus 4.x.x from the Product drop-down list, then select SVM Settings from the Category drop-down list.**
4. **Click Edit SVM Setting policy .**

5. **Under SVM Configuration, configure these settings as needed, then click Save.**
   - **Hypervisor/vCenter Server** — Enter the valid IP address of either the hypervisor that the SVM resides on or the vCenter server (vCenter details are recommended to provide here).
   - **Protocol** — Select **https** or **http**, depending on the protocol the server uses to receive client requests.
   - **vCenter/ESXi Port** — Specify the port number of the SVM. The default port is 443.
   - **Username** — Enter the user name credentials to connect with the server.

   Note

   The user account requires at least read access to the vCenter server or the ESXi host. Domain-based credentials are supported only when the vCenter server or the ESXi host has been configured to support domain-based authentication.

   - **Password** — Enter the password associated with the user.

   Note

   After you save and reopen the **SVM Settings** policy, the vCenter **Password** field appears blank. Though it appears blank, the password is encrypted and saved in the policy settings. Confirm the password to test connection settings.

   - **Confirm password** — confirm the password.
   - **SVM Time Zone** — Select your local time zone from the drop-down list.
   - **NTP Servers(s)** — Select **Use Default** servers or **Use following Servers**. If **Use following Servers** is selected, enter the NTP server details.
6. **Click Test connection settings to test the connection to the hypervisor/vCenter Server and then click Save.**

Perform wake-up agent and Antimalware test (EICAR)

Once the SVM appears as Managed in **Trellix** System Tree, perform wake up agent on the SVM and antimalware test (EICAR) on clients.

Before you begin

Make sure that:

- You deploy the **Trellix MOVE AntiVirus** SVM.
- You apply the NSX-T security policy to the NSX-T security group.
- The policy reflection of On Access policy from NSX-T to **Trellix ePO - On-prem**.
- SVM appears as Managed in **Trellix ePO - On-prem** System Tree.

Note

As the **Trellix** software is not installed in the Agentless, the client appears as unmanaged in the **Trellix ePO - On-prem** System Tree.

Task

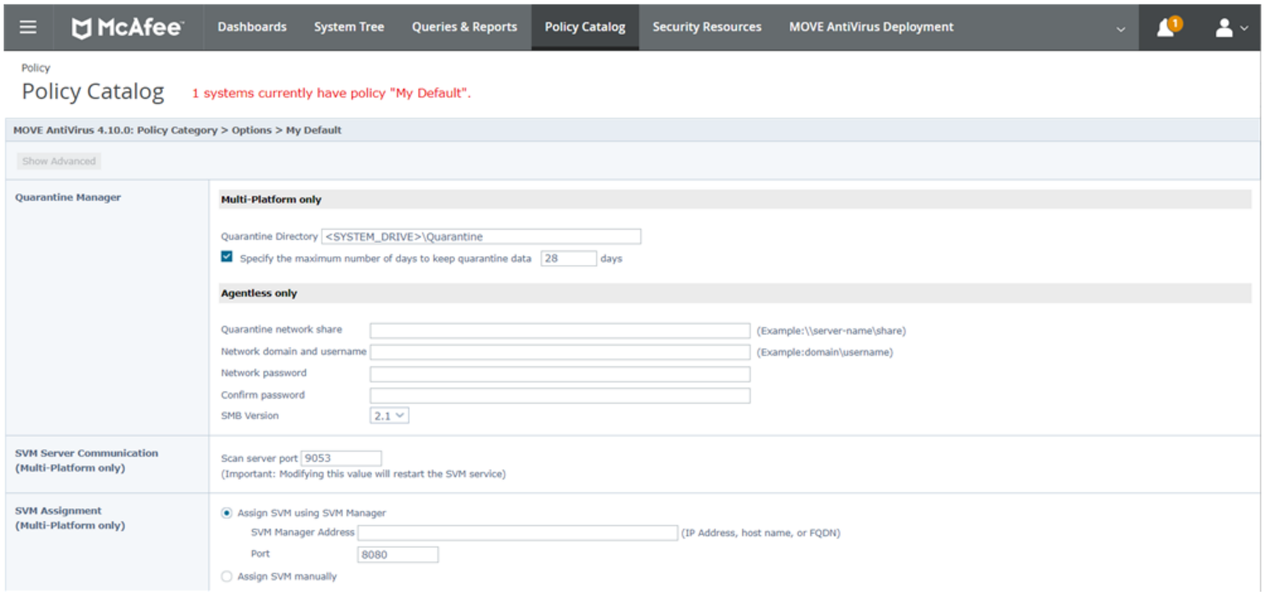
1. **Policy enforcement based on time configured at Trellix ePO - On-prem.**
   1. **In the Trellix ePO - On-prem, click Menu → Automation → MOVE AntiVirus Deployment → Configuration → Agentless → Server Settings.**

      The Server Settings page opens.
   2. **The default Policy Enforcement Interval (Minutes) is 60 minutes. This reflects that all policy changes in every 60 minutes automatically to SVM.**
   3. **Click Run for Run Policy Collection to reflect any policy changes immediately to SVM.**
2. **Once the policy collection is completed successfully, perform a Wake-up Agent on SVM.**
   1. **In the Trellix ePO - On-prem, click System Tree and select the managed SVMs.**
   2. **From the Actions drop-down list, click Agent → Wake up Agents → Wake Up Trellix Agent.**

      The Wake Up Trellix Agent page opens.
   3. **Select Options and Force policy update, then click OK.**

      You can view the status on the Server Task Log.
3. **Once the Wake-up Agent is completed successfully, test the antimalware (EICAR) on client.**
   1. **Log on to any client which is part of cluster where SVM is deployed.**
   2. **Download the test eicar file from eicar.org.**

      Once the malware is detected in client, it denies the access as the quarantine details are not configured by default in **Trellix ePO - On-prem**.
   3. **To delete the malware when it detects, configure the quarantine details.**
      1. Click **Menu** → **Policy** → **Policy Catalog** → **Options** → **My Default** → **Edit** → **Quarantine Manager** → **(Agentless only)**.



