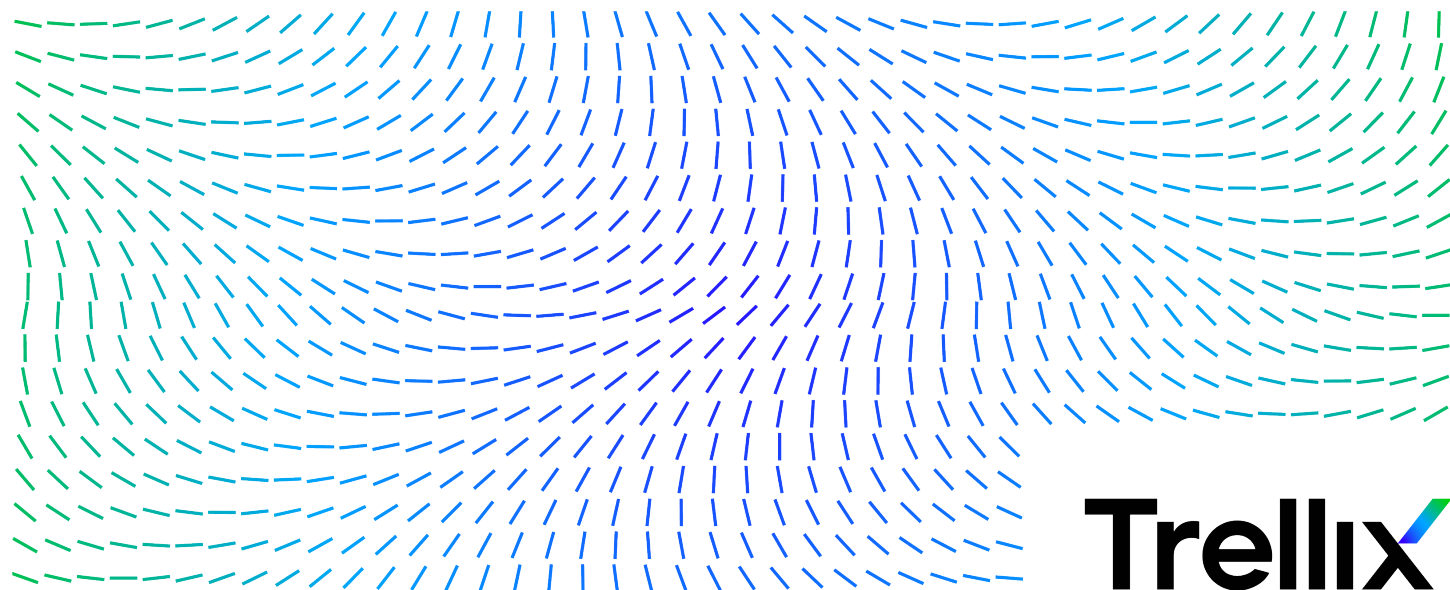


Trellix MOVE AntiVirus 4.10.x Interface Reference Guide



Contents

MOVE AntiVirus page-level reference.	4
General page (Configuration tab).	4
IP Pool page (Configuration tab).	5
NSX Manager Registration page.	6
Trellix MOVE AntiVirus Service Registration (NSX) page.	6
Edit NSX Manager Details page.	8
vShield Manager page (Configuration tab).	8
SVM Repository page (Configuration tab).	9
Check-in SVM (zip) File page.	10
Server Settings page (Configuration tab).	10
Edit Server Settings page (Configuration tab).	11
Infrastructure Details page (Configuration tab).	12
Configure Autoscale Infrastructure Group Details page.	13
Edit Infrastructure Details page (Configuration tab).	14
SVM Manager Configuration (Configuration tab).	16
Check-in SVM Manager OVF (zip) File page.	17
Client Deployment Configuration page.	17
SVM Configuration (Configuration tab).	18
Configure SVM OVF page.	18
Autoscale SVM Details page (Configuration tab).	20
Selection page (Service setup).	21
Configuration page (Service setup).	22
Verification page (Service setup).	23
Selection page (Service remove).	24

Verification page (Service remove).	25
Job Status page (Service setup).	25
Deployment and task status details page.	26
Options page (Trellix MOVE AntiVirus Common).	29
On-access Scan page (Trellix MOVE AntiVirus).	30
On-demand Scan page (Trellix MOVE AntiVirus).	35
Options page (Trellix MOVE AntiVirus).	37
Shared Cloud Solutions page (MOVE AntiVirus).	39
SVM Manager Settings page (MOVE AntiVirus).	40
SVM Settings page (MOVE AntiVirus).	45
Schedule page (Targeted on-demand scan).	49
Summary page (Targeted on-demand scan).	51

MOVE AntiVirus page-level reference

General page (Configuration tab)

Allows you to configure your **Trellix ePO - On-prem** details, **Trellix MOVE AntiVirus SVM (Agentless)**, and **SVM Manager (Multi-Platform)** details on the **Trellix ePO - On-prem** server.

Option	Definition
McAfee ePO Credentials	<ul style="list-style-type: none"> • Password — Type the password of the Trellix ePO - On-prem management console that the administrator has currently logged on. • Confirm Password — Retype the password of the Trellix ePO - On-prem management console that the administrator has currently logged on.
SVM (Agentless) and SVM Manager (Multi-Platform) Configuration	<ul style="list-style-type: none"> • Hostname Prefix (Agentless only) — Type a unique prefix that is added to the host name of the SVM. The prefix can include characters a–z, A–Z, 0–9, and [-], without space. • Password — This field is used to configure your password for Trellix MOVE AntiVirus SVM (Agentless) or SVM Manager (Multi-Platform). (Agentless) Type a password for the available Trellix MOVE AntiVirus SVM. This password is set for the SVM after deployment. (Multi-Platform) Type a password for the available SVM Manager (Multi-Platform). This password is set for the SVM Manager after deployment. <ul style="list-style-type: none"> ▫ The password must be at least 6 characters long. ▫ The password must contain at least one uppercase letter (A–Z) and one numeric character (0–9). • Confirm Password — Retype the password.
Save	Click to store these configurations, so that you can use them for every Trellix MOVE AntiVirus

Option	Definition
	SVM (Agentless) or SVM Manager (Multi-Platform) deployment.
Reset	Click to reset the parameters.

IP Pool page (Configuration tab)


Before configuring the IP address as Static, create an IP Pool. You can then select this IP Pool during the SVM deployment, so that any unused IP address of the IP Pool is automatically assigned to the SVM.

Option	Definition
IP Pool Name	Type a name for the IP Pool.
Start IP	Type the starting IP address for the pool.
End IP	Type the ending IP address for the pool.
Gateway	Type the default gateway address.
Prefix Length	Type the Prefix length.
Primary DNS	(Optional) Type the IP address of the Primary DNS server for hostname-to-IP address resolution.
Secondary DNS	(Optional) Type the IP address of the Secondary DNS server for hostname-to-IP address resolution.
Used / Total	Specifies the total number of IP addresses and the number of used IP addresses of the IP Pool. Example: 2/3 means that 2 IP addresses are used out of the available 3 IP addresses in the IP Pool.
Action	<ul style="list-style-type: none">• Edit — Use this option to edit the IP Pool details.• Delete — Use this option to delete the IP Pool when its IP addresses are not in use.

Option	Definition
Actions	Add IP Pool — Select to configure the IP Pool details required for SVM deployment.


