Product Guide

McAfee MOVE AntiVirus (Agentless) 3.6.0

For use with McAfee ePolicy Orchestrator

COPYRIGHT

TRADEMARK ATTRIBUTIONS

LICENSE INFORMATION

License Agreement

Contents

Preface

This guide provides the information you need to configure, use, and maintain your McAfee product.

Contents

About this document

Thank you for choosing this McAfee product. This document contains important information about the current release. We strongly recommend that you read the entire document.

Conventions

This guide uses these typographical conventions and icons.

Book title, *term*, *emphasis*	Title of a book, chapter, or topic; a new term; emphasis.
Bold	Text that is strongly emphasized.
`User input, code, message`	Commands and other text that the user types; a code sample; a displayed message.
Interface text	Words from the product interface like options, menus, buttons, and dialog boxes.
Hypertext blue	A link to a topic or to an external website.
	**Note:** Additional information, like an alternate method of accessing an option.
	**Tip:** Suggestions and recommendations.
	**Important/Caution:** Valuable advice to protect your computer system, software installation, network, business, or data.
	**Warning:** Critical advice to prevent bodily harm when using a hardware product.

Find product documentation

After a product is released, information about the product is entered into the McAfee online Knowledge Center.

Task

1. Go to the **Knowledge Center** tab of the McAfee ServicePortal at http://support.mcafee.com.
2. In the **Knowledge Base** pane, click a content source:
   - **Product Documentation** to find user documentation
   - **Technical Articles** to find KnowledgeBase articles
3. Select **Do not clear my filters**.
4. Enter a product, select a version, then click **Search** to display a list of documents.

1 Introduction

McAfee Management for Optimized Virtual Environments AntiVirus (McAfee® MOVE AntiVirus) is an anti-virus solution for virtual environments. It removes the need to install an anti-virus application on every virtual machine (VM), yet provides the protection and performance needed for your organization requirements.

Traditional security solutions for virtual machines need anti-virus applications running on every virtual machine (VM) on a hypervisor, contributing to high disk CPU and memory usage. This reduces VM density on each hypervisor.

McAfee MOVE AV solves this issue by offloading all on-access scanning to a dedicated VM that runs McAfee® VirusScan® Enterprise. As a result, traditional anti-virus applications are not required on each guest VM, improving performance and increasing VM density per hypervisor.

McAfee MOVE AV brings advanced malware protection to your virtualized environments, and integrates real-time threat intelligence with security management across your physical and virtual infrastructure.

McAfee MOVE AV provides two deployment options: Agentless and Multi-Platform. Both deployment options provide consistent protection, and are managed and reported by McAfee® ePolicy Orchestrator® (McAfee ePO™) .

Agentless

This solution integrates with VMware vShield using VMware vShield Endpoint. It addresses the challenges of protecting your virtual environment and keeping it free of malware without a McAfee® Agent, resulting in easy deployment and setup.

The Agentless deployment option:

- Uses the VMware vShield Endpoint API to receive scan requests from VMs on the hypervisor.
- Relies on McAfee® VirusScan® Enterprise for Linux for SVA protection and updates.
- Uses McAfee ePO to manage the MOVE configuration on the SVA.
- Leverages the McAfee Agent for policy and event handling.
- Uses McAfee ePO for reports on viruses that are discovered on the VMs.

This document covers installation, configuration, and product usage information for McAfee MOVE AV (Agentless) .

Multi-Platform

This solution removes the need to install an anti-virus 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 offload scan server — that runs McAfee VirusScan Enterprise software. Guest VMs are no longer required to run anti-virus software locally, which improves performance for anti-virus scanning, and increases VM density per hypervisor.

The Multi-Platform deployment option:

- Uses McAfee ePO to manage the MOVE configuration on the client systems, offload scan server, and SVA Manager (OSS Manager).
- Leverages the McAfee Agent for policy and event handling.
- Uses McAfee ePO for reports on viruses that are discovered on the VMs.

This option is described in the product documentation for McAfee MOVE AV (Multi-Platform).

Contents

About McAfee MOVE AV Agentless

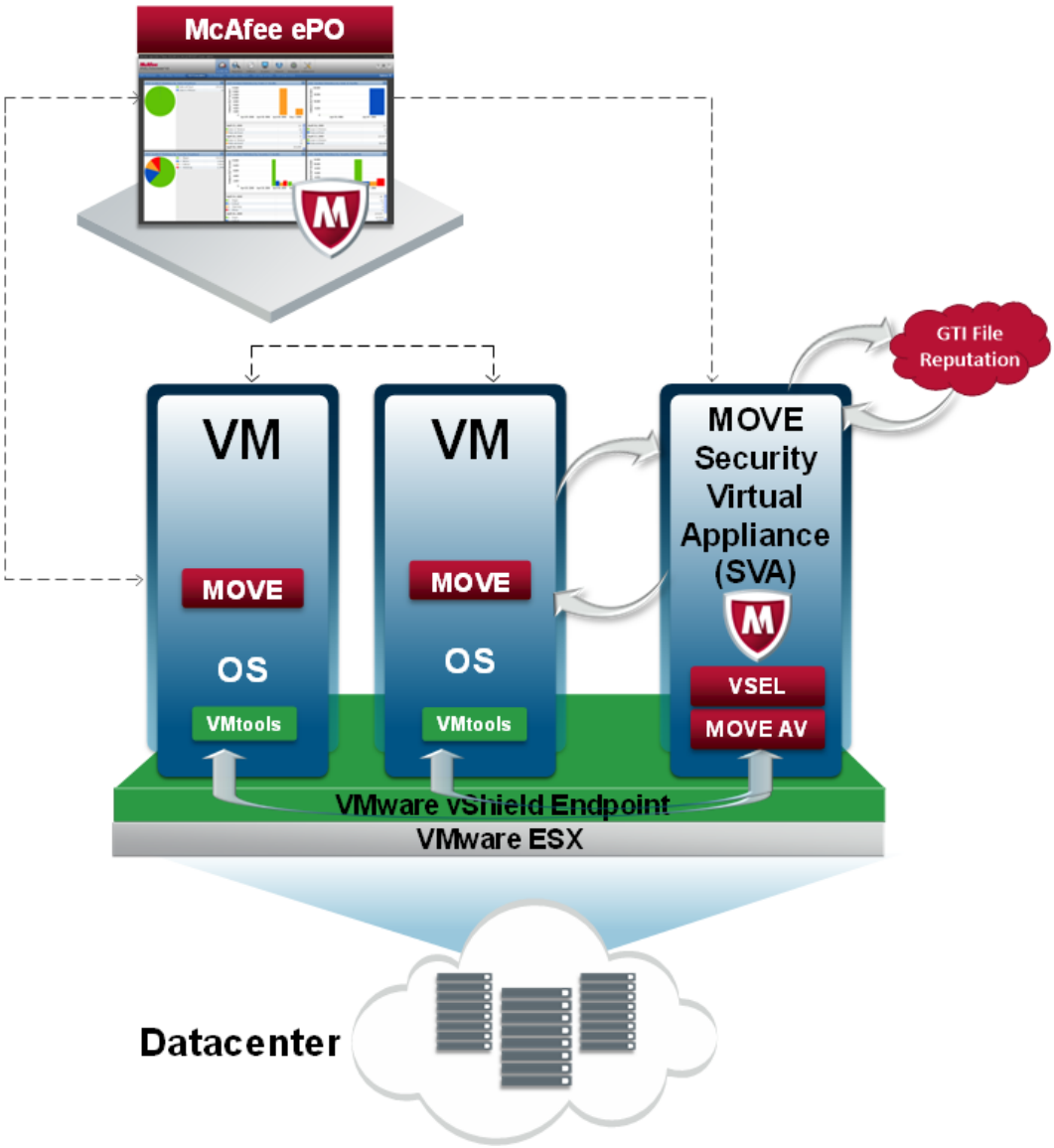
MOVE AV Agentless provides virus protection for virtual machines and contains a Security Virtual Appliance (SVA) delivered as an Open Virtualization Format (OVF) package.

The Agentless solution:

- Uses the VMware vShield Endpoint API to receive scan requests from VMs on the hypervisor
- Relies on McAfee® VirusScan® Enterprise for Linux for SVA protection and updates
- Uses McAfee® ePolicy Orchestrator® (McAfee ePO™) to manage the SVA
- Leverages the McAfee Agent for policy and event handling
- Uses McAfee ePO to provide reports on viruses that are discovered on the VMs

Components and what they do

Each component performs specific functions to keep your environment protected.



ePolicy Orchestrator — Allows you to configure policies to manage McAfee MOVE AV Agentless and provides reports on malware discovered within your virtual environment.

Security Virtual Appliance (SVA) — Provides anti-virus protection for VMs and communicates with the loadable kernel module on the hypervisor, ePolicy Orchestrator, and the GTI servers. The SVA is the only system directly managed by ePolicy Orchestrator. VirusScan Enterprise for Linux, McAfee Agent, and McAfee MOVE AV Agentless comes pre-installed.

File Quarantine — Remote quarantine system, where quarantined files are stored on an administrator-specified network share.

GTI (Global Threat Intelligence) — Classifies suspicious files that are found on the file system. When the real-time malware defense detects a suspicious program, it sends a DNS request for analysis to a central database server hosted by McAfee Labs.

VMware vCenter — Console that manages the ESXi servers, which host the guest VMs that require protection.

Hypervisor (ESXi) — Allows multiple operating systems to run concurrently on a hosted system. The hypervisor is a virtual operating platform that manages the execution of the guest operating systems. ESXi is an embedded hypervisor for servers that runs directly on server hardware without requiring an additional underlying operating system.

vCloud Networking and Security Manager — Manages the vShield components for the SVA and VMware vShield Endpoint, and monitors the health of the SVA.

VMware NSX Manager — Console that allows you to configure, provision, and automate the protection on the endpoints in a data center.

Virtual Machines (VMs) — Completely isolated guest operating system installations within a normal host operating system that support both virtual desktops and virtual servers.

Features

MOVE AntiVirus Agentless features are important for your organization's system security, protection, and performance.

Centralized management

MOVE AntiVirus integrates fully into McAfee ePO, leveraging its infrastructure for automated security reporting, monitoring, deployment, and policy administration.

Optimized scanning

MOVE AntiVirus provides higher operational benefits, and minimizes the performance impact on virtual servers with enhanced scan avoidance and scanning based on overall work load of the hypervisor.