Policy

Policy Catalog 1 systems currently have policy "My Default".

MOVE AntiVirus 4.10.0: Policy Category > Options > My Default

Quarantine Manager	**Multi-Platform only** Quarantine Directory <SYSTEM_DRIVE>\Quarantine ☑ Specify the maximum number of days to keep quarantine data 28 days **Agentless only** Quarantine network share (Example:\\server-name\share) Network domain and username (Example:domain\username) Network password Confirm password SMB Version 2.1
SVM Server Communication (Multi-Platform only)	Scan server port 9053 (Important: Modifying this value will restart the SVM service)
SVM Assignment (Multi-Platform only)	● Assign SVM using SVM Manager SVM Manager Address (IP Address, host name, or FQDN) Port 8080 ○ Assign SVM manually

   4. **(Optional) If you don't want to configure the quarantine details for Agentless, you can choose to delete the malware when it detects.**
      1. Log on to **Trellix ePO - On-prem** as an administrator.
      2. Click **Menu** → **Policy** → **Policy Catalog** → **On Access Scan** → **My Default** → **Edit** → **Actions**.

iii. To disable the quarantine for Agentless, and to delete the malware when it detects, select **Delete files automatically** from the **Threat detection primary response** drop-down list.

Enable NSX tagging through Trellix ePO - On-prem

Using **Trellix ePO - On-prem**, you can create **On Access Scan** and **On Demand Scan** policies with the configurations needed for high security.

Before you begin

Make sure that:

- You have registered the **Trellix MOVE AntiVirus** service with **Trellix ePO - On-prem**.
- You have specified your vCenter details under **SVM Configuration** in the **Trellix MOVE AntiVirus SVM Settings** policy in **Trellix ePO - On-prem.**

Registering the **Trellix MOVE AntiVirus** service exports all **On Access Scan** policies of **Trellix MOVE AntiVirus** from **Trellix ePO - On-prem** to NSX-T. When a new **On Access Scan** policy is created or duplicated, all updates are immediately exported to NSX-T. These policies are included in the NSX-T Service Profiles.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Automation → MOVE AntiVirus Deployment.**
3. **On the Configuration tab under Agentless, click Server Settings → Edit.**

   The Edit Server Settings page opens.
4. **Select these tagging options under NSX Tagging and click Save.**
   - **NSX Virus Found Tag** — In the **Trellix ePO - On-prem** for the **On Access Scan** policy, if the primary action is configured to deny access to files and when malware is detected and deleted on a client system, the client system is tagged with `ANTI_VIRUS.VirusFound.threat=high`. When the file is deleted on a next successful on-demand scan, the tag is removed. On the NSX-T manager console, under **Inventory** → **Tags**, the VM systems with this tag gets added under the scope name `ANTI_VIRUS.VirusFound.threat=high`.
   - **NSX Unprotected Tag** — In the NSX-T Manager console, the system is tagged with this tag when the system is unprotected or the OAS scan is disabled. On the NSX-T manager console, under **Inventory** → **Tags**, the VM systems with this tag gets added under the scope name `MCAFEE.MOVE.unprotected=yes`.

Upgrade Trellix MOVE AntiVirus (Agentless)

Deploying a new SVM to the hypervisor in the previous version of **Trellix MOVE AntiVirus** (Agentless) requires you to unregister the existing SVM, then deploy the latest **Trellix MOVE AntiVirus** SVM to the hypervisor. This option ensures that you have the latest security updates.

Before starting the upgrade, make sure you are on supported versions of all **Trellix** and VMware products, refer the **Trellix MOVE AntiVirus** Release Notes.

If a supported version of **Trellix MOVE AntiVirus** is installed in your environment, you must upgrade to **Trellix MOVE AntiVirus** 4.9.x to install the **Trellix MOVE AntiVirus** 4.10.x with the upgraded extensions .

Upgrade from Trellix MOVE AntiVirus Extension 4.9.x

Before you begin

- **Trellix ePO - On-prem** 5.10.0 Update 11 or above
- VMware vSphere 7.0
- Uninstall **MOVE AntiVirus** Agentless
- Clean up your existing NSX-V deployment

You can't upgrade directly from **Trellix MOVE AntiVirus** version 4.8.x as the direct upgrade from 4.8.x is not supported.

Results

Uninstall Trellix MOVE AntiVirus Agentless from NSX-V environment with existing Trellix ePO - On-prem

To uninstall **Trellix MOVE AntiVirus** Agentless from your systems.

Remove the Security Policies from VMware vSphere Web Client:

1. Log on to the VMware vSphere Web Client as an administrator.
2. Navigate to **Home** → **Network & Security** → **Service Composer** → **Security Polices**.
3. Click the **Edit Security Policies**.
4. Delete the security policies that are added in **Guest Introspection Services**.

Uninstall MOVE AntiVirus Agentless from your NSX-V configuration:

1. Log on to the VMware vSphere Web Client as an administrator.
2. Navigate to **Home** → **Network & Security** → **Installation** → **Service Deployments**.
3. Select **MOVE AntiVirus** and then click the **Delete** icon (X).