NSX Manager Registration page

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

Option	Definition
vCenter Account	Specifies the name of the registered vCenter account.
NSX Manager Name	Specifies the name of your NSX Manager.  Note: Do not include spaces.
Configuration Status	Displays these registration statuses: <ul style="list-style-type: none"> • Configured — Indicates that NSX Manager is registered and ready for deployment. • Not Configured — Indicates that the NSX Manager is not registered. Therefore click Edit and configure it before deployment. • Credentials unknown — Indicates that the NSX Manager is registered with VMware vCenter, but the credentials are unknown. Click Edit and configure it before deployment.
Action	Edit — Click to open the Edit NSX Manager Details dialog box and edit the NSX Manager account details.


Trellix MOVE AntiVirus Service Registration (NSX) page

You can select the required **Trellix MOVE AntiVirus SVM** version and register it with VMware NSX Manager, which was registered to the **Trellix ePO - On-prem** server. This allows you to deploy the **Trellix MOVE AntiVirus SVM** to one or more clusters.

Option	Definition
NSX Manager Name	Specifies the name of the registered NSX Manager.
NSX Manager Address	Specifies the IP address of your NSX Manager.
vCenter Account	Specifies the name of the vCenter account that is registered with NSX Manager and Trellix ePO - On-prem .
Registered SVM Version	Specifies the version of the Trellix MOVE AntiVirus SVM checked in to Trellix ePO - On-prem .
Service Registration Status	<p>Displays these registration statuses values:</p> <ul style="list-style-type: none"> • Registered — Indicates that the Trellix MOVE AntiVirus service is registered and ready for deployment. • Not Registered — Indicates that the Trellix MOVE AntiVirus service is not registered. • Registration Failed — Indicates that the Trellix MOVE AntiVirus service is failed.
Actions	<ul style="list-style-type: none"> • Register — Click to select the latest Trellix MOVE AntiVirus SVM and register it to the vCenter that is added to your NSX Manager. • Unregister — Click to unregister the Trellix MOVE AntiVirus service and to remove it from the vCenter that is added to your NSX Manager. • Upgrade — Click to upgrade the Trellix MOVE AntiVirus service. <div>  Note: Make sure that you have checked in the latest SVM required for the upgrade. Otherwise, the existing Trellix MOVE AntiVirus service is deployed to the ESXi servers. </div>

Edit NSX Manager Details page

Use this page to view and edit the configuration details of your NSX Manager.

Option	Definition
vCenter Account	Specifies the name of the registered vCenter account.
NSX Manager Name	Type the name of the available NSX Manager.  Note: Do not include spaces.
NSX Manager Address	Type the IP address or the host name of the available NSX Manager.
NSX Manager Port	Specifies the port number of NSX Manager.
NSX Manager Username	Type the user name of the available NSX Manager.
NSX Manager Password	Type the password of the available NSX Manager.
Validate Credentials	Click to verify the credentials of the NSX Manager and check that the connection to the NSX Manager works.
Save	Saves the NSX Manager details.
Cancel	Navigates to the previous page.

vShield Manager page (Configuration tab)

Use this page to view and edit the configuration details of the vShield Manager.

Option	Definition
vCenter Account	Specifies the name of the registered vCenter account.

Option	Definition
vShield Manager	Specifies the name of the registered vShield Manager.
Configuration Status	<p>Displays these configuration statuses:</p> <ul style="list-style-type: none">• Configured — Indicates that the vShield Manager is registered and ready for deployment.• Not Configured — Indicates that the vShield Manager is not registered. Therefore, click Edit and configure it before deployment.• Credentials unknown — Indicates that the vShield Manager is registered with VMware vCenter, but the credentials are unknown. Click Edit and configure it before deployment.
Action	Edit — Click to edit and validate the existing vShield Manager configuration.

SVM Repository page (Configuration tab)

You must check in and host the SVM package in **Trellix ePO - On-prem**, so that you can deploy it to the hypervisor. You can view and delete the SVM package using **Trellix ePO - On-prem**.

Option	Definition
SVM Name	Specifies the name of the Trellix MOVE AntiVirus SVM package checked in to Trellix ePO - On-prem .
SVM Version	Specifies the version of the Trellix MOVE AntiVirus SVM package checked in to Trellix ePO - On-prem .
SVM Use Count	Specifies the number of SVMs, which are present in the infrastructure.
Action	Delete — To remove an existing Trellix MOVE AntiVirus SVM when it is not deployed to any hypervisor. It is possible to delete the SVM only when the SVM Use Count is zero.

Option	Definition
Actions	Add SVM — Select to open the Check-in SVM (zip) File page.

Check-in SVM (zip) File page


Allows you to browse and select the SVM package for Agentless deployment, so that it checks-in the SVM package to **Trellix ePO - On-prem**.

Option	Definition
SVM OVF Details	<ul style="list-style-type: none">• Select SVM (zip) file to check-in — Browse to and select the Trellix MOVE AntiVirus SVM package.
OK	Checks-in the SVM package to Trellix ePO - On-prem .
Cancel	Cancels the check-in.

Server Settings page (Configuration tab)

Use this page to view and edit the configuration details of the NSX server.

Option	Definition
Policy Enforcement Interval (Minutes)	Specifies the interval for policy enforcement in minutes.
Policy Collector	Enable this option to enforce unique scan policies on specific virtual machines protected by SVM.
NSX Tagging Interval (Minutes)	Specifies the interval for NSX tagging for detecting malware.
Run Policy Collector	Click Run to collect the policies that are available in NSX Manager.

Option	Definition
	 Note: On successful completion of policy collection, message appears as Policy collection completed successfully .
NSX Tagging	<p>Specifies that the VM is tagged with the tag for detecting malware.</p> <ul style="list-style-type: none"> • NSX Virus Found Tag — Enable this option so that the VM is tagged with ANTI_VIRUS.VirusFound.threat=high on detecting a malware. • NSX Unprotected Tag — Enable this option to automatically retrieve the details of the unprotected VMs, tag them with MCAFEE.MOVE.unprotected=yes, and display them on the NSX Manager. This tag resource indicates that these VMs are not protected by Trellix MOVE AntiVirus. By default, this option is enabled. The MCAFEE.MOVE.unprotected=yes tag is automatically removed from the VMs when they are protected.
Edit	Click to open the Edit Server Settings page and edit the NSX server settings.

Edit Server Settings page (Configuration tab)

Before deploying the SVM, complete this one-time configuration on the **Trellix ePO - On-prem** server, so that these settings are retrieved and used for every SVM deployment, which is done from the same **Trellix ePO - On-prem** server.

Option	Definition
Policy Enforcement Interval (Minutes)	Specify the interval for policy enforcement in minutes. Default interval time is 60 minutes.

Option	Definition
NSX Tagging Interval (Minutes)	Specify the interval for NSX tagging for detecting malware. Default interval time is 60 minutes.
NSX Tagging	<p>Allows you to set the tagging settings on detecting malware.</p> <ul style="list-style-type: none">• NSX Virus Found Tag — Enable this option so that the VM is tagged with ANTI_VIRUS.VirusFound.threat=high on detecting a malware.• NSX Unprotected Tag — Enable this option to automatically retrieve the details of the unprotected VMs, tag them with MCAFEE.MOVE.unprotected=yes, and display them on the NSX Manager. This tag resource indicates that these VMs are not protected by Trellix MOVE AntiVirus. By default, this option is enabled. The MCAFEE.MOVE.unprotected=yes tag is automatically removed from the VMs when they are protected.
Save	Saves the NSX server settings.
Cancel	Navigates to the previous page.

Infrastructure Details page (Configuration tab)


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

Option	Definition
Group Name	Specifies the name of the infrastructure group.
Cloud Account Name	Specifies the account name of the registered vCenter account.

Option	Definition
ESXi / Cluster	Specifies the IP address or name of the hypervisor or the cluster selected as part of the infrastructure group.
IP Pool Name	Specifies the name of the IP Pool used in the infrastructure group.
Provisioning Type	Specifies the provision 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.
Action	<ul style="list-style-type: none"> • Edit — Click to edit the infrastructure group properties. • Delete — Click to delete any of the unused infrastructure group.
Actions	<ul style="list-style-type: none"> • Create — Select to configure the properties for the custom infrastructure group details. It is not mandatory to configure the custom group details when the default group is available.