Flexible deployment

MOVE AntiVirus offers the flexibility to choose your preferred deployment model:

- McAfee ePO-based deployment
- NSX Manager-based deployment
- Manual deployment

McAfee ePO-based deployment

Using the McAfee ePO console, you can deploy the SVA to one or more hypervisors, or an entire vCenter. This deployment provides virus protection for virtual machines on a hypervisor. Using this method, you can also upgrade an existing SVA.

NSX Manager-based deployment

You can register the SVA with VMware NSX Manager and deploy it automatically to one or more clusters. This deployment automatically provides virus protection for virtual machines on a new hypervisor from the moment the hypervisor is added to the cluster.

Greater Data Center visibility

McAfee Data Center Connector, which is also part of the Data Center Security suite, provides a complete view into virtual data centers and imports key properties like servers, hypervisors, and virtual machines through the McAfee ePO console.

You can register a cloud account for VMware vSphere, Amazon Web Services (AWS), or OpenStack with McAfee ePO to discover and gain visibility into all VMs, and protect them with MOVE AntiVirus. For details, see the product documentation for your version of Data Center Connector.

Endpoint Scan and Security reports

With the Data Center Connector for vSphere software, you can quickly retrieve the **Endpoint Scan Report** and **Endpoint Security Report** of all registered endpoints. For details, see *Data Center Connector for vSphere Product Guide*.

2 Installation and configuration

To set up your environment for MOVE AV Agentless, you install VMware vShield Endpoint, configure the Security Virtual Appliance (SVA), and install the product extensions.

VMware vShield Endpoint is installed on an ESXi host:

- As a loadable kernel module within the hypervisor
- As a filter driver within the guest VM

Contents

Requirements

Make sure that your environment includes these components, and that they meet these requirements.

SVA requirements

You must use the virtual machine we provide. This system is a dedicated virtual appliance with VirusScan Enterprise for Linux installed.

The Open Virtualization Format (OVF) is a secure image, so it doesn't require any additional hardening.

The SVA VM is built to meet these minimum hardware requirements:

CPU	2 vCPU, 1.6 GHz or higher
Memory	2 GB RAM or higher
Disk space	8 GB or higher

These items come pre-installed:

Operating system	Ubuntu 12.0.4
Software	VirusScan Enterprise for Linux 2.0
	McAfee Agent 4.8
	McAfee MOVE AV Agentless

We recommend that you set the SVA's time zone, date, and time to match your McAfee ePO server. Otherwise, the on-demand scan (ODS) does not start at the time that you have specified.

Software requirements for McAfee ePO-based deployment

- ePolicy Orchestrator 4.6.8, 5.1.0, 5.1.1, 5.3.0
- Security Virtual Appliance (SVA) 3.6.0
- VMware vSphere 5.1, 5.5, 6.0
- VMware vCloud Networking and Security Manager 5.1, 5.5

For details about system requirements and instructions for setting up the ePolicy Orchestrator environment, see the *McAfee ePolicy Orchestrator Installation Guide*.

New license implementation for McAfee ePO-based deployment

McAfee MOVE AV is offered in 2 different license modes: **Basic License (MOVE-AV-AL_BasicLicense_3.6.0.zip)** and **Advanced License (MOVE-AV-AL_AdvancedLicense_3.6.0.zip)**. You can download and install only one license extension.

- **Basic License** — Packaged with standalone MOVE AV (**MOVE AV for Virtual Desktops** and **MOVE AV for Virtual Servers**). You can't use the McAfee ePO-based SVA deployment feature with this extension. Trying to use this feature produces this error message.

  ```
  Your current product license is insufficient to access this feature. A Server or Virtual
  Desktop Suite license is required. Please visit http://www.mcafee.com/us/products/
  server-security-suite-essentials.aspx or contact your McAfee sales professional to find
  out more about our Data Center products, their features and minimum license needs.
  ```

- **Advanced License** — Packaged with **Server Security Suite Essentials**, **Server Security Suite Advanced**, and **Security Suite for Virtual Desktops**. This license allows you to use the McAfee ePO-based SVA deployment feature.

Product trial version — Allows you to use the McAfee ePO-based SVA deployment feature to manage an environment with 10 hypervisors or fewer. If you use this extension in an environment with more than 10 hypervisors, this error message appears.

```
You are using the product with a trial license that only allows you to manage an environment
with 10 hypervisors or fewer. Please contact your McAfee sales professional to purchase an
unrestricted license.
```

To use the McAfee ePO-based SVA deployment feature in your production environment, you must remove the Basic License extension and install the Advanced License extension.

Requirements for NSX Manager-based deployment

- ePolicy Orchestrator 4.6.8, 5.1.0, 5.1.1, 5.3.0
- Security Virtual Appliance (SVA) 3.6.0

- VMware vSphere 5.1, 5.5
- VMware NSX Manager 6.0.5 and later

For details about system requirements and instructions for setting up the ePolicy Orchestrator environment, see the *McAfee ePolicy Orchestrator Installation Guide*.

For details about system requirements and instructions for setting up the NSX Manager environment, see the product documentation for VMware NSX Manager.

Guest VM operating system minimum requirement

- VMware Tools 5.0 (Patch 1 ESX500-201109402-BG)

  We recommend that you install the latest version of the VMware Tools, so that the latest drivers are installed.

- For information about the Guest VM operating systems that are supported for VMware vShield Endpoint, see VMware's documentation: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1036847

Firewall settings

For successful installation of vsepflt, make sure that you enable the TCP Port (445) for the client systems where firewall is enabled. The TCP Port (445) is used to copy the vsepflt folder package to the client system during vsepflt installation. For client systems which have firewall enabled, by default the TCP Port is blocked. So, the task for enabling the vShield Driver fails.

Download the McAfee MOVE AV (Agentless) packages

Download these packages before they can be installed onto virtual systems or into ePolicy Orchestrator.

The OVF package and ePolicy Orchestrator extensions are required. The Help extension and documentation package are optional.

From the McAfee download site (http://www.mcafee.com/us/downloads/), download these product packages:

- McAfee MOVE AV (Agentless) OVF (`MOVE-AV-AL_OVF_3.6.0.zip`)
- McAfee MOVE AV (Agentless) extension for ePolicy Orchestrator:
  - Main product extension — `MOVE-AV-AL_EXT_3.6.0.zip`
  - License extensions — `MOVE-AV-AL_BasicLicense_3.6.0.zip` and `MOVE-AV-AL_AdvancedLicense_3.6.0.zip`

    You can download and install only one license extension.

  - McAfee MOVE AV (Agentless) Help Extension — `MOVE-AV-AL_HELP_EXT_3.6.0.zip`
- McAfee MOVE AV (Agentless) documentation package (`MOV-AV-AL_DOCS_3.6.0.zip`)

- McAfee MOVE AV (Agentless) restore tool (`MOVE-AV-AL_RestoreTool_3.6.0.zip`)
- McAfee MOVE AV (Agentless) multiple OVF deployment tool (`MOVE-AV-AL_SVA_Deployment_3.6.0.zip`)

  Download this package, if you are not using the NSX Manager-based deployment option.

Install the McAfee MOVE AV Agentless extension

A product's extension must be installed before ePolicy Orchestrator can manage the product.

Before you begin

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

Task

For option definitions, click **?** in the interface.

1 From the Software Manager or McAfee download site, download these files:

Extension	Name
Main product extension	`MOVE-AV-AL_EXT_3.6.0.zip`
License extension	`MOVE-AV-AL_BasicLicense_3.6.0.zip` or `MOVE-AV-AL_AdvancedLicense_3.6.0.zip` You can download and install only one license extension.

2 From the ePolicy Orchestrator console, click **Menu** | **Software** | **Extensions** | **Install Extension**.

3 Browse to and select the extension file, then click **OK**.

4 Verify that the product name appears in the **Extensions** list.

Install the VirusScan Enterprise for Linux extension

Install this extension only to manage the VirusScan Enterprise for Linux policy on the SVA. If you use the default settings, you don't need to perform this task.

VirusScan for Linux is only licensed for use on the SVA, and is not licensed for use on other Linux systems in your environment.

For instructions on how to install, configure, and create a product update task, see the *McAfee VirusScan Enterprise for Linux Configuration Guide*.

Task

For option definitions, click **?** in the interface.

1 From the ePolicy Orchestrator console, click **Menu** | **Software** | **Extensions** | **Install Extension**.

2 Browse to and select each extension file, then click **OK**.

Extension	File
McAfee Agent	**EPOAGENTMETA.ZIP**
McAfee VirusScan Enterprise for Linux	**LYNXSHLD2000.ZIP**
McAfee VirusScan Enterprise for Linux reports	**LYNXSHLD2000PARSER.ZIP**

3 Verify that the product name appears in the **Extensions** list.

Install VMware Endpoint

You must install vCloud Networking and Security Manager (vShield 5.1, 5.5) on your virtual environment before you can install and configure the software.

For instructions, see the *VMware vShield Endpoint Quick Start Guide* at http://www.vmware.com/pdf/vshield_50_quickstart.pdf.

Here is an overview of the tasks required to install VMware vShield Endpoint.

Task

1 Install ESXi.

2 Install and configure vCloud Networking and Security Manager.

3 Add component and vShield Endpoint licenses in vCenter.

4 Install vShield Endpoint on the hypervisors.

5 Deploy the SVA using the vCenter Client.

6 Install VMware Tools on the guest VM and select **Custom install of VMware tools**:

   a In the vSphere Client, right-click the appropriate VM, then select **Guest** | **Install/Upgrade VMware Tools**.

   b In the **Install/Upgrade Tools** dialog box, select **Interactive Tools Upgrade** and click **OK**.

   c Depending on your environment, select **setup.exe** or **setup64.exe** and run it as administrator.

   d Select **Custom**, then click **Next**.

   e Expand **VMware Device Drivers** | **VMCI Drivers**, then select **vShield Drivers** | **This feature will be installed on local hard drive**.

See also

Requirements on page 13

Setting up the SVA

You must deploy the OVF and configure the SVA before you can begin using the Agentless deployment option.

OVF deployment options

The provided OVF must be deployed to each hypervisor to protect the associated VMs.

There are three deployment options.

- **McAfee ePO-based deployment** - You can check in the SVA and deploy it using McAfee ePO to one or more clusters. You can select one or more hosts, a group of hosts or an entire vCenter to deploy and specify the schedule for deployment. This deployment method allows you to deploy the SVA with all prerequisites necessary for a successful deployment of SVA.
- **VMware NSX Manager-based deployment** — You can register the SVA with VMware NSX Manager and deploy it automatically to one or more clusters. You can select one or more Network and Security services to deploy and specify the schedule for deployment.
- **Multiple OVF deployment** — Using the provided Perl deployment script, you can deploy the OVF to multiple hypervisors. The provided CSV file must be filled out with the configuration information for each OVF before you can run the Perl deployment script.
- **Manual deployment** — You can manually deploy the SVA to each hypervisor from the vSphere Client. The vSphere Client must be connected to a vCenter server, and not directly to a hypervisor.