Unregister MOVE Service from Trellix ePO - On-prem

1. Log on to the **Trellix ePO - On-prem** console.
2. Navigate to **Home** → **Network & Security** → **Installation** → **Service Deployments**.
3. Click **Service** → **NSX Manager** → **Unregister** to unregister from the vCenter Account.
4. In VMware vSphere Web Client, navigate to **Network & Security** → **Service Definitions** → **Services** and then verify that **Trellix MOVE AntiVirus** service is not present.

Clean up your existing NSX-V deployment

The **Trellix MOVE AntiVirus** Agentless 4.10.x upgrade only supports NSX-T configuration. The **Trellix MOVE Agentless** cannot support NSX-T configuration, while you have NSX-V configuration. So before upgrading the **Trellix MOVE AntiVirus**, make sure to get rid of all the previous NSX-V configurations.

Before you begin

NSX-V configuration in VMware vSphere Client

NSX-V configuration in **Trellix ePO - On-prem**

Task

1. **Unassign the policies and Security Groups configured under Service composer in VMware vSphere Client.**
2. **Undeploy SVA and Guest introspection from the Service Deployment in the VMware vSphere Client.**

Note

Once you undeploy the SVA, the client will be not protected.

3. **Unregister the NSX Manager from the Trellix ePO - On-prem under MOVE AntiVirus Deployment → Service.**

Download 4.10.x software extensions and packages

You can download these extensions and packages either from:

- The **Trellix ePO - On-prem** server, Software Catalog. For more information see, *Check in the software extensions and download packages from Software Catalog in the* ***Trellix ePO - On-prem***.
- The **Trellix** download site.

Note

Make sure to download the required extensions and packages from the **Trellix** download site.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Check in the extension and packages individually:**
   a. **Select Menu → Software → Extensions → Install Extension.**
   The Install Extension page opens.
   b. **Browse and select the extension files in the same order as mentioned below, and then click Open → OK:**

Extension description	Extension name
Trellix MOVE AntiVirus Agentless extension	i. MDCC_5.3.x.xx.zip ii. VSPHEREDCEXTN_5.4.x.xx.zip iii. DC__GS__4000_4.10.x.xx.zip iv. DC__AM__4000_4.10.x.xx.zip v. MOVEAVLIC400_4.10.x.xx.zip
Agentless SVM OVF package. For more information see, *Check in the* ***Trellix MOVE AntiVirus*** *SVM package to* ***Trellix ePO - On-prem***.	**MOVE-AV-AL_SVM_OVF_4.10.X.zip**

c. **Review the extension details and click OK.**

Upgrade the extensions on Trellix ePO - On-prem

The **Trellix MOVE AntiVirus** 4.10.x extension upgrades from 4.9.x extension on the **Trellix ePO - On-prem** server.

Task

1. **Click Menu → Software → Extensions → Install Extensions.**

   The Install Extension page opens.
2. **Browse and select the Trellix MOVE AntiVirus Agentless extension files in the same order as mentioned below, and then click Open → OK:**
   a. **MDCC_5.3.x.xx.zip**
   b. **VSPHEREDCEXTN_5.4.x.xx.zip**
   c. **DC__GS__4000_4.10.x.xx.zip**
   d. **DC__AM__4000_4.10.x.xx.zip**
   e. **MOVEAVLIC400_4.10.x.xx.zip**
3. **Review the extension details and click OK.**
4. **To initiate the vCenter account synchronization, click Menu → Configuration → Registered Cloud Accounts.**
5. **Select the registered cloud account and click Sync.**
6. **Verify that the vCenter account synchronization is completed successfully after upgrading the MOVE AntiVirus extension.**

Assign vCenter and Clients for NSX-T environment

There are two scenarios when you plan to assign vCenter and Clients for the NSX-T environment.

Scenario A

To use the same vCenter and Clients under it:

1. Delete the mob for the vCenter.
2. Resync the vCenter in RCA.

Scenario B

To Use new vCenter and Clients under it:

1. Add a new vCenter as **Compute Manager** in NSX-T console.
2. Configure the vCenter in NSX-T console.

Register a VMware vCenter account with Trellix ePO - On-prem (Agentless)

To use **Trellix MOVE AntiVirus** to manage the security of the virtual machines in your data center, you must first add your VMware vCenter to the **Trellix ePO - On-prem** server.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**

2. **Select Menu → Configuration → Registered Cloud Accounts.**
3. **From the bottom-left click Actions → Add Cloud Account to open the Add Cloud Account dialog box.**
4. **From the Choose Cloud Provider drop-down list, select VMware vSphere and click OK.**
5. **On the vCenter Account Details page, configure these options.**

Note

You must have a vCenter Server user account with administrator rights to use the autoscale feature.

Option	Description
Account Name	A name for the VMware vCenter account in **Trellix ePO - On-prem**. Account names can include characters a–z, A–Z, 0–9, and [_.-], without space.
Server Address	(Needed) IP address or the host name of the available VMware vCenter.
vCenter Username	(Needed) User name of the available VMware vCenter account.
vCenter Password	(Needed) Password of the available VMware vCenter account.
Sync Interval (In Minutes)	Specify the interval for running the next vCenter discovery (default value is 5 minutes).
Port	The port number needed to establish the connection with the available VMware vCenter (default port is 443).
Tag	The administrator specifies this to identify the VMs. Tag name can include characters a–z, A–Z, 0–9, and [_.-], with space.