Configure Autoscale Infrastructure Group Details page


Allows you to configure these properties for the custom infrastructure group details.

Option	Definition
Group Name	<p>Type a unique name for the virtual infrastructure group.</p> <div>  Note: Do not include spaces. </div>

Option	Definition
Infrastructure Type	Select whether you want to create a group based your hypervisor or cluster.
Select Host or Select Cluster	<ul style="list-style-type: none">• Select Host — Select the IP address of your host.• Select Cluster — Select the IP address of your 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	Select the IP Pool type as Static or DHCP from the drop-down list.
AD Server	Select the registered Active Directory server, so that the deployed SVM is automatically added to the selected domain.
Provisioning Type	Select the provision type as Thin or Thick from the drop-down list.
Network Name	Select the required management network from the drop-down list.
Datastore Name	Select the configured datastore for the infrastructure.
Save	Saves the infrastructure group details.
Back	Navigates to the previous page.

Edit Infrastructure Details page (Configuration tab)

This page allows you to edit the properties of an existing infrastructure group details.

Option	Definition
Group Name	<p>Type a unique name for the virtual infrastructure group.</p> <div>  Note: Do not include spaces. </div>
Select Virtual Account	Select the infrastructure cloud account to edit.
Infrastructure Type	Select whether you want to create a group based your hypervisor or cluster.
Select Host or Select Cluster	<ul style="list-style-type: none"> • Select Host — Select the IP address of your host. • Select Cluster — Select the IP address of your 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	Select the IP Pool type as Static or DHCP from the drop-down list.
AD Server	Select the registered Active Directory server, so that the deployed SVM is automatically added to the selected domain.
Provisioning Type	Select the provision type as Thin or Thick from the drop-down list.
Network Name	Select the required management network from the drop-down list.
Datastore Name	Select the configured datastore for the infrastructure.
Save	Saves the infrastructure group details.

Option	Definition
Back	Navigates to the previous page.

SVM Manager Configuration (Configuration tab)

Allows you to view and configure the SVM Manager OVF details for SVM Manager deployment to your hypervisor.

Option	Definition
SVM Manager OVF Name	Specifies the name of the SVM Manager OVF package checked in to the Trellix ePO - On-prem server.
SVM Manager OVF Version	Specifies version of the SVM Manager OVF package checked in to the Trellix ePO - On-prem server.
Action	<ul style="list-style-type: none">• Delete — Click to delete any of the checked in SVM Manager OVF.
Actions	<ul style="list-style-type: none">• Add SVM Manager — Click to open the Check-in SVM Manager OVF (zip) File page.
Deployment Configuration	<ul style="list-style-type: none">• Infrastructure Group — Select the Default Group or an infrastructure group you created.• 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 applied to the SVM Manager.• Deploy SVM Manager — Click to deploy the SVM Manager to your hypervisors.• Upgrade SVM Manager — Click to upgrade the existing SVM Manager.• Delete SVM Manager — Click to remove the SVM Manager checked in to the Trellix ePO - On-prem.

Check-in SVM Manager OVF (zip) File page

Allows you to 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.

Option	Definition
SVM Manager OVF Check-in	<ul style="list-style-type: none">• Select SVM Manager OVF (zip) file to check-in — Browse to and select the SVM Manager OVF package for deployment.• Specify the location of McAfee ePO 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.
OK	Checks in the SVM Manager OVF package to the Trellix ePO - On-prem server.
Cancel	Navigates to the previous page.

Client Deployment Configuration page

Using this page, you can configure and deploy the client package to virtual machines, so that **Trellix ePO - On-prem** can manage the **Trellix MOVE AntiVirus** configuration on client systems.

Option	Definition
Client Configuration	Client Package — Select the client package from the drop-down list for deployment.
SVM Manager	<ul style="list-style-type: none">• Available SVM Manager — Specifies the SVM Manager that is deployed on your hypervisor.• SVM Assignment Rules — Specifies the tag and IP-based rules, if the selected client systems are part of the assignment rules.
Proceed	Initiates the client deployment.

Option	Definition
Cancel	Cancels the client deployment.

SVM Configuration (Configuration tab)

You must configure an SVM OVF template in **Trellix ePO - On-prem**, so that it is used for SVM autoscaling. You can view and delete the SVM OVF template using **Trellix ePO - On-prem**.

Option	Definition
SVM OVF Name	Specifies the name of the Trellix MOVE AntiVirus SVM OVF template checked in to the Trellix ePO - On-prem server.
SVM OVF Version	Specifies the version of the Trellix MOVE AntiVirus SVM OVF package checked in to Trellix ePO - On-prem .
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 when it is not deployed to any hypervisor. It is possible to delete the SVM only when the SVM Use Count is zero.
Actions	Add SVM — Select to open the Configure SVM OVF page.

Configure SVM OVF page

Using this page, you can export an SVM OVF template to make a master image of an SVM, from which you can deploy many SVMs. You can also specify the location of the SVM OVF template that you exported using export utility tool, so that **Trellix MOVE AntiVirus** can deploy SVMs, as needed.

Option	Definition
Configure SVM OVF template	<ul style="list-style-type: none"> • Export an existing SVM or create and export from a VM — Allows you to export an SVM OVF template from an existing SVM or a VM. <ul style="list-style-type: none"> ▫ 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, 4.6.0. ▫ SVM OVF Name — Type a name for the SVM OVF template, for example, ESVM 4.6.0. ▫ Description — (Optional) Type details about the SVM OVF template, to help identify the SVM OVF template. • Specify the SVM OVF location available in the McAfee ePO system — Allows you to specify the location of the SVM OVF template that you exported using export utility tool. <ul style="list-style-type: none"> ▫ 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, 4.6.0. ▫ SVM OVF Name — Type a name for the SVM OVF template, for example, ESVM 4.6.0. ▫ Description — (Optional) Type details about the SVM OVF template, to help identify the SVM OVF template.

Option	Definition
Proceed	Click to export and check in an SVM OVF template to the Trellix ePO - On-prem server.
Cancel	Click to cancel the SVM export.

Autoscale SVM Details page (Configuration tab)

Use this page to view the details of the SVMs, which are deployed using the autoscale feature. You can view the deployed SVM and the infrastructure group details.

Option	Definition
Preset	<p>Allows you to select an option to filter and display the deployed SVM modes:</p> <ul style="list-style-type: none">• All — Filters and displays all the SVMs deployed using the autoscale deployment.• Standby — Filters and displays all the standby SVMs.• Ready — Filters and displays all the ready SVMs.• Running — Filters and displays all the running SVMs.
Hostname	Specifies the 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 a number of 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	Definition
	<ul style="list-style-type: none"> • All — Filters and displays all the SVMs deployed using the autoscale deployment. • 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 will be 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 powered on, but not protecting the client systems. • Running — These SVMs are currently protecting the client systems.
SVM Status	Specifies whether the SVMs are running.
Action	Edit — Click to edit the configuration details of a host.
Actions	<ul style="list-style-type: none"> • Delete SVMs — Select to delete the selected SVM. • Update Standby SVMs — Select to upgrade the selected SVM.

Selection page (Service setup)

Allows you to select the hypervisor where the **MOVE** service and prerequisites have to be installed.

Option	Definition
Hypervisors	Lists the hypervisors present under the registered VMware vCenter account.
vCenter Account	Specifies the name of the VMware vCenter account that is registered with Trellix ePO - On-prem .