There are two configuration options.

- Automatic configuration
- Manual configuration

McAfee ePO-based deployment

Using McAfee ePO, you can check in, configure, and deploy the latest SVA to one or more hypervisors, or an entire vCenter. You can also upgrade an existing SVA.

New license implementation for McAfee ePO-based deployment

McAfee MOVE AV is offered in 2 different license modes: **Basic License (MOVE-AV-AL_BasicLicense_3.6.0.zip)** and **Advanced License (MOVE-AV-AL_AdvancedLicense_3.6.0.zip)**. You can download and install only one license extension.

- **Basic License** — Packaged with standalone MOVE AV (**MOVE AV for Virtual Desktops** and **MOVE AV for Virtual Servers**). You can't use the McAfee ePO-based SVA deployment feature with this extension. Trying to use this feature produces this error message.

  ```
  Your current product license is insufficient to access this feature. A Server or Virtual
  Desktop Suite license is required. Please visit http://www.mcafee.com/us/products/
  server-security-suite-essentials.aspx or contact your McAfee sales professional to find
  out more about our Data Center products, their features and minimum license needs.
  ```

- **Advanced License** — Packaged with **Server Security Suite Essentials**, **Server Security Suite Advanced**, and **Security Suite for Virtual Desktops**. This license allows you to use the McAfee ePO-based SVA deployment feature.

Product trial version — Allows you to use the McAfee ePO-based SVA deployment feature to manage an environment with 10 hypervisors or fewer. If you use this extension in an environment with more than 10 hypervisors, this error message appears.

```
You are using the product with a trial license that only allows you to manage an environment
with 10 hypervisors or fewer. Please contact your McAfee sales professional to purchase an
unrestricted license.
```

To use the McAfee ePO-based SVA deployment feature in your production environment, you must remove the Basic License extension and install the Advanced License extension.

Requirements for McAfee ePO-based deployment

Review these requirements before deploying the SVA using the ePolicy Orchestrator server. Make sure that:

- You have installed the latest extension for Data Center Connector for vSphere. For more information, see the product documentation for Data Center Connectors.

  If you install the McAfee MOVE AV (Agentless) extension before installing the Data Center Connector for vSphere extension and registering the vCenter account, the hypervisors do not appear under the McAfee MOVE AV (Agentless) page.

- You have registered a VMware vCenter account. For more information, see the product documentation for Data Center Connectors.
- The VMware vCenter account credentials specified in the **Registered Cloud Account** page of McAfee ePO for discovering the virtual instances must have these permissions.

Datastore.AllocateSpace	Host.Config.Settings
Global.Licenses	Network.Assign
Host.Config.AdvancedConfig	Sessions.ValidateSession
Host.Config.NetService	System.Anonymous
Host.Config.Network	System.Read
Host.Config.Patch	System.View
VirtualMachine.Interact.PowerOff	VirtualMachine.Interact.PowerOn
VirtualMachine.Inventory.Delete	VirtualMachine.Config.Rename
VApp.Import	VirtualMachine.GuestOperations.Execute
VirtualMachine.Config.AddNewDisk	VirtualMachine.GuestOperations.Modify
VirtualMachine.Config.AdvancedConfig	VirtualMachine.Interact.ToolsInstall

- You have installed the McAfee MOVE AV (Agentless) extension.
- You have installed and configured vShield manager.
- The McAfee ePO server and client systems are in domain. They should be able to communicate using their Fully Qualified Domain Name (FQDN).
- You have configured and registered all the LDAP servers, which are managing the client systems to be protected, on the McAfee ePO server. For successful installation of vsepflt, the domain user used to register the LDAP server must have the admin rights.

Set up a common configuration for SVA deployment

Before deploying the SVA, complete this common configuration on the McAfee ePO server, so that these settings are retrieved and used for every SVA deployment, which is done from the same McAfee ePO server.

Task

For option definitions, click **?** in the interface.

1 Log on to McAfee ePO as an administrator.

2 Click **Menu** | **Automation** | **MOVE AV Agentless**.

3 From the **Configuration** tab, click **General** and configure these details:

Table 2-1 McAfee ePO credentials

Options	Description
Password	Type the password of the McAfee ePO management console that the administrator has currently logged on.
Confirm Password	Retype the password of the McAfee ePO management console that the administrator has currently logged on.

Table 2-2 MOVE SVA configuration

Option	Description
Hostname Prefix	Type a unique prefix that is added to the host name of the SVA. The prefix can include characters a–z, A–Z, 0–9, and [-], without space.
Password	Type a password to be used as SVA password during deployment. • 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 of the available SVA.

4 Click **Save** to store these configurations, so that you can use them for every SVA deployment.

Configure the IP Pool details

An IP Pool is a range of IP addresses within the network. When you deploy the SVA, it is possible to configure the IP addresses of the SVA as Static or DHCP. Before configuring the IP address as Static, create an IP Pool. You can then select this IP Pool during the SVA deployment, so that any unused IP address of the IP Pool is automatically assigned to the SVA.

Before you begin

Make sure that you have installed the McAfee MOVE AV (Agentless) extension.

An IP pool's range cannot intersect one another, thus one IP address can belong to only one IP pool.

When using DHCP for the SVA, the IP Pool option is not applicable.

Task

For option definitions, click **?** in the interface.

1 Log on to McAfee ePO as an administrator.

2 Click **Menu** | **Automation** | **MOVE AV Agentless**.

3 From the **Configuration** tab, click **IP Pool** to open the **IP Pool: IP Pool Details** page with these SVA details and actions:

4 Click **Actions** | **Add IP Pool** to open the **Add IP Pool** page and configure these settings as needed:

Options	Description
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.
DNS Suffix	(Optional) Type the domain name of the DNS server.
Primary DNS	(Optional) Type the IP address of the Primary 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 2 IP addresses are used out of the available 3 IP addresses in the IP Pool.
Action	**Delete** — Use this option to delete the IP Pool when its IP addresses are not in use.

5 Click **Validate** to verify the IP Pool settings, then click **OK** to add the IP Pool. You can also use the **Delete** option under **Action** to remove an existing IP Pool.

Check in the SVA package to McAfee ePO

You must check in and host the SVA package in McAfee ePO, so that you can deploy it to the hypervisor. You can view and delete the SVA package using McAfee ePO.

Before you begin

Make sure that you have installed the McAfee MOVE AV (Agentless) 3.6.0 extension.

Make sure that you do not change the file name of the SVA package.

Task

For option definitions, click **?** in the interface.

1 Log on to McAfee ePO as an administrator.

2 Click **Menu** | **Automation** | **MOVE AV Agentless**.

3 From the **Configuration** tab, click **OVF Repository** to open the **MOVE SVA repository configuration** page with these SVA details and actions:

Options	Description
SVA Name	Name of the SVA package checked in to McAfee ePO.
SVA Version	Version of the SVA package checked in to McAfee ePO.
Action	• **Delete** — To remove an existing SVA when it is not deployed to any hypervisor.

4 Click **Actions** | **Add SVA** to open the **Check-in SVA (zip) file** page.

5 From **Select SVA (zip) file to check-in**, browse to and select the SVA package, then click **OK**. This action checks in the SVA package to McAfee ePO.

You can check in version 3.6 SVA package only.

Edit vShield Manager configuration

After configuring and registering the vShield Manager account with vCenter, you can edit the existing vShield Manager configuration using McAfee ePO.

Before you begin

You have configured and registered the vShield Manager account.

Using this configuration available on the ePolicy Orchestrator server, you are able to view the registration status of the vShield Manager and take the required action, as appropriate.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click **Menu** | **Automation** | **MOVE AV Agentless**.

3 From the **Configuration** tab, click **vShield Manager**. The **vShield Manager : Configuration** page appears with these details.

Option	Description
vCenter Account	Specifies the name of the registered vCenter account.
vShield Manager	Specifies the name of the registered vShield Manager.
Registration Status	Displays these registration statuses: • **Registered** — Indicates that the vShield Manager is registered and ready for deployment. • **Not Registered** — 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, however, the credentials are unknown. Therefore, click **Edit** and configure it before deployment.
Action	**Edit** — Click to edit and validate the existing vShield Manager configuration.

4 Click **Edit** under **Action** to open the **vShield Manager Configuration** dialog box and edit these vShield Manager account details.

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

Option	Description
vCenter Name	Specifies the name of the registered vCenter account.
vShield Manager Name	Specifies the name of the registered vShield Manager.
vShield Manager Address	Type the IP address or the host name of the available vShield Manager.
vShield Manager Username	Type the user name of the available vShield Manager.
vShield Manager Password	Type the password of the available vShield Manager.

Make sure that the credentials have administrative permissions.

5 Click **Validate** to verify the credentials of the vShield Manager and check that the connection to the vShield Manager works, then click **OK** to register the vShield Manager account.

Deploy SVA using McAfee ePO

Using the McAfee ePO console, deploy the SVA to one or more hypervisors. This deployment provides virus protection for virtual machines on the hypervisor.

Before you begin

- Make sure that you have installed the McAfee MOVE AV (Agentless) 3.6.0 extension.
- Make sure that you have checked in the SVA package to McAfee ePO.
- Make sure that you have appropriate permissions for the VMware vCenter account.
- Make sure that you have configured and registered a vShield Manager account with vCenter. You can edit the existing vShield Manager configuration using the **Edit** option under **Menu** | **Automation** | **MOVE AV Agentless** | **Configuration** | **vShield Manager**.
- Make sure that the client systems have the required VMTools installed.
- You have configured and registered all the LDAP servers, which are managing the client systems to be protected, on the McAfee ePO server. For successful installation of vsepflt, the domain user used to register the LDAP server must have the admin rights.
- Make sure that your McAfee ePO and client systems are in the domain. They must be able to communicate using their FQDN.
- Before deploying or removing the SVA using McAfee ePO, make sure that you manually synchronize the vCenter account using McAfee ePO. This action is important because the SVA deployment using McAfee ePO depends on the latest synchronization status provided by Data Center Connector for vSphere. For details, see the product documentation for Data Center Connector for vSphere.