6. **Click Test Connection to validate VMware vCenter account details and verify the connection to the VMware vCenter, then click Next → Finish.**
7. **When prompted to confirm, click OK to register the vCenter account and wait for vCenter sync to complete.**

This action registers the VMware vCenter and imports all discovered virtual machines, which are unmanaged, into the System Tree. The instances are imported with the same organization as the VMware vCenter.

Note

The virtual machines that **Trellix ePO - On-prem** added and managed are retained with the existing policy settings, but the virtualization properties for these systems are added.

Set up a general configuration for deployment (Agentless)

Before deploying **Trellix MOVE AntiVirus** SVM, configure settings on the **Trellix ePO - On-prem** server, so that they are retrieved and used for every **Trellix MOVE AntiVirus** SVM deployment.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Automation → MOVE AntiVirus Deployment.**
3. **In the Configuration tab, click General under General list.**

   The General Configuration page opens.
4. **Enter and confirm the password for Trellix ePO - On-prem Credentials section.**

   Trellix ePO - On-prem credentials

Options	**Description**
Password	Type the password of the **Trellix ePO - On-prem** console that the administrator has currently logged on
Confirm Password	Confirm the password

5. **Enter and confirm password for SVM (Agentless) and SVM Manager (Multi-Platform) Configuration section.**

   Note

   The **SVM (Agentless) and SVM Manager (Multi-Platform) Configuration** section shows a default password.

   Caution

   The password you enter is set to the SVM and you can't update it once the SVM is deployed. This password is not applicable to the SVM, which is already deployed.

   If required, change the password.

SVM (Agentless) and SVM Manager (Multi-platform) Configuration

Option	Description
Hostname Prefix (Agentless only)	Type a unique prefix that is added to the host name of the **Trellix MOVE AntiVirus** SVM. The prefix can include characters a–z, A–Z, 0–9, and [-], without space
Password	Type a password to be used as the **Trellix MOVE AntiVirus** SVM password during deployment. • The password must be at least 6 characters • The password must contain at least one uppercase letter (A-Z) and one numeral (0–9)
Confirm Password	Confirm the password

6. **Click Save to store these configurations, so that you can use them for every Trellix MOVE AntiVirus SVM deployment.**

Validate your NSX Manager using Trellix ePO - On-prem

The vSphere Connector extension automatically detects once vCenter sync is successful in RCA page and then it shows the details of your NSX Manager accounts in the **Trellix ePO - On-prem**. You must now register these NSX Manager servers with **Trellix ePO - On-prem**.

Using this configuration available on the **Trellix ePO - On-prem**, you can edit the details and validate the credentials of your NSX Manager.

Note

It is not recommended to provide the same **NSX manager** name for multiple vCenter accounts when registering NSX Manager.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Automation → MOVE AntiVirus Deployment.**
3. **In the Configuration tab, click NSX Manager under Agentless.**
   The **NSX Manager: Registration** page displays these options:

Option	Description
vCenter Account	Displays the name of the registered vCenter account
NSX Manager Name	Displays the name of your NSX Manager
Configuration Status	Specifies whether the NSX Manager is configured
Action	**Edit** — Click to edit and validate the credentials and other details of the NSX Manager accounts, which are automatically detected and sent to **Trellix ePO - On-prem**

4. **Click Edit under Action to open the Edit NSX Manager Details dialog box and edit these NSX Manager account options.**

Note

Make sure that your NSX Manager account and its details are ready.

Option	Description
vCenter Account	Specifies the name of the registered vCenter account **Note:** This option is predefined.
NSX Manager Name	Specifies the name of the available NSX Manager **Note:** Do not include spaces.
NSX Manager Address	Specifies the IP address or the host name of the available NSX Manager

Option	Description
	Note: This option is predefined.
NSX Manager Port	Specifies the port number of NSX Manager
NSX Manager Username	Specifies the user name of the available NSX Manager
NSX Manager Password	Specifies the password of the available NSX Manager

5. **Click Validate Credentials to verify the credentials of the NSX Manager and verify that the connection to the NSX Manager works.**
6. **Click Save to store the NSX Manager account details.**

Check in the Trellix MOVE AntiVirus SVM package to Trellix ePO - On-prem

Check in the **Trellix MOVE AntiVirus** SVM package to **Trellix ePO - On-prem**, so that it is available with VMware NSX Manager to deploy it to the cluster. You can view and delete the **Trellix MOVE AntiVirus** SVM package using **Trellix ePO - On-prem**.

Important

For a successful check-in, do not change the file name of the **Trellix MOVE AntiVirus** SVM package.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Automation → MOVE AntiVirus Deployment.**
3. **On the Configuration tab under Agentless, click SVM Repository to open the SVM OVF Details page with these Trellix MOVE AntiVirus SVM OVF options:**

Options	Description
SVM OVF Name	Name of the **Trellix MOVE AntiVirus** SVM package checked in to **Trellix ePO - On-prem**.
SVM OVF Version	Version of the **Trellix MOVE AntiVirus** SVM package checked in to **Trellix ePO - On-prem**.

Options	Description
SVM OVF Use Count	Specifies the number of hypervisors that are using this **Trellix MOVE AntiVirus** SVM.
Action	• **Delete** — To remove an existing **Trellix MOVE AntiVirus** SVM when it is not registered with any NSX Manager.

4. **Click Actions → Add SVM to open the Check-in SVM OVF (zip) file page.**
5. **Click Choose File to select the Trellix MOVE AntiVirus SVM package, then click Open → OK.**

   Note

   You can check in up to three versions of **Trellix MOVE AntiVirus** SVM starting from 4.x.x.