Option	Definition
Deployment Type	Displays the SVM deployment status as Install or Upgrade .
Next	Navigates to the next page.
Cancel	Cancels the current page.

Configuration page (Service setup)

Allows you to configure SVM Hostname, SVM Version, Datastore, Provision Type, Management Network, and IP Configuration. All these parameters are retrieved automatically and they can be edited later.

Option	Definition
Hypervisor	Lists the hypervisors present under the registered VMware vCenter account.
SVM Version	Version of the SVM package checked in to Trellix ePO - On-prem .
SVM Hostname	Specifies the hostname of the SVM.
Datastore (Free Space)	Specifies the free space present in the datastore, where the SVM service virtual machines storage is added.
Provision Type	Specifies the provision type as Thick or Thin .
Management Network	Displays the management network specified in the SVM.
IP Configuration	Specifies the DHCP IP or Static IP Pool to be used.
Action	Click Edit to change the configurations of a single hypervisor.

Option	Definition
Actions	Group Edit — You can select multiple hypervisors and click Actions → Group Edit to change the hypervisor settings, so that the changed values are applicable to all selected hypervisors.
Back	Navigates to the previous page.
Next	Saves the hypervisor details and then navigates to the next page.
Cancel	Cancels the current page.

Verification page (Service setup)

You can verify the various parameters of the services that are installed during the deployment. This step also validates the prerequisites for the SVM deployment.

Option	Definition
Hypervisor	Lists the hypervisors present under the registered VMware vCenter account.
vCenter Account	Specifies the vCenter account of the hypervisor.
vShield Manager	Specifies the vShield Manager account.
SVM Version	Version of the SVM package checked in to Trellix ePO - On-prem .
SVM Hostname	Specifies the hostname of the SVM.
Datastore (Free Space)	Specifies the free space present in the datastore, where the SVM service virtual machines storage is added.
Provision Type	Specifies the provision type as Thick or Thin .

Option	Definition
Management Network	Displays the management network specified in the SVM.
IP Configuration	Displays the IP configuration allotted for the virtual appliance.
Verification Status	Displays the verification status of these components: <ul style="list-style-type: none">• SVM configurations• Host details• The compatibility status of components such as VMware vCenter, vShield Manager, host, VMTools, and Endpoint version• The available datastore space
Back	Navigates to the previous page.
Deploy	Deploys the SVM to the selected hypervisor.
Cancel	Cancels the current page.

Selection page (Service remove)

Using the **Trellix ePO - On-prem** console, remove the SVM from one or more hypervisors.

Option	Definition
Hypervisors	Lists the hypervisors present under the registered VMware vCenter account, where the SVM is already deployed.
vCenter Account	Specifies the name of the VMware vCenter account that is registered with Trellix ePO - On-prem .
SVM Version	Specifies the version of the SVM.
Next	Navigates to the next page.

Option	Definition
Cancel	Navigates to the previous page.

Verification page (Service remove)

You can review the verification details after selecting the required hypervisors from which you must remove the SVM.

Option	Definition
Hypervisors	Lists the hypervisors present under the registered VMware vCenter account.
vCenter Account	Specifies the name of the VMware vCenter account that is registered with Trellix ePO - On-prem .
SVM Version	Specifies the version of the SVM.
SVM VM Name	Displays the name of the SVM host.
Validation Status	Displays the validation status that specifies whether the SVM can be removed.
Back	Navigates to the previous page.
Remove	Removes the SVM from the selected hypervisor.
Cancel	Cancels the current page.

Job Status page (Service setup)

After initiating the SVM deployment or upgrade, you can view the deployment status and its details on the **Trellix ePO - On-prem** server.

Item	Description
Hypervisors	Specifies the name of the hypervisor.

Item	Description
vCenter Name	Specifies the name of VMware vCenter account that is registered with Trellix ePO - On-prem .
Deployment Type	Displays whether the SVM deployment type is Deploy , Upgrade , or Remove .
Status	Specifies the deployment status such as Started , Completed , Failed , Completed with error , and Fatal error .
Start Time	Indicates the date and time when the SVM deployment started.
End Time	Indicates the date and time when the SVM deployment ended.

Deployment and task status details page

After initiating a deployment, you can view the deployment job status and task status details on the **Trellix ePO - On-prem** server.

Job status

Item	Description
Start Time	Indicates the date and time when the SVM deployment started.
End Time	Indicates the date and time when the SVM deployment ended.
Deployment Type	Displays the deployment type: Agentless (For SVM) Deploy , Upgrade , and Remove . Multi-Platform (For SVM Manager) SVM Manager , Upgrade SVM Manager , and Remove SVM Manager .

Item	Description
	(For SVM) Configure and export an SVM OVF template
Status	Specifies the deployment status such as Started , Completed , Failed , Completed with error , and Fatal error .
vCenter Name / IP address	Specifies the name of VMware vCenter account that is registered with Trellix ePO - On-prem .
Hypervisors / Hostname	<p>Agentless: Specifies the name of the hypervisor.</p> <p>Multi-Platform:</p> <ul style="list-style-type: none"> • (For SVM Manager) Specifies the name of the hypervisor. • (For SVM) Specifies the host name of the SVM. • (For client) Specifies the host name of the client.

Task status for Hypervisor

Item	Description
Node Type	<p>Agentless: Specifies whether the node is an SVM or a hypervisor.</p> <p>Multi-Platform:</p> <ul style="list-style-type: none"> • (For SVM Manager) Specifies whether the node is an SVM Manager or a hypervisor, SVM, or a VM. • (For SVM) Specifies whether the node is an SVM or endpoint. • (For client) Specifies the node type as Endpoint.
Task Type	Specifies the set of internal tasks that happen in a deployment or an upgrade job. The task list for a single job is displayed in sequence with Start Time , End Time , and Failure Reasons , if applicable.

Item	Description
	For the list of tasks and details, see <i>Task status details</i> .
Node Name	Agentless: Displays the SVM VM name, or Hypervisor name. Multi-Platform: <ul style="list-style-type: none"> • (For SVM Manager) Displays the SVM Manager name, or hypervisor name, SVM, or the guest VM name. • (For SVM) Displays the name of the VM. • (For client) Displays the host name of the client system.
Status	Specifies the task status such as Started , Completed , Skipped , Failed , and In Progress .
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 status for Guest

Item	Description
Node Type	Agentless: Specifies the node as VM. Multi-Platform: <ul style="list-style-type: none"> • (For SVM) Specifies whether the node is an SVM or endpoint. • (For client) Specifies the node type as Endpoint.
Task Type	Specifies the set of internal tasks that happen in a deployment or an upgrade job. The task list for a single job is displayed in sequence with Start Time , End Time , and Failure Reasons , if applicable.

Item	Description
	For the list of tasks and details, see <i>Task status details</i> .
Node Name	Displays the VM name.
Status	Specifies the task status such as Started , Completed , Skipped , Failed , and In Progress .
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.

Option	Description
Back	Navigates to the previous page.
Close	Closes the current page.

Options page (Trellix MOVE AntiVirus Common)


Allows you to configure the settings to defend files, services, and registry keys on virtual machines and to log events and alerts.


Option	Definition
Self-Protection	<ul style="list-style-type: none">• Enable Self-Protection — Select to prevent Trellix MOVE AntiVirus services and files from being stopped or modified.• Enable Self-Protection for MOVE CLI — Select to protect the command line utility from being accessed by unauthorized users.<ul style="list-style-type: none">▫ Password — Type a password.▫ Confirm Password — Retype the password.