The SVA deployment process using McAfee ePO involves these three simple steps:

1 **Common configuration** — Before deploying the SVA, complete this common configuration of the MOVE SVA and McAfee ePO, so that these settings are retrieved and used for every SVA deployment, which is done from the same McAfee ePO server.

2 **Service deployment** — Select the hypervisor and configure the parameters necessary for deployment. You must verify the parameters and prerequisites before starting the deployment.

3 **Job and task status details** — After initiating the SVA deployment or upgrade, view the **Job Status Details** and **Task Status Details** for the deployment on the McAfee ePO server.

The rollback functionality is available while deploying and upgrading the SVA. For example if the SVA deployment fails, the system automatically rolls back the deployment at the individual task level and reverts the system to its original state.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click **Menu** | **Automation** | **MOVE AV Agentless**.

3 From the **Service** tab, click **Actions** | **Deploy** to open the **Selection** page with these details.

- **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 McAfee ePO.
- **SVA Version** — Specifies the version of the SVA.
- **SVA Deployment Status** — Highlights any of these statuses during the deployment. This status is applicable to both the first time and upgrade deployment.

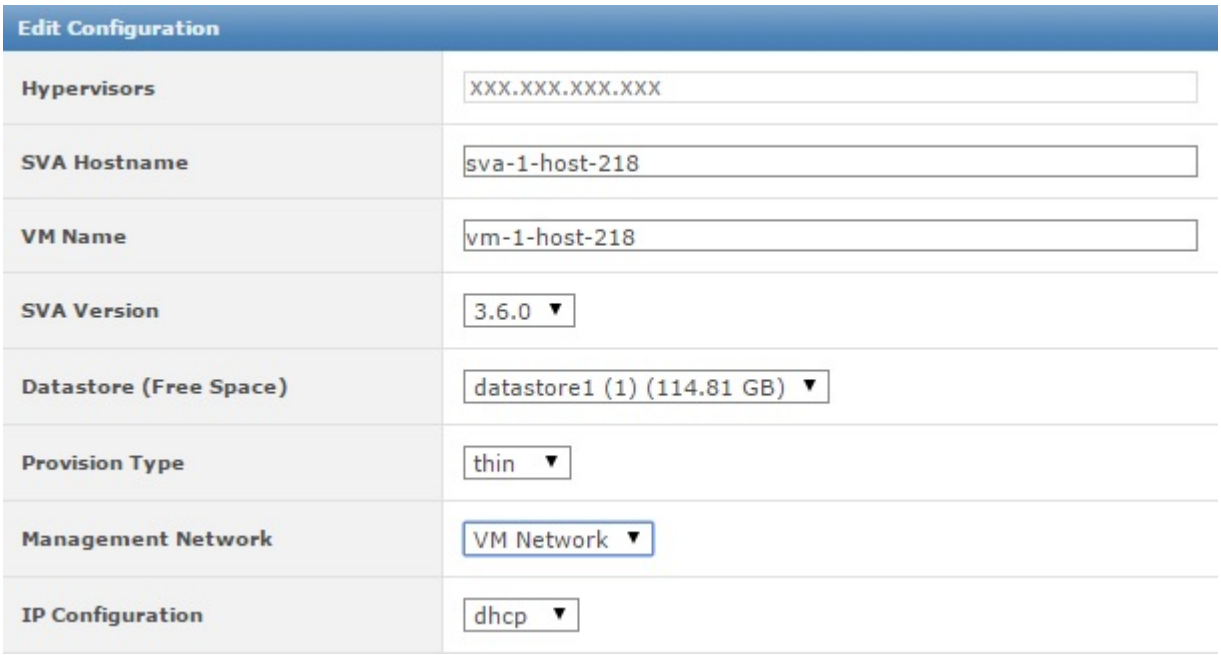
Status	Description
In Progress	Specifies that the SVA deployment is in progress.
Deployed	Indicates that the SVA deployment or upgrade completed successfully.
Deployment completed with error	Indicates that the SVA deployment is completed, however, there are some issues that must be fixed manually.
Deployment failed	Specifies that the SVA deployment or upgrade failed. You can check the **Task Status Details** under **MOVE AV Agentless**	**Status**.
Deployment failed with fatal error	Indicates that the deployment failed with some errors that require the administrators. Revert the system to its original state, fix the issues, and then redeploy the SVA.
Upgrade completed with error	Indicates that the SVA deployment is completed, however, there are some issues that must be fixed manually.

4 From the **Selection** page, select the required hypervisor to deploy the SVA, then click **Next** to open the **Configuration** page with these service setup details:

- **Hypervisors** — Lists the hypervisors present under the registered VMware vCenter account.
- **SVA Version** — Specifies the version of the SVA.

- **SVA Host Name** — Displays the name of the SVA host. Example: **SVA-1- host-5421**.
  - Here, **SVA** — Indicates the **SVA Hostname Prefix**, which is defined in the **General Configuration** page.
  - **1** — Specifies the vCenter ID.
  - **host-5421** — Specifies the Host ID.
- **Datastore (Free Space)** — Specifies the free space present in the datastore, where the SVA service virtual machines storage is added.
- **Provision Type** — Specifies the provision type.
- **Management Network** — Specifies the details of the Management Network.
- **IP Configuration** — Specifies the DHCP IP or Static IP Pool to be used.
- **Action** — From here, you can click **Edit** and change these settings.

All necessary details are automatically retrieved on the **Configuration** page. You can edit only if it is necessary to change any of the options.



5 Click **Save** and review the configurations of the hypervisor and SVA, then click **Next** to view the validation of these components and their status.

- SVA configurations
- Host details
- The compatibility status of components such as VMware vCenter, vShileld Manager, host, VMTools, and Endpoint version
- The available datastore space

You can view these Validation Statuses:

- **Passed** — Indicates that all prerequisites are available and configured correctly.
- **Failed** — Indicates any of the prerequisites is not available or not configured correctly.

- **Warning** — Check for specific warnings like:
  - VM Tools are not running.
  - Compatibility checking failed.
  - VMs are not part of the domain as McAfee ePO.

6 From the **Verification** page, click **Deploy** to start the SVA deployment.

You can now navigate to the **Status** tab and view the deployment tasks and their details.

View the SVA deployment details

After initiating the SVA deployment or upgrade, you can view the **Job Status Details** and **Task Status Details** for the deployment on the McAfee ePO server.

Before you begin

- Make sure that you have installed the McAfee MOVE AV (Agentless) extension.
- Make sure that you have initiated the SVA deployment using McAfee ePO.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click **Menu** | **Automation** | **MOVE AV Agentless**.

3 From the **Status** tab, you can view the SVA deployment or upgrade details.

4 Click any of the SVA deployment jobs to view these **Job Status Details** and its **Task Status Details**.

Table 2-3 Job status

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

Table 2-4 Task status

Item	Description
Node Type	Specifies whether the node is an SVA or a hypervisor, or a VM
Task Type	Specifies the set of internal tasks that happen within 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. For the list of tasks and details, see *Task status details*.
Node Name	Displays the SVA VM name, or Hypervisor name, or the guest 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.

The rollback functionality is available while deploying and upgrading the SVA. For example, if the SVA deployment fails, the system automatically performs the rollback of the deployment at individual task level and reverts the system to its original state.

Task type and status details

These are the task types that specify the set of internal tasks that happen within 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.

Table 2-5 During SVA deployment

Task type	Description
Installing vShield Endpoint	Indicates that the vShield Endpoint installation is in progress.
Deploying SVA	Indicates that the SVA deployment is in progress.
Powering on SVA	Specifies that the SVA is turned on.
Registering SVA with McAfee ePO	Registers the SVA with McAfee ePO.
Validating MOVE Service Status	Validates the status of the MOVE Service whether it is active.
Registering vendor with VSM	Registes the vendor with vShield Manager.
Registering solution with VSM	Registers the solution with vShield Manager.
Setting SVA IP and Port to VSM	Sets the SVA IP and Port to vShield Manager.
Activating SVA (Enabling security)	Specifies that the SVA is activated and the malware protection is enabled.

Table 2-5 During SVA deployment *(continued)*

Task type	Description
Enabling vShield Driver	Enables vShield Driver on the client machines.
Testing EICAR	Tests EICAR on one of the client machine on which vShield Driver installation is successful.

Table 2-6 During SVA removal

Task type	Description
Disabling vShield Driver	Disables vShield Driver on the client systems.
Deactivating SVA (Disabling Security)	Specifies that the SVA is deactivated and the malware protection is disabled.
Clearing SVA IP and Port from VSM	Removes the IP and Port details of the SVA from the vShield Manager.
Unregistering solution from VSM	Removes the registration of the SVA from the vShield Manager.
Unregistering vendor from VSM	Removes the registration of the vendor from the vShield Manager.
Powering off SVA	Specifies that the SVA is turned off.
Removing SVA	Removes the powered off SVA from the hypervisor.
Uninstalling vShield Endpoint	Indicates that the vShield Endpoint removal is in progress.
Returning Static IP to IPPool	Returns the used Static IP to the IP Pool.

Table 2-7 During SVA upgrade

Task type	Description
Deploying SVA	Indicates that the SVA deployment is in progress. When the latest SVA is already deployed on the hypervisor, the **Deploying SVA** task is skipped. Hence, other SVA related tasks do not start.
Uninstalling vShield Endpoint	Indicates that the vShield Endpoint removal is in progress.
Installing vShield Endpoint	Indicates that the vShield Endpoint installation is in progress.
Deactivating SVA (Disabling Security)	Specifies that the SVA is deactivated and the malware protection is disabled.
Clearing SVA IP and Port from VSM	Removes the IP and Port details of the SVA from the vShield Manager.
Unregistering solution from VSM	Removes the registration of the SVA from the vShield Manager.
Unregistering vendor from VSM	Removes the registration of the vendor from the vShield Manager.
Powering off SVA	Specifies that the SVA is turned off.
Renaming SVA	Renaming the old powered off SVA.
Renaming SVA	Renaming the new deployed off SVA.
Powering on SVA	Specifies that the SVA is turned on.
Registering SVA with McAfee ePO	Registers the SVA with McAfee ePO.
Validating MOVE Service Status	Validates the status of the MOVE Service whether it is active.
Registering vendor with VSM	Registes the vendor with vShield Manager.
Registering solution with VSM	Registers the solution with vShield Manager.
Setting SVA IP and Port to VSM	Sets the SVA IP and Port to vShield Manager.
Activating SVA (Enabling security)	Specifies that the SVA is activated and the malware protection is enabled.