   The package to **Trellix ePO - On-prem** is checked in.
6. **(Optional) On the Configuration tab under Agentless, click Server Settings to enable NSX Unprotected Tag.**

Register the Trellix MOVE AntiVirus service with NSX-T Manager using Trellix ePO - On-prem

After registering your vCenter account details on NSX-T Manager and **Trellix ePO - On-prem**, use **Trellix ePO - On-prem** to enable the registration of **Trellix MOVE AntiVirus** (Agentless) as a service in NSX-T Manager.

The details of the registered vCenter, SVM OVF Version, and NSX-T Manager are automatically retrieved and displayed on the **Trellix ePO - On-prem** server. But you must register the **Trellix MOVE AntiVirus** service with the vCenter account. This registration permits the deployment of the service to the ESXi servers.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Automation → MOVE AntiVirus Deployment.**
3. **On the Service tab, click NSX Manager to open the MOVE Service Registration page with these options.**

Option	Description
NSX Manager Name	Displays the name of the registered NSX-T Manager.
NSX Manager Address	Displays the IP address of your NSX-T Manager.

Option	Description
vCenter Account	Displays the name of the vCenter account that is registered with NSX-T Manager and **Trellix ePO - On-prem**.
Registered SVM Version	Displays the version of the **Trellix MOVE AntiVirus** SVM package checked in to **Trellix ePO - On-prem**.
Service Registration Status	Displays registration status values **Registered**, **Not Registered**, and **Registration Failed**.
Actions	• **Register** — Click to select the latest **Trellix MOVE AntiVirus** SVM and register it to the vCenter that is added to your NSX-T Manager. • **Unregister** — Click to unregister the **Trellix MOVE AntiVirus** service and to remove it from the vCenter. • **Upgrade** — Click to upgrade the **Trellix MOVE AntiVirus** service. ⚠ **Caution:** Make sure that you checked in the latest **Trellix MOVE AntiVirus** SVM required for the upgrade. Otherwise, the existing **Trellix MOVE AntiVirus** service is deployed to the ESXi servers.

4. **Click Register under Actions to open the MOVE Service Registration dialog box.**
5. **Select the latest Trellix MOVE AntiVirus SVM and click OK.**
   The **Trellix MOVE AntiVirus** service is now registered with the vCenter account that is registered with your NSX-T Manager.
6. **On the NSX-T Data Center console, verify that the Trellix MOVE AntiVirus service is now available under System → Service Deployments → Catalog.**

Deploy the Trellix MOVE AntiVirus SVM

To provide **Trellix MOVE AntiVirus** (Agentless) protection to the virtual machines on your ESXi servers, you must install the **Trellix MOVE AntiVirus** service (**Trellix MOVE AntiVirus** SVM) on your ESXi servers.

Before you begin

Make sure that:

- The host, where you are deploying the SVM using NSX-T Manager, is part of a cluster
- The datacenter is using a vSphere distributed switch
- The Guest Introspection service is installed on all ESXi servers
- The virtual machines have the latest VMware Tools installed and have the Guest Introspection Thin Agent enabled for both Windows and Linux VMs.
- You have appropriate permission to perform the SVM deployment using **Trellix ePO - On-prem**. You can enable this permission by navigating through **Menu** → **Users** → **Permission Sets** → **MOVE AV [Agentless] SVM Deployment** → **Edit**.

Deploy the **Trellix MOVE AntiVirus** services on a set of clusters. Manage service deployments here by adding new services or deleting existing ones.

This deployment automatically provides virus protection for virtual machines on a new hypervisor from the moment the hypervisor is added to the clusters. When a new cluster is added, deploy the **Trellix MOVE AntiVirus** SVM again.

Task

1. **Log on to the NSX-T Data Center manager as an administrator.**
2. **In the NSX-T Data Center manager console, navigate to System and then in the left pane, click Service Deployment.**
3. **Select Partner service from the drop-down list and then click Deploy Service.**
4. **To configure the service deployment:**
   a. **Enter the name under Service Deployment Name.**
   b. **Select your desired Compute Manager, Cluster, and Data Store.**
   c. **Click Edit Details.**

      A Networks dialog box appears on your screen.
   d. **Choose your Management NIC and their Network, Network Type as per your environment and click Save.**
5. **In the NSX-T Data Center manager, select System → Service Deployment, click Save. The service deployment starts and after successful Service deployment SVA is installed vCenter.**

Results

Service Status	ID	Description
UNKNOWN	3	Specifies that the **Trellix MOVE AntiVirus** service status is unknown
UP	N/A	Not applicable
DOWN	1	Specifies that the **Trellix MOVE AntiVirus** service is stopped

The **Trellix MOVE AntiVirus** service is now deployed to the cluster when the **Installation Status** is **Successful** and the **Service Status** is **UP**.

Verify the SVM deployment on Trellix ePO - On-prem

To verify the Managed State of the deployed SVM.

Before you begin

Make sure that:

- The **Trellix MOVE AntiVirus** service is registered with **Trellix ePO - On-prem**.
- You deploy the **Trellix MOVE AntiVirus** SVM.
- The **Installation Status** appear as **Succeeded** and **Service Status** as **Up** in NSX-T console.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → System Tree → Systems.**
3. **Under Managed State column, verify the SVM state as Managed.**

Note

The SVM name is in the format of **<NSX Manager Name>-<Hostname prefix>-host-xx** .

Post-upgrade tasks

Configure the security group and security policy in NSX-T Manager

You must create the security policy and apply it to the security group of VMs that you want to protect.