Option	Definition
Events	<p>Allows you to set where to display threat events. Available options are:</p> <ul style="list-style-type: none"> • Log events to Windows Application log — Select to display alerts in the local system's Windows Event Log. • Send events to McAfee ePO — Select to display alerts in the Trellix ePO - On-prem Threat Event Log
Logging	<p>Rotate log file content when the file size reaches ___ MB — Enter the maximum size the Rotate Server log files can reach. Default size is 10 MB.</p>


On-access Scan page (Trellix MOVE AntiVirus)


The Trellix MOVE AntiVirus on-access scan tab contains settings for what files should be scanned and when.

Option	Definition
On-access scan	<p>Enable on-access scan — Select to use on-access scanning.</p> <ul style="list-style-type: none"> • Scan — Available options (and their default states) are: <ul style="list-style-type: none"> ▫ When writing to disk ▫ When reading from disk ▫ On network drives ▫ Opened for backup (Multi-Platform only) <p>More than one option can be selected.</p> <div style="background-color: #e6f2ff; padding: 10px; margin: 10px 0;"> <p> Note: The Opened for backup setting can impact backup operation performance for Trellix MOVE AntiVirus clients.</p> </div> <p>Specify maximum time for each file scan ___ seconds — The amount of time to wait for a scan to complete, in seconds. Defaults to 45</p>

Option	Definition
	<p>seconds. This is the duration for which a Trellix MOVE AntiVirus Agent waits for scan response of a file from the SVM. Typically, file scans are fast. However, file scans might take longer time due to large file size, file type, or heavy load on the SVM. In case, the file scan takes longer than the scan timeout limit, the file access is allowed and a scan timeout event is generated.</p> <p>Cache scan results for files smaller than ____MB (Multi-Platform only) — Set the maximum file size (in MB) up to which scan results must be cached. Defaults to 40 MB. Files smaller than this threshold are copied completely to the SVM and scanned. If the file is found to be clean, its scan result is cached based on its SHA 1 checksum for faster future access. Files larger than this size threshold are transferred in chunks that are requested by the SVM and scanned.</p> <div data-bbox="769 1014 1360 1134">  Warning: Caching the scan results for large files might reduce the scan performance. </div> <p>Deferred Scan (Multi-Platform only) — The deferred scan feature optimizes file scanning for files where the previous scanning is timed out for reasons such as large file size, file structure, and file composition.</p> <ul style="list-style-type: none"> • Enable on-access deferred scan — Select to enable the deferred scan. Here are the file size ranges and scan time-out: <ul style="list-style-type: none"> ▫ > 40 MB and <=200 MB — 480 seconds ▫ > 200 MB and <=4096 MB — 900 seconds ▫ > 4096 MB and above — 1800 seconds
Actions	<p>Threat detection primary response — If you select Delete files automatically and quarantine or Delete files automatically, and if that fails Deny access to files. If the primary behavior is set to Deny access to files, no secondary action is available.</p>

Option	Definition
Threat Detection	<p>Notify users when a threat is detected on a on-access scan (Multi-Platform only) — Select to notify users when a threat is detected on a on-access scan.</p>
File types to scan	<p>Specifies what file extensions to scan.</p> <ul style="list-style-type: none"> • All files — Select to scan all files. • Default + Additional files (Multi-Platform only) — Select to scan the default file types or any additional file types. You can add, edit, and remove any additional file types, which are included for scanning. By default, this option is selected. <ul style="list-style-type: none"> ▫ Add — Opens the Add Extension dialog box. You can add the extension of the new file type for scanning. <div data-bbox="808 947 1360 1104">  Note: On successful addition, extension of the file type is listed under Additional Types tab. </div> <ul style="list-style-type: none"> ▫ Edit — Opens the Edit Extension dialog box for the selected extension of the file type to modify as needed. ▫ Remove — Removes the selected extension of the file type from the list. • Following only — Select to specify a list of file extensions to scan. You can add, edit, and remove file extensions that are included for scanning. If you click Following only, customize the list of extensions to scan by clicking Add, Edit, or Remove. Do not include the period when specifying extensions. Wildcards are not supported, and exact matches are required. For example, specifying DOC will not scan DOCX files.
Exclusions	<p>Specifies which folders are to be excluded from scanning.</p>


Option	Definition
	<ul style="list-style-type: none"> • Path Exclusions — Specifies a list of folders to exclude from scanning. By default, the Trellix common framework files are excluded. Click Add, Edit, Remove, Import, or Clear to modify the list. <div data-bbox="803 462 1360 651">  Note: Mapped network drives are not supported. If you want to exclude a network path, use the UNC path without the starting "\\\" characters. </div> <ul style="list-style-type: none"> ▫ Add — Opens the Add/Edit Exclusion Item dialog box. You can add new folders to exclude from scanning. ▫ Edit — Opens the Add/Edit Exclusion Item dialog box for the selected item to modify as needed. ▫ Remove — Removes the selected item from the list. ▫ Import — Opens the Import Exclusion Path dialog box. You can browse and import the file to add exclusion path. ▫ Clear — Clears the whole list of Path Exclusions. • Process Exclusions (Multi-Platform only) — Specifies a list of processes to exclude from scanning. By default, there are various processes already defined to be excluded. Click Add, Edit, or Remove to modify the list. <ul style="list-style-type: none"> ▫ Add — Opens Add Exclusion Process dialog box. You can add new process to exclude from scanning. ▫ Edit — Opens Edit Exclusion Process dialog box for the selected item to modify as needed. ▫ Remove — Removes the selected process exclusion from the list. • Publisher Exclusions (Multi-Platform only) — You can choose to Trust authenticated signed files (from Microsoft and Trellix), so that the scanning performance improves by optimized use of resources at the SVM by sending less files for scan from endpoints.


Option	Definition
	<ul style="list-style-type: none"> ▫ Cache validity for publisher-based trust on signed files ____ days — Specifies the cache validity for publisher based trust on signed files. Defaults to 30 days. ▫ Maximum wait time for publisher trust verification ____ seconds — Specifies the maximum wait time for publisher trust verification. Defaults to 2 seconds. ▫ Certificate revocation check - Select and configure the certificate revocation check. These are the available options: <ul style="list-style-type: none"> ▫ none — Trellix MOVE AntiVirus does not do certificate revocation check. ▫ for end Certificate locally — Trellix MOVE AntiVirus checks whether the end certificate of the file is valid or has it being revoked. This is checked from the Windows CRL (local cache) that is maintained by Windows locally. ▫ for full certificate chain locally — Trellix MOVE AntiVirus checks the complete chain of certificate for a particular digitally signed file against the Windows CRL (local cache) that is maintained by Windows locally. ▫ for end certificate locally as well as by getting CRL from the issuing CA — Trellix MOVE AntiVirus checks against the Windows CRL (local cache) that is maintained by Windows locally and also checks against the issuing CA's (certificate authority) CRL that is done over network. <div style="background-color: #e6f2ff; padding: 10px; margin: 10px 0;">  Note: CRL = certificate revocation list </div> <ul style="list-style-type: none"> ▫ Certificate validity period — Select and configure the certificate validity period. Available options are Valid forever, and Valid for lifetime of signing certificate.


Enabling **Trellix MOVE AntiVirus** network scanning capabilities, then accessing files across the network severely impacts the access time for network-based files. **Trellix** recommends scanning a file using a scanner closest to the file itself. If a file resides on a network share, rather than enabling **Trellix MOVE AntiVirus** network scanning, use the **Trellix** anti-virus product on the system where the file resides to scan the file. If the file resides on a NetApp Filer we recommend using VirusScan Enterprise for Storage to scan the file. With this approach you maintain good performance while still providing protection

On-demand Scan page (Trellix MOVE AntiVirus)

The **Trellix MOVE AntiVirus** on-demand scan page allows you to configure on-demand scan settings for your virtual environment.