Table 2-7 During SVA upgrade *(continued)*

Task type	Description
Removing SVA	Removing the powered off old SVA from hypervisor
Enabling vShield Driver	Enables vShield Driver on the client machines.
Testing EICAR	Tests EICAR on one of the client machine on which vShield Driver installation is successful.

Table 2-8 During rollback

Task type	Description
Rollback : Uninstalling vShield Endpoint	Rolls back the Installing vShield Endpoint task.
Rollback : Powering off SVA	Rolls back the Powering on SVA task.
Rollback : Remove SVA	Rolls back the Deploying SVA task.
Rollback : Testing EICAR	Rolls back the testing EICAR SVA upgrade.
Rollback : Returning Static IP to IPPool	Rolls back the static IP to IPPool which was assigned to the deployed SVA.

Remove SVA using McAfee ePO

Using the McAfee ePO console, remove the SVA from one or more hypervisors.

Before you begin

- Make sure that you have registered the vCenter with vShield Manager.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Click **Menu** | **Automation** | **MOVE AV Agentless**.

3 From the **Service** tab, click **Actions** | **Undeploy** to open the **Selection** page with these details.

- **Hypervisors** — Lists the Hypervisors, present under the registered VMware vCenter account, where the SVA is already deployed.
- **vCenter Account** — Specifies the name of the VMware vCenter account that is registered with McAfee ePO.
- **SVA Version** — Displays the SVA version.

4 From the **Selection** page, select the required hypervisors from where you want to remove the SVA and click **Next** to open the **Verification** page with these details:

- **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 McAfee ePO.
- **SVA Version** — Specifies the version of the SVA.
- **SVA VM Name** — Displays the name of the SVA host.
- **Validation Status** — Displays the validation status that specifies whether the SVA can be removed.

5 Click **Remove** to remove the SVA from the selected hypervisors.

After initiating the SVA removal process, you can view the **Job Status Details** and **Task Status Details** for the removal on the McAfee ePO server.

Table 2-9 Job status

Item	Description
Start Time	Indicates the date and time when the SVA deployment started.
End Time	Indicates the date and time when the SVA deployment ended.
Deployment Type	Displays the SVA deployment type as **Remove**.
Status	Specifies the deployment status such as **Started**, **Completed**, **Failed**, **Completed with error**, and **Fatal error**.
vCenter Name	Specifies the name of VMware vCenter account that is registered with McAfee ePO.
Hypervisors	Specifies the name of the hypervisor.

Table 2-10 Task status

Item	Description
Node Type	Specifies whether the node is an SVA or a hypervisor.
Task Type	Specifies the set of internal tasks that happen within 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. For the list of tasks and details, see *Task status details*.
Node Name	Displays the name or IP address of the SVA.
Status	Specifies the task status such as **Started**, **Completed**, **Failed**, and **Skipped**.
Failure Reason	Specifies the reason for the failure of the task. Example: • **SVAs are still registered** • **Returning DHCP IP is not applicable**
Start Time	Indicates the date and time when the task started.
End Time	Indicates the date and time when the task ended.

Deploy VMware Endpoint

You must deploy VMware Endpoint on your virtual environment before you can install and configure the software.

Task

1. Log on to the VMware vCenter Web Client as an administrator.
2. Click **Networking & Security** | **Installation** | **Service Deployments** to open the **Networking & Security Service Deployment** page.
3. Click **+** to open the **Deploy Network & Security Services** page.
4. Select the **VMware Guest Introspection** service to deploy, then select **Deploy now**. You can also specify the schedule for deployment.
5. Click **Next** to open the **Select clusters** page.
6. Select the data center and clusters where you want to deploy the SVA, then click **Next** to load the **Datastores**.

7 On the **Select storage** page, select the **Datastore** where you want to add the SVA service virtual machines storage, or select **Specified on host**.

The selected datastore must be available on all hosts in the selected cluster.

If you selected **Specified on host**, the datastore for the ESX host must be specified in the AgentVM Settings of the host before it is added to the cluster. For details, see vSphere API/SDK documentation.

8 Configure and verify the management network.

9 Assign a network and IP address range for each service to use, then click **Next**. The **Ready to complete** page appears.

Make sure that you have created the required static IP pool when you are not using the **DHCP** option. For details about configuring this network and IP address range with NSX Manager and vSphere Web Client, see *NSX Administration Guide* available at http://pubs.vmware.com/NSX-6/index.jsp.

10 Review the settings, then click **Finish** to save the settings. This action initiates the VMware Endpoint deployment to all hypervisors in the selected cluster. The VMware Endpoint deployment might take a few minutes to complete.

VMware NSX Manager-based deployment

Using McAfee ePO and VMware vCenter Web Client, you can register, configure the SVA with VMware NSX Manager, and deploy it to one or more clusters.

This deployment automatically provides virus protection for virtual machines on a new hypervisor from the moment the hypervisor is added to the cluster. For details about how to configure, monitor, and maintain the VMware NSX system with NSX Manager and vSphere Web Client, see *NSX Administration Guide* available at http://pubs.vmware.com/NSX-6/index.jsp.

Add NSX Manager and SVA details to McAfee ePO

Add NSX Manager and SVA details to McAfee ePO, so that you can validate the certificate details of NSX Manager and register it with the SVA.

Before you begin

- From the McAfee download site, download **MOVE-AV-AL_OVF_3.6.0.zip**. If you installed the ePolicy Orchestrator server 4.6.x with Installer for McAfee Endpoint Suites, go to the postInstall directory in the unzipped package of EASI_DataCenter and download the **MOVE-AV-AL_OVF_3.6.0.zip** file.
- Make sure that you have installed the McAfee MOVE AV Agentless extension.
- Make sure that you have the VMware NSX Manager credentials ready.

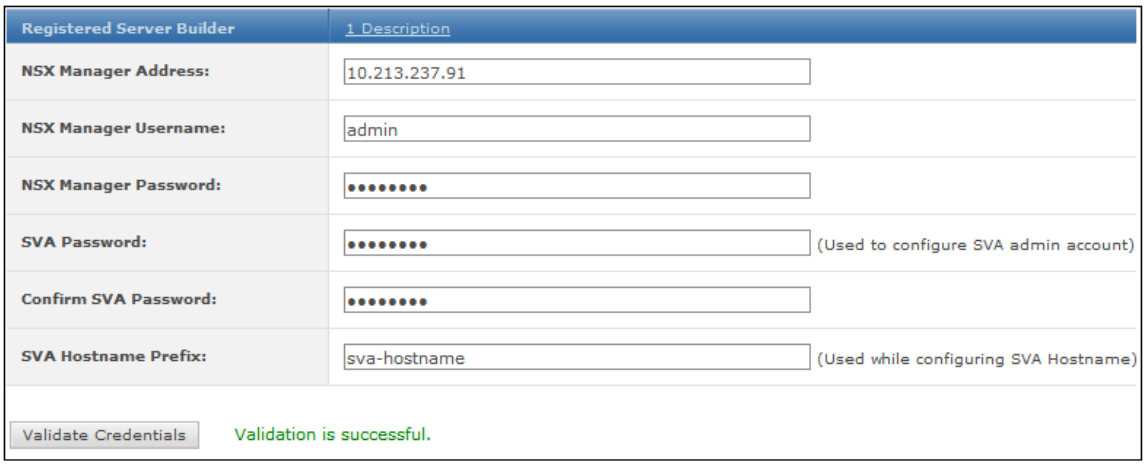
Task

For option definitions, click **?** in the interface.

1 Log on to McAfee ePO as an administrator.

2 Click **Menu** | **Configuration** | **Registered Servers**, then click **New Server** to open the **Registered Server Builder** page.

3 From the **Server Type** drop-down list on the **Description** page, select **NSX Manager**, and specify a unique user-friendly name and some details that can help you identify the server, then click **Next**.



4 On the **Details** page, configure these settings as needed:

- **NSX Manager Address** — Type the IP address or the host name of the available 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.
- **SVA Password** — Type the password of the available SVA.
  - The password must be at least six characters long.
  - The password must contain at least one uppercase letter (A-Z) and one numeric character (0–9).
- **Confirm SVA Password** — Retype the password of the available SVA.
- **SVA hostname prefix** — Type the unique host name, per NSX Manager, for the SVA to be deployed on hosts. The host name can include characters a–z, A–Z, 0–9, and [-], without space.

You cannot edit the SVA credentials after you add them to McAfee ePO.

You can edit the existing NSX Manager details with the **Edit** option under **Registered Servers** | **Actions**.

5 Click **Validate Details** to open the **Certificate verification** page.

The certificate validation can be done only after validating the NSX Manager credentials. Any change to the NSX Manager certificate after adding the NSX Manager details in the McAfee ePO server interrupts the communication between NSX Manager and McAfee ePO. To restore the communication, validate the NSX Manager details in the McAfee ePO server.

6 Click **OK**. This action verifies and validates the NSX Manager certificate.

7 Click **Save**.

Check in the SVA package to McAfee ePO

You must check in and host the SVA package in McAfee ePO, so that you can use it with VMware NSX Manager, then deploy it to the cluster. You can view and delete the SVA package using McAfee ePO.

Before you begin

- From the McAfee download site, download **MOVE-AV-AL_OVF_3.6.0.zip**. If you installed the ePolicy Orchestrator server 4.6.x with Installer for McAfee Endpoint Suites, go to the postInstall directory in the unzipped package of EASI_DataCenter and download the **MOVE-AV-AL_OVF_3.6.0.zip** file.
- Make sure that you have installed the McAfee MOVE AV (Agentless) extension.

Make sure that you do not change the file name of the SVA package.

Task

For option definitions, click **?** in the interface.

1 Log on to McAfee ePO as an administrator.

2 Click **Menu** | **Configuration** | **MOVE repository** to open the **MOVE SVA repository configuration** page with these SVA details and actions:

Options	Description
SVA Name	Name of the SVA package checked in to McAfee ePO.
SVA Version	Version of the SVA package checked in to McAfee ePO.
Used	• **Yes** — Specifies that the SVA is registered with at least one NSX Manager. • **No** — Specifies that the SVA is not registered with any NSX Manager.
Actions	• **Delete** — To remove an existing SVA from McAfee ePO when it is not registered with NSX Manager. • **Add SVA** — To open the **Check-in SVA OVF (zip) file** page.

3 Click **Actions** | **Add SVA** to open the **Check-in SVA OVF (zip) file** page.

4 From **Select SVA (zip) file to check-in**, browse to and select the SVA package, then click **OK**. This action checks in the SVA package to McAfee ePO.