The security policies for **Trellix MOVE AntiVirus** are automatically exported from **Trellix ePO - On-prem** after you register the **Trellix MOVE AntiVirus** service on **Trellix ePO - On-prem**. This configuration is a one-time initial activity for a vCenter. But you must repeat this configuration when a new datacenter is added.

Create an NSX-T service profile

Create an NSX-T service profile with **Trellix MOVE AntiVirus** (Agentless).

Before you begin

Make sure that:

- The **Trellix MOVE AntiVirus** service is registered with **Trellix ePO - On-prem**.
- You deploy the **Trellix MOVE AntiVirus** SVM.

Task

1. **Log on to the NSX-T manager console as an administrator.**
2. **Select Security → Endpoint Protection → Endpoint Protection Rules, then click the Security Profiles tab.**
3. **In the Service Profiles page, click Add Service Profile.**
4. **Complete the details of the service profile:**
    a. **In the Service Profile Name, enter the name of the service profile.**
    b. **In the Service Profile Description, enter a description for the profile (optional).**

   c. **In the Vendor Template, select the policy configured in the Trellix ePO - On-prem.**

5. **Click Save. The status of the Service Profile changes to Success on successful configuration.**

Results

You have created your NSX-T service profile for the **Trellix MOVE AntiVirus** (Agentless).

Create an NSX-T security policy and rule

Create an NSX-T security policy with **Trellix MOVE AntiVirus** (Agentless) enabled as a Guest Introspection Service.

Before you begin

Make sure that:

- The **Trellix MOVE AntiVirus** service is registered with **Trellix ePO - On-prem**.
- You deploy the **Trellix MOVE AntiVirus** SVM.

Task

1. **Log on to the NSX-T manager console as an administrator.**
2. **Select Security → Endpoint Protection → Endpoint Protection Rules, then click the Rules tab.**
3. **In the Rules page, click +Add Policy.**

   The policy gets listed in the list of available policies.
4. **In the list of policies, click the desired policy and click +Add Rule.**
5. **In the new rule, rename the rule name and click the Edit icon under the Groups column.**

   The **Set Groups** dialog box appears on the screen.
6. **Select a group in the list and click Apply.**

   The selected group appears in the list.
7. **Click the Edit icon under the Service Profiles column.**

   The **Set Service Profile** dialog box appears on the screen.
8. **Select a service profile in the list and click Save.**

   The selected service profile appears in the list.
9. **Click Publish to change the status from Uninitialized to Success.**

Results

You have created your NSX-T security policy for deploying **Trellix MOVE AntiVirus** (Agentless).

Create an NSX-T Security Group

Select the required Clusters or Virtual Machines from the available vCenter and configure them as a security group. This configuration allows you to assign the security policy to the group and protect its VMs.

Before you begin

Make sure that:

- VMware vSphere is installed and added to the cluster.
- The **Trellix MOVE AntiVirus** service is registered with NSX-T Data Center Manager using **Trellix ePO - On-prem**.

- You deploy the **Trellix MOVE AntiVirus** SVM

Task

1. **Log on to the NSX-T manager console as an administrator.**
2. **Select Security → Endpoint Protection → Endpoint Protection Rules, then click the Rules tab.**
3. **In the list of policies, click the desired policy and click +Add Rule.**
4. **In the new rule, rename the rule name and click the Edit icon under the Groups column.**

   The **Set Groups** dialog box appears on the screen.
5. **In the Set Groups dialog box, click +Add Group.**
6. **Enter the name in the Group Name field.**
7. **Click Set Members under the Compute Members column.**

   The **Select Members** dialog box appears on the screen.
8. **Under Membership Criteria, click +Add Criteria to add multiple criteria. Maximum number of allowed criteria are five.**
9. **In the Criteria row, select the desired values from the dropdown lists and enter the field values, then click Apply.**
10. **Click Save and click View Members to check the effective list of virtual machines in the group.**

Results

Your security group is added and contains the virtual machines to be protected from the selected cluster.

Policy Reflection from NSX-T to Trellix ePO - On-prem

After applying the Security Policy (for example, SP1) to Security Group (for example, SG1), the On Access policy which is assigned in SP1 will be applied to all VMs which are part of SG1.

Before you begin

Make sure that:

- The virtual machines (VMs) are installed with the latest VMware Tools and the Guest Introspection Thin Agent is enabled for both Windows and Linux. For more information see, *Install the Guest Introspection Thin Agent for Virtual Machines*.
- You deploy the **Trellix MOVE AntiVirus** SVM.
- You apply the NSX security policy to the NSX security group

The policies assigned to VMs are reflected in the **Trellix ePO - On-prem** under **Policy Catalog**.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Policy → Policy Catalog.**

   The Policy Catalog page opens.
3. **Select MOVE AntiVirus 4.x.x from the Product drop-down list.**
4. **Select On Access Scan from the Category drop-down list.**
5. **Click Assignments to view the assigned VMs.**
6. **To view all VMs from SG1 in Trellix ePO - On-prem Policy Catalog, make sure that all VMs are:**

   - In turned on state.
   - Installed with the latest VMtools.

Configure the vCenter details in SVM Settings policy in Trellix ePO - On-prem

You must specify these details under **SVM Configuration** in the **Trellix MOVE AntiVirus SVM Settings** policy in **Trellix ePO - On-prem**.