Option	Definition
On-demand scan	<ul style="list-style-type: none"> • Enable on-access scan — Select to enable on-demand scanning. ▫ Specify maximum time for each file scan____seconds — Specify the maximum time (in seconds) for scanning each file. Defaults to 45 seconds. ▫ Run on-demand scan for every____days — Specify the interval time (in days) for on-demand scanning. Defaults to 7 days. ▫ On-demand scan will stop after____minutes — Specify the maximum time (in minutes) for on-demand scanning. Defaults to 150 minutes. ▫ Cache scan results for files smaller than____MB (Multi-Platform only) — Specify the files size (in MB) of the scan results to cache. Defaults to 40 MB. <div style="background-color: #e6f2ff; padding: 10px; margin: 10px 0;">  Warning: Caching the scan results for large files might reduce the scan performance. </div> <p>Deferred Scan (Multi-Platform only) — The deferred scan feature optimizes file scanning for files where the previous scanning is timed out for reasons such as large file size, file structure, and file composition.</p> <ul style="list-style-type: none"> • Enable on-demand deferred scan — Select to enable the deferred scan. Here are the file size ranges and scan time-out: <ul style="list-style-type: none"> ▫ > 40 MB and <=200 MB — 480 seconds ▫ > 200 MB and <=4096 MB — 900 seconds



Option	Definition
	<ul style="list-style-type: none"> ▫ > 4096 MB and above — 1800 seconds
Actions	<p>Threat detection first response — If you select Delete files automatically and quarantine or Delete files automatically, and if that fails Notify only. If the first behavior is set to Notify only, no secondary action is available.</p>
File types to scan	<p>Specifies what file extensions to be scanned.</p> <ul style="list-style-type: none"> • All files — Select to scan all files. • Default + Additional files (Multi-Platform only) — Select to scan the default file types or any additional file types. You can add, edit, and remove any additional file types, which are included for scanning. <ul style="list-style-type: none"> ▫ Add — Opens the Add Extension dialog box. You can add the extension of the new file type for scanning. <div data-bbox="812 1071 1360 1220">  Note: On successful addition, extension of the file type is listed under Additional Types tab. </div> ▫ Edit — Opens the Edit Extension dialog box for the selected extension of the file type to modify as needed. ▫ Remove — Removes the selected extension of the file type from the list. • Following only — Select to specify a list of file extensions to scan. You can add, edit, and remove file extensions that are included for scanning. <p>If you click Following only, customize the list of extensions to scan by clicking Add, Edit, or Remove. Do not include the period when specifying extensions. Wildcards are not supported, and exact matches are required. For example, specifying DOC will not scan DOCX files.</p>


Option	Definition
Exclusions	<p>Specifies which folders are to be excluded from scanning.</p> <ul style="list-style-type: none"> • Path Exclusions — Specifies a list of folders to exclude from scanning. By default, the Trellix common framework files are excluded. Click Add, Edit, Remove, Import, or Clear to modify the list. <div style="background-color: #e6f2ff; padding: 10px; margin: 10px 0;">  Note: Mapped network drives are not supported. If you want to exclude a network path, use the UNC path without the starting '\\\' characters. </div> <ul style="list-style-type: none"> ▫ Add — Opens the Add/Edit Exclusion Item dialog box. You can add new folders to exclude from scanning. ▫ Edit — Opens the Add/Edit Exclusion Item dialog box for the selected item to modify as needed. ▫ Remove — Removes the selected item from the list. ▫ Import — Opens the Import Exclusion Path dialog box. You can browse and import the file to add exclusion path. ▫ Clear — Clears the whole list of Path Exclusions.

Options page (Trellix MOVE AntiVirus)

From the Trellix MOVE AntiVirus **Options** tab, you can configure the quarantine manager options that apply to both on-access scanner and on-demand scanner. Also, specifies the SVM assignment details for Multi-Platform.

Option	Definition
Quarantine Manager	<p>(Multi-Platform only)</p> <ul style="list-style-type: none"> • Quarantine Directory — Specify where quarantined items are stored by changing the quarantine directory. Default is <SYSTEM_DRIVE>\Quarantine

Option	Definition
	<div data-bbox="787 283 1360 399">  Important: Mapped network drives and UNC network path names are not supported. </div> <ul style="list-style-type: none"> Specify the maximum number of days to keep quarantine data ____ days — Select this option to automatically delete quarantined data after a specified number of days. Defaults to 28 days. <div data-bbox="771 619 950 661">(Agentless only)</div> <ul style="list-style-type: none"> Quarantine network share — Quarantined files are stored on the specified network share. The share is mounted as CIFS, so the remote share must support this protocol. Read and write permissions are required. Trellix MOVE AntiVirus supports only windows share path for quarantine network share. Linux share path is not supported for quarantine network share. Enter the server name so that it can be resolved by the SVM. How this is entered depends on the environment and how the SVM is configured. Network domain and username — Type the domain and user name used to access the specified share. Network password — Type the network password. Confirm password — Retype the network password.
SVM Server Communication (Multi-Platform only)	<p>Scan server port — Specifies the port number of the scan server of the SVM. The default port is 9053.</p> <div data-bbox="787 1564 1360 1680">  Important: Modifying the port value will restart the SVM service. </div>
SVM Assignment (Multi-Platform only)	<p>Assign SVM using SVM Manager — Select to specify which SVM a group of virtual machines uses.</p>

Option	Definition
	<ul style="list-style-type: none"> • SVM Manager Address — Specify the address of the SVM Manager such as IP Address, host name, and FQDN. • Port — Type the port number. Default is 8080. <p>Assign SVM manually — Manually specify the SVM which a group of virtual machines should use.</p> <ul style="list-style-type: none"> • IP Address, host name, or FQDN of SVM-1 — Enter IP Address, host name, or FQDN of SVM-1, and the SVM 1 Port. Default is 9053. • IP Address, host name, or FQDN of SVM-2 — Enter IP Address, host name, or FQDN of SVM-2, and the SVM 2 Port. Default is 9053. <div>  Note: The specified port is used for client to communicate to the SVM. </div>

Shared Cloud Solutions page (MOVE AntiVirus)

Shared Cloud Solutions page allows you to configure settings for using **Threat Intelligence Exchange** and **Intelligent Sandbox** features.

Option	Definition
Enable TIE	<p>Enabled — Select to enable Threat Intelligence Exchange so that it provides context-aware adaptive security for your virtual environment.</p> <p>TIE determines file and certificate reputation when a Portable Executable (PE) file is accessed on a managed endpoint.</p> <p>PE file includes these formats: .cpl, .exe, .dll, .ocx, .sys, .scr, .drv, .efi, .fon</p>
TIE Non-PE Lookup	<p>Enabled — Select to enable Threat Intelligence Exchange to determine file and certificate reputation when a non-PE file is accessed on a managed endpoint.</p>

Option	Definition
Threat Intelligence Exchange (TIE)	<p>Select the reputation action from the drop-down list to scan by Threat Intelligence Exchange. Available options are:</p> <ul style="list-style-type: none"> • Known Malicious — This is a malicious file • Most Likely Malicious — Almost certainly a malicious file • Might be Malicious — Appears to be a suspicious file • Unknown — Cannot make a determination at this time • Might be trusted — Appears to be a benign file • Most likely trusted — Almost certainly a trusted file
Advanced Threat Defense (ATD)	<p>Allows you to define the settings for use of Intelligent Sandbox feature.</p> <ul style="list-style-type: none"> • Submit files to ATD at and below — Select the type of file to be scanned by Intelligent Sandbox from the drop-down list. Available options are: <ul style="list-style-type: none"> ▫ Most Likely Malicious — Almost certainly a malicious file ▫ Unknown — Cannot make a determination at this time ▫ Most Likely Trusted — Almost certainly a trusted file • Limit files size to ___MB — Specify the maximum size (in MB) of the file to send to Intelligent Sandbox. Defaults to 5 MB.