Register the SVAs with VMware NSX Manager

Select the required SVA version and register it with VMware NSX Manager, which was added to the McAfee ePO server. This registration allows you to deploy the SVA to one or more clusters.

Before you begin

- From the McAfee download site, download **MOVE-AV-AL_OVF_3.6.0.zip**. If you installed the ePolicy Orchestrator server 4.6.x with Installer for McAfee Endpoint Suites, go to the postInstall directory in the unzipped package of EASI_DataCenter and download the **MOVE-AV-AL_OVF_3.6.0.zip** file.
- The required SVA packages are checked in to the SVA repository in McAfee ePO.
- The NSX Manager is registered with McAfee ePO.

Task

For option definitions, click **?** in the interface.

1. Log on to McAfee ePO as an administrator.
2. Click **Menu** | **Configuration** | **MOVE Service Registration**. This action lists all NSX Managers registered in McAfee ePO.
3. From the **Actions** column on the **MOVE Service configuration** page, click **Register** to open the **Register NSX server** dialog box.
4. From the **Choose SVA version** drop-down list, select the required version of SVA to be registered, then click **OK**.

You can now view the SVA registration status such as **Success**, **Failed**, **Not registered**, and **Upgraded** under the **Last Action Status** column.

Deploy the SVA using VMware NSX Manager

Using the VMware NSX Manager console, deploy the SVA to one or multiple clusters.

Before you begin

- The MOVE SVA must be registered with VMware NSX Manager.
- The McAfee MOVE AV Agentless extension is installed on the McAfee ePO server.
- The host, where you are deploying the SVA using NSX Manager, must be part of a cluster.
- All hosts must be configured with a distributed virtual switch.
- Make sure that you do not migrate the vshiled-pg network of VMs or SVA.
- The VMware Endpoint is deployed on every cluster.

This deployment automatically provides virus protection for virtual machines on a new hypervisor from the moment the hypervisor is added to the clusters. However, when a new cluster is added, deploy the SVA again.

Task

1. Log on to the VMware vCenter Web Client as an administrator.
2. Click **Networking & Security** | **Installation** | **Service Deployments** to open the **Networking & Security Service Deployment** page.
3. Click **+** to open the **Deploy Network & Security Services** page.
4. Select the **McAfee MOVE AV** service to deploy, then select **Deploy now**. You can also specify the schedule for deployment.
5. Click **Next** to open the **Select clusters** page.
6. Select the data center and clusters where you want to deploy the SVA, then click **Next** to load the **Datastores**.

7 On the **Select storage** page, select the **Datastore** where you want to add the SVA service virtual machines storage, or select **Specified on host**.

The selected datastore must be available on all hosts in the selected cluster.

If you selected **Specified on host**, the datastore for the ESXi host must be specified in the **AgentVM Settings** of the host before it is added to the cluster. For details, see vSphere API/SDK documentation.

8 On the **Configure Management** page:

a Select **Distributed switch** for **Network**.

b Select **IP pool** (recommended) or **DHCP** for **IP address**.

The selected **DPort Group** must be available on all hosts in the selected cluster. If you selected **Specified on host**, the network for the ESXi host must be specified in the **AgentVM Settings** of the host before it is added to the cluster. For details, see vSphere API/SDK documentation. Make sure that you have created the required static IP pool when you are not using the **DHCP** option. For details about configuring this network and IP address range with NSX Manager and vSphere Web Client, see *NSX Administration Guide* available at http://pubs.vmware.com/NSX-6/index.jsp.

9 Click **Next** to open the **Ready to complete** page.

Make sure that you migrate all Host networks and VMs to DVport group.

10 Review the settings and click **Finish**. This action initiates the SVA deployment to all hypervisors in the selected cluster. The SVA deployment might take a few minutes to complete. You can then view the managed SVA in the System Tree of McAfee ePO.

After adding the NSX Manager details in the McAfee ePO server, any change to the NSX Manager certificate interrupts the communication between NSX Manager and McAfee ePO. To restore the communication, edit and validate the NSX Manager details in the McAfee ePO server.

11 After deploying the SVA, retrieve this **Service status** on the VMware vCenter Web Client console.

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

12 Add any new host to the cluster:

a Configure the required datastore before adding the host.

b Migrate the host to the virtual distributed switch.

For details, see *NSX Administration Guide* available at http://pubs.vmware.com/NSX-6/index.jsp.

Configuring the security group and security policy

You can create a security group that includes all VMs in the vCenter and assign them security policies, which you can create using the VMware vCenter Web Client.

This configuration is a one-time initial activity for a vCenter. However, you must do this configuration again when a new data center is added.

Create a global security group

You can select all data centers from the available vCenter and configure them as a security group, so that you can assign a security policy to this group and protect it from viruses.

Before you begin

- VMware vSphere 5.5 is installed and added to the cluster.
- The MOVE SVA is registered with VMware NSX Manager.
- The McAfee MOVE AV (Agentless) extension is installed on the McAfee ePO server.

Task

1 Log on to the VMware vCenter Web Client as an administrator.

2 Click **Networking & Security** | **Service Composer** | **Security Groups**, then click the **New Security Group** icon to open the **Name and description** page.

3 Specify a unique user-friendly name and any details to identify the security group, then click **Next** to open the **Define dynamic membership** page.

4 Keep the default configuration for the dynamic membership criteria that objects must meet to be part of this security group, then click **Next** to open the **Select objects to include** page.

5 From the **Datacenter** tab under **Filter**, select the required data centers, then click **Next** to open the **Select objects to exclude** page.

If you include and exclude a cluster in the same **Security Group**, the exclusion takes priority. Objects that are excluded are not protected.

6 Select the objects to exclude, then click **Next** to open the **Ready to complete** page.

7 Review the settings, then click **Finish** to create the security group.

Configure the security policy with MOVE AV Service

You can configure a security policy and configure it, so that you can assign the policy to a security group and protect the systems from viruses.

Before you begin

- VMware vSphere 5.5 is installed and it is added to the cluster.
- The MOVE SVA is already registered with VMware NSX Manager.
- The McAfee MOVE AV (Agentless) extension is installed on the McAfee ePO server.

Task

1 Log on to the VMware vCenter Web Client as an administrator.

2 Click **Networking & Security** | **Service Composer** | **Security Policies**, then click the **New Security Policy** icon to open the **Name and description** page.

3 Specify a unique user-friendly name and some details that can help you identify the server, then click **Next** to open the **Endpoint Services** page.

4 Click **+** to open the **Add Endpoint Service** page, then specify these **Endpoint Service** details:

For this...	Do this...
Name	Type the name of the MOVE service.
Description	Type some details about the MOVE service, which help you to identify the SVA.
Actions	• **Apply** — Select this to apply the SVA. • **Block** — Select this to block the SVA.
Service Type	From the drop-down list, select **Anti Virus**.
Service Name	From the drop-down list, select **McAfee MOVE AV**.
Service Configuration	From the drop-down list, select **MOVE-Global Policy**.
State	• **Enabled** — Select this to enable the service. • **Disabled** — Select this to disable the service.
Enforce	Keep the default value.

5 Click **OK** to open the **Firewall Rules** page.

6 Configure the **Firewall Rules** and **Network Introspection Services**, then click **Next** to open the **Ready to complete** page.

7 Review the settings, then click **Finish** to create the **Security Policy**.

8 Apply this security policy on the security group by clicking **Service Composer** | **Security Policies** | **Actions** | **Apply Policy**.

Deploy multiple OVFs

As part of the SVA setup and configuration, you must deploy the OVF to hypervisor.

Before you begin

- From the McAfee download site, download and extract the contents of **MOVE-AV-AL_OVF_3.6.0.zip**.
- Install the VMware OVF Tool (version 3.0 or 3.5) on the system where you are running the deployment.
- VMware vShield Endpoint must be installed on the host or hypervisor.
- Disable vMotion on the SVA. You can host the SVA on the hypervisor's local disk to avoid using vMotion.

Task

1 Gather this information, which you require to run the configuration script:

SVA	IP address
vCloud Networking and Security Manager	IP address or DNS name User name and password
vCenter	IP address or DNS name User name and password

Don't use special characters when creating the user name or password for vCenter. Using special characters results in failure to deploy the SVA.

This account can be a local admin or domain account on the vCenter server.

ePolicy Orchestrator	Server IP address and port User name and password

You must have a valid ePolicy Orchestrator user name that uses ePolicy Orchestrator authentication.

2 Extract the `MOVE-AV-AL_SVA_Deployment_3.6.0.zip` file and open the CSV file.

3 In the CSV file, provide the required information for each OVF, then save the CSV file.

4 From the folder where you extracted `MOVE-AV-AL_SVA_Deployment_3.6.0.zip`, run `launch.bat` to start the command prompt.

5 Enter `2` to deploy the SVA.

The script parses the CSV file and sends it to the SVA.

6 Turn on the VM.

CSV file properties

If you deploy the OVF from the Perl Deployment package, you must fill out a CSV file containing the SVA configuration information. We provide a CSV file template that contains these columns. See the associated OVF property for details.

The **Hypervisor**, **Datastore**, and **ePO Server Network** are case-sensitive and must match the values displayed in the vSphere Client.

Column header	OVF property
Hypervisor	The hypervisor where you deploy the OVF You can specify the IP address or hypervisor. If providing the hypervisor, make sure to specify the name that appears in the vCenter console.
SVA	The name of the VM
Datastore	The datastore for the SVA virtual disk

Column header	OVF property
ePO Server Network	The name of the ESXi network that the McAfee ePO server uses to manage the McAfee SVA. To successfully deploy the SVA to a hypervisor with a network that is serviced by a distributed switch (vDS), at least two hypervisors must be connected to the vDS to provide DVPort backing.
ip_config	Network Type
SVA_IP	Network IP address
SUBNET_MASK	Network Netmask
Gateway	Network Gateway
DNS_Server1 (Optional)	DNS Primary Server
DNS_Server2 (Optional)	DNS Secondary Server
Domain (Optional)	SVA Domain
Network (Optional)	Network
Broadcast Address (Optional)	Network Broadcast Address

Manually deploy the OVF

Manually deploy the OVF to the selected hypervisor to ensure protection.