Note

If you failed to provide the vCenter details:

- The IP address for the threat events generated for client will not appear.
- The Security tags will not work.
- The **Agentless Anti-Malware Protection Status** for the clients will not appear.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Policy → Policy Catalog.**
3. **Select MOVE AntiVirus 4.x.x from the Product drop-down list, then select SVM Settings from the Category drop-down list.**
4. **Click Edit SVM Setting policy .**
5. **Under SVM Configuration, configure these settings as needed, then click Save.**
   - **Hypervisor/vCenter Server** — Enter the valid IP address of either the hypervisor that the SVM resides on or the vCenter server (vCenter details are recommended to provide here).
   - **Protocol** — Select **https** or **http**, depending on the protocol the server uses to receive client requests.
   - **vCenter/ESXi Port** — Specify the port number of the SVM. The default port is 443.
   - **Username** — Enter the user name credentials to connect with the server.

     Note

     The user account requires at least read access to the vCenter server or the ESXi host. Domain-based credentials are supported only when the vCenter server or the ESXi host has been configured to support domain-based authentication.

   - **Password** — Enter the password associated with the user.

     Note

     After you save and reopen the **SVM Settings** policy, the vCenter **Password** field appears blank. Though it appears blank, the password is encrypted and saved in the policy settings. Confirm the password to test connection settings.

   - **Confirm password** — confirm the password.
   - **SVM Time Zone** — Select your local time zone from the drop-down list.

- **NTP Servers(s)** — Select **Use Default** servers or **Use following Servers**. If **Use following Servers** is selected, enter the NTP server details.

6. **Click Test connection settings to test the connection to the hypervisor/vCenter Server and then click Save.**

Perform wake-up agent and Antimalware test (EICAR)

Once the SVM appears as Managed in **Trellix** System Tree, perform wake up agent on the SVM and antimalware test (EICAR) on clients.

Before you begin

Make sure that:

- You deploy the **Trellix MOVE AntiVirus** SVM.
- You apply the NSX-T security policy to the NSX-T security group.
- The policy reflection of On Access policy from NSX-T to **Trellix ePO - On-prem**.
- SVM appears as Managed in **Trellix ePO - On-prem** System Tree.

Note

As the **Trellix** software is not installed in the Agentless, the client appears as unmanaged in the **Trellix ePO - On-prem** System Tree.

Task

1. **Policy enforcement based on time configured at Trellix ePO - On-prem.**
   1. **In the Trellix ePO - On-prem, click Menu → Automation → MOVE AntiVirus Deployment → Configuration → Agentless → Server Settings.**

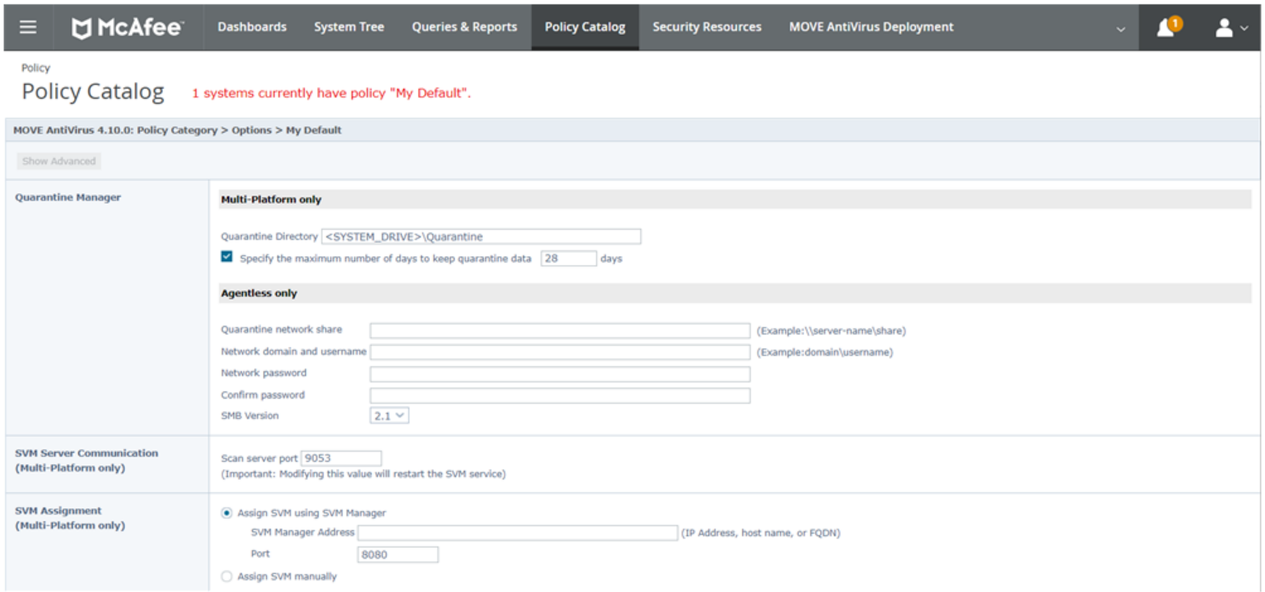
      The Server Settings page opens.
   2. **The default Policy Enforcement Interval (Minutes) is 60 minutes. This reflects that all policy changes in every 60 minutes automatically to SVM.**
   3. **Click Run for Run Policy Collection to reflect any policy changes immediately to SVM.**
2. **Once the policy collection is completed successfully, perform a Wake-up Agent on SVM.**
   1. **In the Trellix ePO - On-prem, click System Tree and select the managed SVMs.**
   2. **From the Actions drop-down list, click Agent → Wake up Agents → Wake Up Trellix Agent.**

      The Wake Up Trellix Agent page opens.
   3. **Select Options and Force policy update, then click OK.**

      You can view the status on the Server Task Log.
3. **Once the Wake-up Agent is completed successfully, test the antimalware (EICAR) on client.**
   1. **Log on to any client which is part of cluster where SVM is deployed.**
   2. **Download the test eicar file from eicar.org.**

      Once the malware is detected in client, it denies the access as the quarantine details are not configured by default in **Trellix ePO - On-prem**.
   3. **To delete the malware when it detects, configure the quarantine details.**

i. Click **Menu** → **Policy** → **Policy Catalog** → **Options** → **My Default** → **Edit** → **Quarantine Manager** → **(Agentless only)**.