SVM Manager Settings page (MOVE AntiVirus)

Configure these SVM Manager settings that allow you to set the OSS assignment and threshold warning.

Option	Definition
SVM Manager Configuration	SVM Manager configuration allows you to assign your SVM to your client systems based on the

Option	Definition
	<p>configurations specified in the Trellix ePO - On-prem server.</p> <ul style="list-style-type: none"> • SVM Port — Specifies the port number of the SVM. The default port is 8443. • Client Port — Specifies the port number of client system. The default port is 8080.
SVM Autoscale Settings	<p>Enable auto scaling of SVMs — Enabling this option deletes all existing SVMs after the new SVMs are deployed and are ready to protect the client systems. It is also important to note that disabling the Enable auto scaling of SVMs option deletes all ready and standby SVMs, but the running SVMs continue to protect the client systems.</p> <ul style="list-style-type: none"> • Customize SVM Settings — You can define the SVMs settings that the maximum number of clients would connect to SVM for protection, the number of standby SVMs needed, and the SVM capacity threshold level. <ul style="list-style-type: none"> ▫ 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 would 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 back up SVM as 4, 2 standby SVMs will be deployed automatically. • Alarms — Defines the threshold level for number of connected endpoints for each SVM. <ul style="list-style-type: none"> ▫ Threshold for number of connected endpoints (per SVM) Min____% Max____% — Specify the SVM capacity threshold level. A warning appears when the number of connected endpoints is more than this level. Default value for minimum is 10 and maximum is 90.

Option	Definition
Assignment Rules	<p>Tag Assignment Rules — Displays the list of assigned rules that have been created using their tag group for a set of endpoints to a selected SVM.</p> <ul style="list-style-type: none"> • Rule Name — Specifies a unique user-friendly name that can help you to identify the rule. • Client Tags — Specifies the tag name of the endpoints, which have been assigned to the SVM. • SVM Tags — Specifies the tag name of the SVM, which has been assigned to the client. • Infrastructure Groups — Specifies the virtual infrastructure group, which has been created using the Menu → Automation → MOVE AntiVirus Deployment → Configuration → Infrastructure Details option. • Minimum Threshold (%) — Specifies the SVM's minimum capacity threshold level. • Add — Opens the Add/Edit SVM Tag Assignment Rule dialog box. You can configure these settings as needed. <ul style="list-style-type: none"> ▫ Rule name — Type a unique user-friendly name that can help you identify the rule. ▫ Select and add to client tags — Select the tag names of the endpoints, which must be assigned to the SVM. ▫ Select and add to SVM tags — Select the tag name of the SVM, which must be assigned to the client. ▫ Select and add to infrastructure groups — Select the Default Group or an infrastructure group you have created using the Menu → Automation → MOVE AntiVirus Deployment → Configuration → Infrastructure Details option, so that SVM deployment can be done to specific virtual group in your organization. ▫ Customize SVM Settings — This is the SVM assignment rule specific auto scale settings. Here, each rule can individual SVM deployment settings. You can define different rules which

Option	Definition
	<p>overwrite the common auto scale settings defined under SVM Autoscale Settings.</p> <ul style="list-style-type: none"> ▫ Number of backup SVMs — Type the number of standby SVMs needed. Default value is 2. ▫ Alarms — Defines the threshold level for number of connected endpoints for each SVM. ▫ Threshold for number of connected endpoints (per SVM) Min____% Max____% — Specify the SVM capacity threshold level. A warning appears when the number of connected endpoints is more than this level. Default value for minimum is 10 and maximum is 90. • Edit — Opens the Add/Edit SVM Tag Assignment Rule dialog box for the selected SVM assignment rule to modify the settings as needed. • Remove — Removes the selected SVM assignment rule from the list. • Move Up — Moves the selected SVM assignment rule up. • Move Down — Moves the selected SVM assignment rule down. <p>IP Assignment Rules — Displays the list of assigned rules that have been created using their IP address range for a set of endpoints to a selected SVM.</p> <ul style="list-style-type: none"> • Rule Name — Specifies a unique user-friendly name that can help you to identify the rule. • Client IP Address Range — Specifies the IP address or a range of IP addresses of the endpoints, which have been assigned to the SVM. • SVM IP Address Range — Specifies the IP address or a range of the SVMs, which have been assigned to the client. • Infrastructure Groups — Specifies the virtual infrastructure group, which has been created using the Menu → Automation → MOVE AntiVirus Deployment → Configuration → Infrastructure Details option.



Option	Definition
	<ul style="list-style-type: none"> • Minimum Threshold (%) — Specifies the SVM's minimum capacity threshold level. • Add — Opens the Add/Edit SVM IP Assignment Rule dialog box. You can configure these settings as needed. <ul style="list-style-type: none"> ▫ 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, which must be assigned to the SVM. ▫ SVM IP Addresses — Select the IP address or a range of the SVMs, which must be assigned to the client. ▫ Select and add to infrastructure groups — Select the Default Group or an infrastructure group you have created using the Menu → Automation → MOVE AntiVirus Deployment → Configuration → Infrastructure Details option, so that SVM deployment can be done to specific virtual group in your organization. ▫ Customize SVM Settings — This is the SVM assignment rule specific auto scale settings. Here, each rule can individual SVM deployment settings. You can define different rules which overwrite the common auto scale settings defined under SVM Autoscale Settings. ▫ Number of backup SVMs — Type the number of standby SVMs needed. Default value is 2. ▫ Alarms — You can define the threshold level for number of connected endpoints for each SVM. <ul style="list-style-type: none"> ▫ Threshold for number of connected endpoints (per SVM) Min____% Max____% — Specify the SVM capacity threshold level. A warning appears when the number of connected endpoints is more than this level. Default value for minimum is 10 and maximum is 90. • Edit — Opens the Add/Edit SVM Assignment Rule dialog box for the selected SVM Assignment Rule to modify the settings as needed.

Option	Definition
	<ul style="list-style-type: none"> • Remove — Removes the selected SVM assignment rule from the list. • Move Up — Moves the selected SVM assignment rule up. • Move Down — Moves the selected SVM assignment rule down. <p>Assign SVM if no rule is defined for the above client — Assigns the SVM to endpoints, if no rules are created for these endpoints. By default, this option is enabled.</p> <p>Enable to get SVM preference from the same subnet — Select your SVM Manager to assign the OSS from the same subnet.</p> <ul style="list-style-type: none"> • Default lease time___minutes — Specifies the lease validity for the OSS assigned to endpoints. The default interval is 240 minutes. The load balancing depends on this value. • Threshold for SVM Capacity Warning___% — Specify the OSS capacity threshold level. A warning appears when the number of connected endpoints is more than this level. The default level is 90%.


SVM Settings page (MOVE AntiVirus)

SVM Settings page allows you to configure SVM, enable Trellix GTI , and on-demand scan (ODS) scheduler.

Option	Definition
SVM Settings	<p>Concurrent on-demand scans — Allows you to define on-demand scan settings per SVM.</p> <ul style="list-style-type: none"> • Restrict number of on-demand scans to___per SVM — Limits the number of concurrent scans to be run on the SVM. Default value is 2. • Restrict number of targeted on-demand scans to___per SVM — Limits the number of targeted scans to be run on the SVM. Default value is 1.