Before you begin

- From the McAfee download site, download **MOVE-AV-AL_OVF_3.6.0.zip**. If you installed the ePolicy Orchestrator server 4.6.x with Installer for McAfee Endpoint Suites, go to the postInstall directory in the unzipped package of EASI_DataCenter and download the **MOVE-AV-AL_OVF_3.6.0.zip** file.
- VMware vShield Endpoint must be installed on the hypervisor.
- To ensure that vMotion does not move the SVA from the selected hypervisor, deploy the SVA on local datastore.
- The vSphere Client must be connected to a vCenter server to successfully deploy the OVF.
- To successfully deploy the SVA to a hypervisor with a management network that is serviced by a distributed switch (vDS), at least two hypervisors must be connected to the vDS to provide DVPort backing.

Task

1 From the vSphere Client, select the resource pool on the hypervisor where you want to deploy the OVF, then click **File** | **Deploy OVF Template** to open the OVF wizard.

2 Apply these settings to deploy the OVF:

For this option...	Do this...
Source	Browse to and select **move-sva.ovf** file.
OVF Template Details	Review details about the OVF.
End User License Agreement (EULA)	Accept this to continue.
Name and Location	Specify the name of the SVA and the inventory location.
Storage	Select the datastore for the SVA. This page is displayed only if the hypervisor has multiple datastores.
Disk Format	Select the required disk provisioning.
Network Mapping	Map the OVF networks to the existing networks on the selected hypervisor.
Properties	If you specify the configuration information about the **Properties** page, then the SVA is automatically configured during the initial start. See *OVF properties*. To manually configure the SVA, do not specify the settings on the **Properties** page. See *Manually configure the SVA*. We recommend manually configuring the SVA. If you deploy the SVA from VMware vCenter, do not specify any NSX Manager details.
Nails	Set the required VSEL password. You can also leave this option blank.
Keys	If a value is set for **Keys**, all passwords are encrypted. You can use the key value to decrypt the passwords. If there is no value set, the passwords are expected to be in plain text.
Ready to Complete	Review the options you selected.

3 Click **Finish**.

Configure the SVA

There are two SVA configuration options: automatic configuration and manual configuration.

- The SVA is automatically configured when you select any of these deployment options:
  - McAfee ePO-based deployment
  - VMware NSX Manager-based deployment
  - Multiple OVF deployment

  Or,

  - When you provide the configuration information about the Properties page during manual deployment.

- If you select the Manual Deployment option and don't provide the configuration information about the **Properties** page, you must manually configure the SVA.

The MOVE AV Agentless Security Virtual Appliance (SVA) OVF (Open Virtualization Format) template has a preconfigured Time Zone, DATE and TIME, using default values. So, the scheduled on-demand scans in MOVE AV Agentless start at a different time than what you have configured.

Task

1 Log on to the SVA using the root or administrator account.

2 Run the command `sudo dpkg-reconfigure tzdata` to reconfigure the Time Zone.

3 When prompted, type your password.

4 Select your local Geographic Region and Time Zone from the list.

5 Run the command `sudo date -s "16 APR 2012 16:05:00"` to configure the DATE and TIME.

In this example, the DATE and TIME is configured to be: 16 April 2012 4:05 PM.

6 When prompted, type your password.

Tasks

- *Manually configure the SVA* on page 41
  The first time you log on, the configuration script automatically runs.

Manually configure the SVA

The first time you log on, the configuration script automatically runs.

Before you begin

Gather this information, which you need when you run the configuration script:

SVA	IP address
vCloud Networking and Security Manager	IP address or DNS name User name and password
vCenter	IP address or DNS name User name and password
ePolicy Orchestrator	Server IP address and console-to-application server communication port is required (default is 8443) User name and password

You must have a valid ePolicy Orchestrator user name that uses ePolicy Orchestrator authentication.

If you provided the configuration information in the **Properties** setting and it doesn't show up in ePolicy Orchestrator, log on to the SVA and follow this task.

Use this command to manually run the configuration script `sudo /opt/McAfee/move/bin/sva-config`.

Task

1 Turn on the VM.

2 From the vSphere Client, open the console.

3 At the prompt, log on with these credentials:

- User name: `svaadmin`
- Password: `admin`

The configuration script runs automatically the first time you log on.

4 Follow the prompts and answer questions as they apply to your environment.

OVF properties

If you manually deploy the OVF from the vSphere Client, the **Properties** page contains these settings. If these settings are specified during deployment, the SVA is configured automatically the first time you start your system.

Category	Setting	Description
DNS	Primary Server	The IP address of the primary DNS server.
DNS	Secondary Server	The IP address of the secondary DNS server.
ePolicy Orchestrator	FIPS Mode	Specified if FIPS mode is enabled on the ePolicy Orchestrator server.
ePolicy Orchestrator	IP Address	The IP address or DNS name of the ePolicy Orchestrator server.
ePolicy Orchestrator	Password	The user's password.
ePolicy Orchestrator	Port	The console-to-application server communication port used when connecting to the ePolicy Orchestrator server. Default is 8443.
ePolicy Orchestrator	User name	The user name used to access the ePolicy Orchestrator server. You must have a valid ePolicy Orchestrator user name that uses ePolicy Orchestrator authentication.
Network	Type	How to configure the SVA's IP address for the management network (DHCP or static). Default is DHCP. When DHCP is specified, you don't require to enter any other network settings. The DNS servers must be automatically discovered. Any DNS server specified overwrites the automatically discovered DNS server.
Network	Broadcast Address	The SVA's broadcast address.*
Network	Gateway	The SVA's default gateway.*
Network	IP Address	The static IP Address of the SVA.*
Network	Netmask	The netmask for the SVA's management network.*
Network	Network	The network for the SVA's static IP address.* This property is optional. If this setting remains blank, it is created from the IP address and the Netmask.
SVA	Domain	The SVA's domain name and the default domain name for DNS queries.

Category	Setting	Description
SVA	Host name	The host name of the SVA.
SVA	savaadmin Password	The password of the svaadmin account.
vCloud Networking and Security Manager	IP Address	The IP address or DNS name of the vCloud Networking and Security Manager.
vCloud Networking and Security Manager	Password	The password used to register the SVA with the vCloud Networking and Security Manager.
vCloud Networking and Security Manager	User name	The user name used to register the SVA with the vCloud Networking and Security Manager.

* This is only applicable when the **Network Type** is **static**.

Uninstalling McAfee MOVE AV (Agentless)

A full uninstall involves removing these components: McAfee MOVE AV service, MOVE SVA, NSX Manager details, and the McAfee MOVE AV (Agentless) extension.

Remove the SVA from the cluster

Using the VMware vCenter Web Client Networking and Security console, you can remove the SVA, which is deployed to one or more clusters.

Task

1 Log on to the VMware vCenter Web Client as an administrator.

2 Click **Networking & Security** | **Installation** | **Service Deployments** to open the **Networking & Security Service Deployment** page.

3 Select **McAfee MOVE AV** and click the **Delete service deployment** icon. The **Confirm Delete** message appears.

4 Click **Delete now** to confirm, then click **OK**. You can also schedule to delete it later.

Make sure that you wait until the SVA is removed from all clusters.

Remove the MOVE Endpoint Service from the Security Policy

Remove the MOVE Endpoint Service from the Security Policy using the VMware vCenter Web Client console.

Task

1 Log on to the VMware vCenter Web Client as an administrator.

2 Click **Networking & Security** | **Service Composer** | **Security Policies**, then select an existing **Security Policy** and click the **Edit Security Policy** icon to open the **Name and description** page.

3 Change the **Name** and **Description**, if necessary, then click **Next** to open the **Endpoint Services** page.

4 Select the required MOVE Endpoint Service, then click the **Delete** icon.

5 Click **Finish**. This action removes the MOVE Endpoint Service.

Unregister the VMware NSX Manager from McAfee ePO

Select the registered VMware NSX Manager and unregister it from the McAfee ePO server.

Task

1. Log on to McAfee ePO as an administrator.
2. Click **Menu** | **Configuration** | **MOVE Service Registration**. This action lists all NSX Managers registered in McAfee ePO.
3. From the **Actions** column on the **MOVE Service configuration** page, click **Unregister** for the registered NSX Manager. A confirmation dialog box appears.
4. Click **OK** to confirm.

Remove NSX Manager details from McAfee ePO

Remove NSX Manager details from the McAfee ePO server, so that you can do a clean removal of the product.

Task

For option definitions, click **?** in the interface.

1. Log on to McAfee ePO as an administrator.
2. Click **Menu** | **Configuration** | **Registered Servers** to open the **Registered Servers** page.
3. Select the existing **NSX Manager** that you want to remove, then click **Actions** | **Delete**. A confirmation dialog box appears.
4. Click **Yes** to confirm.

Uninstall the extension

Uninstall the McAfee MOVE AV (Agentless) extension from ePolicy Orchestrator.

Task

For option definitions, click **?** in the interface.

1. From the ePolicy Orchestrator console, click **Menu** | **Software** | **Extensions**.
2. Next to the extension you want to remove, click **Remove**.

Extension	Name
Main product extension	`MOVE-AV-AL_EXT_3.6.0.zip`
License extension	`MOVE-AV-AL_License_EXT_3.6.0.zip`

This action removes the McAfee MOVE AV (Agentless) extension and the MOVE SVA package, which is already checked in to the McAfee ePO server.

3 Monitoring and managing your environment

The Agentless deployment option monitors the status of virtual desktops and changes behavior from the ePolicy Orchestrator console.

Contents

Integration with ePolicy Orchestrator

The Agentless deployment option uses the ePolicy Orchestrator framework for delivering and enforcing policies. This approach provides a single management solution that allows you to deploy the software to all your virtual machines.

ePolicy Orchestrator communicates policy information to the SVA on a regular interval through the McAfee Agent. The McAfee Agent enforces policies on the SVA, collects event information, and transmits the information back to ePolicy Orchestrator.

Policy management

Through the ePolicy Orchestrator console, you can configure policies for your managed product from a central location.

How policies are enforced

When you change policies in the ePolicy Orchestrator console, the changes take effect on the SVA at the next agent-server communication. To enforce policies immediately, send an agent wake-up call to the targeted SVA from the ePolicy Orchestrator console.

Policies and their categories

Policy information is grouped into two categories: **SVA** and **Scan**. You can create, modify, or delete as many policies as needed under these categories. ePolicy Orchestrator provides a preconfigured **McAfee Default** policy, which cannot be edited or deleted but can be copied. You then modify these copies to suit your needs.

How policies are applied

Policies are applied to any **System Tree** group or system by inheritance or assignment. *Inheritance* determines whether the policy settings for any system are taken from its parent.

By default, inheritance is enabled throughout the System Tree. You can break inheritance by direct policy assignment. The Agentless deployment option, as managed by ePolicy Orchestrator, enables you to create policies and assign them without regard to inheritance. When you break this inheritance by assigning a new policy to a system, all groups and systems that are children of the selected system inherit the new policy.