Policy Catalog 1 systems currently have policy "My Default".

MOVE AntiVirus 4.10.0: Policy Category > Options > My Default

Quarantine Manager

Multi-Platform only

Quarantine Directory <SYSTEM_DRIVE>\Quarantine

☑ Specify the maximum number of days to keep quarantine data 28 days

Agentless only

Quarantine network share (Example:\\server-name\share)

Network domain and username (Example:domain\username)

Network password

Confirm password

SMB Version 2.1

SVM Server Communication (Multi-Platform only)

Scan server port 9053

(Important: Modifying this value will restart the SVM service)

SVM Assignment (Multi-Platform only)

● Assign SVM using SVM Manager

SVM Manager Address (IP Address, host name, or FQDN)

Port 8080

○ Assign SVM manually

d. **(Optional) If you don't want to configure the quarantine details for Agentless, you can choose to delete the malware when it detects.**
   i. Log on to **Trellix ePO - On-prem** as an administrator.
   ii. Click **Menu** → **Policy** → **Policy Catalog** → **On Access Scan** → **My Default** → **Edit** → **Actions**.
   iii. To disable the quarantine for Agentless, and to delete the malware when it detects, select **Delete files automatically** from the **Threat detection primary response** drop-down list.

Enable NSX tagging through Trellix ePO - On-prem

Using **Trellix ePO - On-prem**, you can create **On Access Scan** and **On Demand Scan** policies with the configurations needed for high security.

Before you begin

Make sure that:

- You have registered the **Trellix MOVE AntiVirus** service with **Trellix ePO - On-prem**.
- You have specified your vCenter details under **SVM Configuration** in the **Trellix MOVE AntiVirus SVM Settings** policy in **Trellix ePO - On-prem**.

Registering the **Trellix MOVE AntiVirus** service exports all **On Access Scan** policies of **Trellix MOVE AntiVirus** from **Trellix ePO - On-prem** to NSX-T. When a new **On Access Scan** policy is created or duplicated, all updates are immediately exported to NSX-T. These policies are included in the NSX-T Service Profiles.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Automation → MOVE AntiVirus Deployment.**
3. **On the Configuration tab under Agentless, click Server Settings → Edit.**

The Edit Server Settings page opens.

4. **Select these tagging options under NSX Tagging and click Save.**

   - **NSX Virus Found Tag** — In the **Trellix ePO - On-prem** for the **On Access Scan** policy, if the primary action is configured to deny access to files and when malware is detected and deleted on a client system, the client system is tagged with ANTI_VIRUS.VirusFound.threat=high. When the file is deleted on a next successful on-demand scan, the tag is removed. On the NSX-T manager console, under **Inventory** → **Tags**, the VM systems with this tag gets added under the scope name ANTI_VIRUS.VirusFound.threat=high.
   - **NSX Unprotected Tag** — In the NSX-T Manager console, the system is tagged with this tag when the system is unprotected or the OAS scan is disabled. On the NSX-T manager console, under **Inventory** → **Tags**, the VM systems with this tag gets added under the scope name MCAFEE.MOVE.unprotected=yes.

Uninstall Trellix MOVE AntiVirus (Agentless)

The process of removing **Trellix MOVE AntiVirus** (Agentless) consists of removing the **Trellix MOVE AntiVirus** service from the clusters and removing the configurations and extensions from **Trellix ePO - On-prem**.

Uninstall the Trellix MOVE AntiVirus 4.x.x in an NSX-T environment

A full uninstallation involves removing these components: **Trellix MOVE AntiVirus** SVM, **Trellix MOVE AntiVirus** service, NSX-T Manager details, and the **Trellix MOVE AntiVirus** extension.

Remove Trellix MOVE AntiVirus SVM from the cluster

Using the NSX-T console, you can remove the **Trellix MOVE AntiVirus** service, which is deployed to one or more clusters.

Task

1. **Log on to NSX-T console as an administrator.**
2. **Click System → Service Deployments → Deployment.**
3. **Click the Available Actions icon and click Delete or Force Delete.**

   The Delete Service Deployment window opens.
4. **Click Delete to delete the service deployment.**

Unregister the Trellix MOVE AntiVirus service with NSX Manager from Trellix ePO - On-prem

Select the registered VMware NSX-T Manager and unregister it from the **Trellix ePO - On-prem** server.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Automation → MOVE AntiVirus Deployment → Service → NSX Manager. This action lists all NSX-T Managers registered in Trellix ePO - On-prem.**
3. **From the Actions column on the MOVE Service Registration page, click Unregister for the registered NSX-T Manager. A confirmation dialog box appears.**
4. **Click OK to confirm.**

Uninstall the extension

Uninstall the **Trellix MOVE AntiVirus** extensions from **Trellix ePO - On-prem**.

Task

1. **Log on to Trellix ePO - On-prem as an administrator.**
2. **Select Menu → Software → Extensions.**
3. **From the Extensions tab under McAfee group, select Data Center Security.**
4. **Click Remove next to each extension in this order.**

    - MOVE AntiVirus License
    - MOVE AntiVirus
    - MOVE AntiVirus Common
    - vSphere Connector Extension
    - MDCC

COPYRIGHT