Option	Definition
	<div data-bbox="805 289 1360 399">  Important: A high value reduces the scanning performance. </div> <p data-bbox="768 457 1008 489">(Multi-Platform only)</p> <ul data-bbox="760 510 1349 1066" style="list-style-type: none"> • Client load — Select the load type, which specifies the workload and activities on clients. Available options are: <ul data-bbox="776 636 1312 1066" style="list-style-type: none"> ▫ Low (Higher number of clients) — Lower file activity on the clients. SVM can handle more clients. Default number of clients is 300. ▫ Medium (Moderate number of clients) — Medium file activity on the clients. Default number of clients is 250. ▫ High (Fewer number of clients) — Higher file activity on the clients. SVM can handle fewer clients. Default number of clients is 150. ▫ Custom — You can customize workload and activities for your clients. <div data-bbox="805 1104 1360 1255">  Note: We recommend 250 because increasing this value might cause performance issues or scan delays or both. </div> <ul data-bbox="760 1276 1349 1791" style="list-style-type: none"> • Alert me — Allows you to set the alerts on number of client connections and scan time. <ul data-bbox="776 1360 1349 1791" style="list-style-type: none"> ▫ When number of client connections to the SVM reaches___% — Specify the SVM capacity level (in percentage) for number of client connections. A warning appears when the number of connected clients is more than this level. Default value is 90. ▫ When average scan time on the SVM exceeds___seconds — Specify the SVM's average scan time (in seconds). A warning appears when the average scan time on the SVM exceeds this level. Default value is 10 seconds.

Option	Definition
Trellix GTI	<p>Enable Trellix GTI — Select to enable Trellix GTI scan feature.</p> <ul style="list-style-type: none"> • Sensitivity level — Select the sensitivity level of the Trellix GTI scan from the drop-down list. Available options are: <ul style="list-style-type: none"> ▫ Very Low — Trellix GTI scans in low level. ▫ Low — Trellix GTI scans in low level. ▫ Medium — Trellix GTI scans in medium level. ▫ High — Trellix GTI scans in high level. ▫ Very High — Trellix GTI scans in high level. • GTI timeout — Enter a value ranging from 10 to 50 seconds.
Scanning Options	<ul style="list-style-type: none"> • Enable scanning inside archive files — Select to enable scanning inside archived files. • Enable scanning for MIME-encoded files — Select to enable scanning for MIME-encoded files. • Enable scanning for potentially unwanted programs — Select to enable scanning for potentially unwanted programs.
ODS Scheduler	Allows you to set on-demand scanning time on day-to-day and time-to-time basis.
Performance	<ul style="list-style-type: none"> • Limit the number of items that can exist in the server cache to ____ — Enter the appropriate amount to limit the number of items that can exist in the server cache. Default value is 1000000. <p>(Agentless only)</p> <ul style="list-style-type: none"> • Cache scan result of file size up to ____MB — Set the maximum file size (in MB) up to which scan results must be cached. Defaults to 40 MB. Files smaller than this threshold are copied completely to the Offload Scan Server and scanned. If the file is found to be clean, its scan result is cached based on its SHA-1 checksum for faster future access.

Option	Definition
	Files larger than this size threshold are transferred in chunks that are requested by the offload scan server and scanned.
SVM Configuration	<p>(Multi-Platform only)</p> <ul style="list-style-type: none"> • SVM Manager port — Specify the port number of SVM Manager system. The default port is 8443.
	<p>(Agentless only)</p> <ul style="list-style-type: none"> • Hypervisor/vCenter server — Type the valid IP address of the hypervisor or vCenter server. • Protocol — Select protocol type as http or https. • vCenter/ESXi Port — Specify the port number of the SVM. The default port is 443. • Username — Type the vCenter user name. • Password — Type the vCenter password. <div data-bbox="789 993 1360 1224"> <p> Important: After you save and reopen an SVM policy, the vCenter password will appear blank. Even though it appears blank, it is saved in the policy settings. The password must be entered again to test connection settings.</p> </div> <ul style="list-style-type: none"> • Confirm password — Retype the vCenter password. • SVM time zone — Set the MOVE SVM time zone as required. We recommend that you set the MOVE SVM time zone, date, and time to match with your Trellix ePO - On-prem server. This is important for the on-demand scan to start at the exact time you have specified. • NTP Server(s) — Select Use default servers to use default NTP servers and select Use following servers to specify your own NTP servers. • Test connection settings — Click to test the connection to the hypervisor or vCenter server.

Schedule page (Targeted on-demand scan)

Use this page to specify the schedule for targeted on-demand scan.

Option	Definition
Schedule status	Specifies whether the task runs according to its schedule. If the schedule is disabled, the task can only be run from the Systems → System Tree page by clicking Actions → Targeted ODS [MOVE] .
Schedule type	<p>Specifies the interval for running the targeted on-demand scan task. Options include:</p> <ul style="list-style-type: none"> • Daily — Specifies that the task runs every day, at a specific time, on a recurring basis between two times of the day, or a combination of both. • Weekly — Specifies that the task runs on a weekly basis. Such a task can be scheduled to run on a specific weekday, all weekdays, weekends, or a combination of them. You can schedule such a task to run at a specific time of the selected days, or on a recurring basis between two times of the selected days. • Monthly — Specifies that the task runs on a monthly basis. Such a task can be scheduled to run on one or more specific days of each month at a specific time. • Once — Starts the task on the time and date you specify. • At System Startup — Starts the task the next time you start the server. • At logon — Starts the task the next time you log on to the server. • When idle — Starts the task the next time the client goes idle. Once initiated, the task continues to run until it's complete, even if the system does not stay idle. <div style="background-color: #e6f2ff; padding: 10px; margin-top: 10px;">  Note: After the task is run for the first time, it does not run again. </div> <ul style="list-style-type: none"> • Run immediately — Starts the task immediately.

Option	Definition
	<ul style="list-style-type: none"> • Run on dialup — Starts the task the next time that the managed system establishes a dialup connection to the network.
Effective period	<p>Specify the following:</p> <ul style="list-style-type: none"> • End date — The date on which the task becomes unavailable to the scheduled interval. • Start date — The date on which the task is available to begin running at the scheduled intervals.
Start time	<p>Specify the time at which this task need to begin, and:</p> <ul style="list-style-type: none"> • Whether to run the task only once at the Start time, or to continue running until a later time. You can also specify the interval at which the task runs during this interval.
Task runs according to	<p>Specifies whether the task schedule runs according to the Local time on managed system or Coordinated Universal Time (UTC).</p>
Options	<p>Specifies how the task behaves and the actions that can be taken if the task runs too long, or whether the task should run if it was missed. Options include:</p> <ul style="list-style-type: none"> • Enable randomization X hours Y minutes — Specifies that this task runs randomly within the time you specify. Otherwise, this task starts at the scheduled time regardless if other client tasks are scheduled to run at the same time. • Run missed task X minute delay — Runs the task after a user-configured number of minutes once the managed system is restarted. • Stop the task if it runs for X hours Y minutes — Stops the task when it has run for a user-configured amount of time.

Option	Definition
Next	Navigates to the Summary page.
Save	Saves and runs the targeted on-demand scan for the selected VMs.
Cancel	Navigates to the current page.

Summary page (Targeted on-demand scan)

Review the details of the task assignment before saving it.

Option	Definition
Name	Displays the name you provided for the task assignment.
Description	Displays any description you provided for the task assignment.
Type	Displays the type of task chosen for this assignment.
Schedule	Displays the schedule information provided for this task assignment.
Lock task inheritance	Displays whether task inheritance was locked for this task assignment.
Back	Navigates to the previous page.
Save	Saves the assignment.
Cancel	Navigates to the current page.

COPYRIGHT

Copyright © 2023 Musarubra US LLC.

Trellix, FireEye and Skyhigh Security are the trademarks or registered trademarks of Musarubra US LLC, FireEye Security Holdings US LLC and their affiliates in the US and /or other countries. McAfee is the trademark or registered trademark of McAfee LLC or its subsidiaries in the US and /or other countries. Other names and brands are the property of these companies or may be claimed as the property of others.