Configuring policies

You can create, modify, or delete as many policies as you need. The extension provides a preconfigured **McAfee Default** policy, which cannot be edited or deleted but can be copied and used as a base for new policies.

The **SVA** policy allows the administrator to define how and when anti-virus scans run on a hypervisor. These policies are applied to the hypervisor instead of the VM or system. The **Scan** policy allows the administrator to configure scan settings for when a threat is found.

Create an SVA policy

Create a new policy to change behavior on managed systems.

Task

For option definitions, click **?** in the interface.

1. From the ePolicy Orchestrator console, click **Menu** | **Policy** | **Policy Catalog**.
2. From the **Product** drop-down list, select **MOVE AV Agentless 3.6.0**.
3. From the **Category** drop-down list, select **SVA**.
4. Click **New Policy**.
5. On the **New Policy** page, configure the policy settings, then click **OK**.
6. In the **Authentication** tab of the **Policy Settings** page for the newly created policy, configure these settings to control basic behavior.
   - **Protocol** — Select **https** or **http**, depending on the protocol the server uses to receive client requests.
   - **Hypervisor/vCenter Server** — Enter the valid IP address of either the hypervisor that the SVA resides on or the vCenter server.

- **User** — Enter the user name credentials to connect with the server.
- **Password** — Enter the password associated with the user.

After you save and reopen an SVA policy, the vCenter password will appear blank. Even though it appears blank, it is saved in the policy settings. The password must be re-entered to test connection settings. 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.

7 In the **Scan Settings** tab, configure these settings to control which files are scanned.

Increasing the **Cache scan result of file size up to (MB)** might negatively impact performance. The complete file must transfer to the SVA to create an accurate hash of the file's contents.

- **Scan Time** — Green symbolizes a time slot where a scan might start; white symbolizes when a scan might not start. Each grid cell can be toggled available (green) or unavailable (white) by clicking the cell, column header, or row header.

8 In the **Quarantine settings** tab, configure the network share, so that all detected malware is quarantined to the specified network share.

However, the malware that is detected on any virtual machine is quarantined only when you have enabled the **Quarantine configuration** option under **Scan policy**.

Create a scan policy

Create a **Scan** policy to change behavior on managed systems.

Task

For option definitions, click **?** in the interface.

1 From the ePolicy Orchestrator console, click **Menu** | **Policy** | **Policy Catalog**.

2 From the **Product** drop-down list, select **MOVE AV Agentless 3.6.0**.

3 From the **Category** drop-down list, select **Scan**.

4 Click **New Policy**.

5 On the **New Policy** page, configure the policy settings, then click **OK**.

6 In the **General** tab of the **Policy Settings** page for the newly created policy, configure the settings to control basic behavior.

7 In the **Scan Items** tab, configure these settings to control which files are scanned.

Table 3-1 Scan Items

Option	Definition
On-Access Scan files	When an attempt is made to open, close, or rename a file, the scanner intercepts the operation and takes these actions. 1 The scanner determines if the file should be scanned based on this criteria: • The file's extension matches the configuration. • The file has not been cached, excluded, or previously scanned. 2 If the file meets the scanning criteria, the scanner compares the information in the file to the known malware signatures in the currently loaded DAT files. • If the file is clean, the result is cached and read, write, or rename operation is granted. • If the file contains a threat, the operation is denied and the configured action is taken.
File types to scan	• **All files** — Select to scan all files. • **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. • **Default + Additional files** — 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. In version 3.6, this option is selected by default. However, when upgrading from previous versions to 3.6, the last selected option is retained.
Compressed files	• **Scan inside archives (e.g. .ZIP)** — Examines archive (compressed) files (such as .ZIP, .CAP. LZH, and .UUE files) and their contents. • **Decode MIME encoded files** — Detects, decodes, and scans Multipurpose Internet Mail Extensions (MIME) encoded files.
Heuristics	Uses heuristics to find unknown unwanted programs, Trojans, and macro threats.
McAfee Global Threat Intelligence file reputation	Configure the sensitivity level (between **Very Low** and **Very High**) when determining if a detected sample is malware. By increasing the sensitivity level, you might also get more false positive results.
Unwanted program detection	**Detect unwanted programs** — The on-access and on-demand scanners detect unwanted programs based on the Unwanted Programs Policy that you configured. When a detection occurs, the scanner that detected the potentially unwanted program applies the action that you configured on the **Actions** tab for that scanner.

8 In the **Exclusions** tab, configure the **Path Exclusions** by adding, editing, or removing a specific file path.

The MOVE Agentless allows you to fine-tune the list of file types scanned. For example, you can exclude from scanning individual files, folders, and disks. These exclusions might be needed because the scanners could scan and lock a file when that file is being used by a database or server. This could cause the database or server to fail or generate errors.

Wildcards are supported, however, environment variables and UNC paths are not supported.

For more information on how to use wildcards when creating exclusions in MOVE AV Agentless 3.x, see this McAfee KnowledgeBase article: KB82110.

9 In the **Actions** tab, configure **When a threat is found behavior**. You must select a first action and a secondary action.

For the first action, available options are **Delete files automatically** and **Deny access to files**. The only current secondary action option is **Deny access to files**.

10 In the **Quarantine** tab, enable the **Quarantine configuration** option, so that the malware that is detected on any virtual machine is quarantined.

Before enabling, make sure that you have provided correct quarantine details in the **SVA** policy. For details, see *Create an SVA policy*.

See also

Using the SVA policy quarantine settings on page 53

Apply a policy

You must apply a policy for it to take effect. You can apply McAfee MOVE AV (Agentless) **Scan** policy to individual virtual machine, group, or even to SVA machines. However, you can apply the **SVA** policy to SVA virtual machines only.

Task

For option definitions, click **?** in the interface.

1 From the ePolicy Orchestrator console, click **Menu** | **Systems** | **System Tree**.

2 Select the group containing the SVA.

3 Click **Assigned Policies**.

4 In the **Product** drop-down list, select **MOVE AV Agentless 3.6.0**.

5 In the **Actions** column of the currently applied policy, select **Edit Assignment**.

6 In the **Policy Assignments** page, change these settings:

- **Inherit from** — Select **Break inheritance** and assign the policy and settings below option.
- **Assigned Policy** — Select the policy that you created earlier from the **Assign Policy** drop-down list.

7 Click **Save**.

Test the installation

After completing the installation and configuration process, use this test to make sure that your VMs are protected.

Before you begin

- Make sure the policy is configured and has been delivered to the client before testing.
- The On-Access Scanner (OAS) must be enabled.

Task

For option definitions, click **?** in the interface.

1 From the client, attempt to download the EICAR test file from http://www.eicar.org/85-0-Download.html.

The file should be prevented from downloading.

2 From the ePolicy Orchestrator console, click **Menu** | **Systems** | **System Tree**.

3 Select the system from the list, then select **Actions** | **Agent** | **Wake Up Agents**.

Client events are sent to ePolicy Orchestrator.

4 View the **Threat Event Log**: click **Menu** | **Reporting** | **Threat Event Log**.

A new event is present, which indicates that malware was detected on the client.

See also

View the Threat Event Log on page 58

How quarantine works

McAfee MOVE AV (Agentless) implements a remote quarantine system, where quarantined files are stored on an administrator-specified network share.

In McAfee MOVE AV (Agentless) 2.6, the option for enabling **Quarantine configuration** and **Quarantine network share** were present under the **Scan** policy, however, the latter has now been moved to the **SVA** policy. This allows you to enable or disable quarantine for specific virtual machines. For details about assigning the **Scan** policy to specific virtual machines, see *How VM-based scan configuration works*.

The quarantine network share is mounted on the SVA during policy enforcement at `/mnt/quarantine` using the Common Internet File System (CIFS) protocol. If mounting fails, the **Quarantine Mount Failed** event is generated and mounting is attempted at the next policy enforcement.

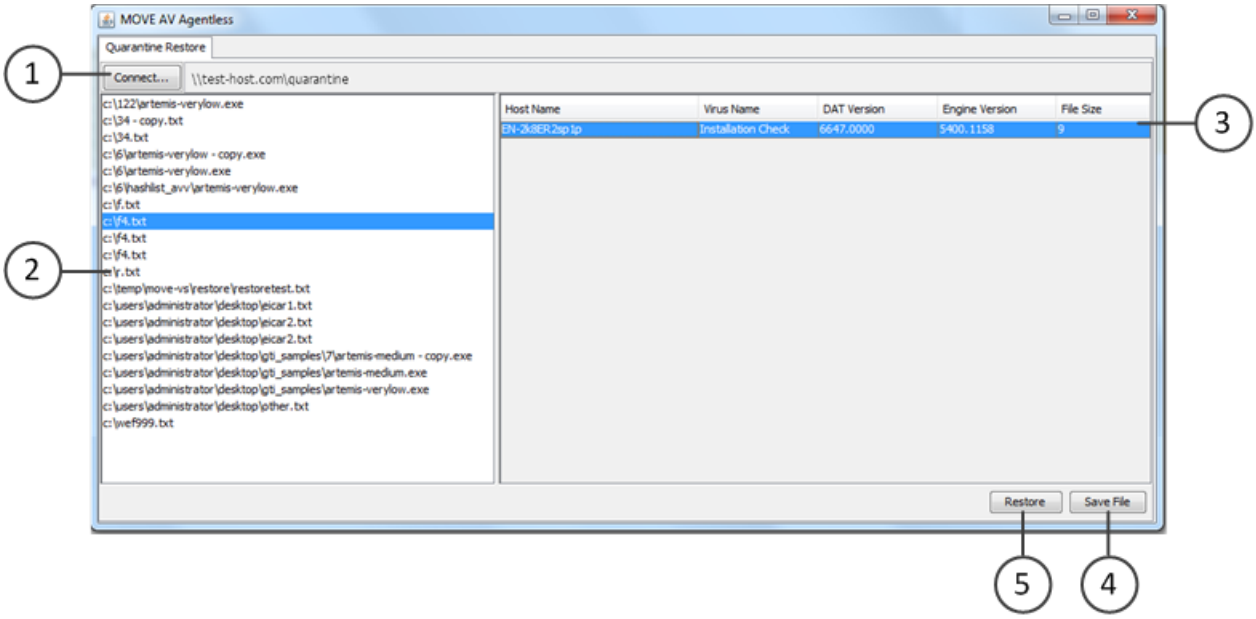
A file is quarantined when:

- The **Quarantine configuration** option, which is present under **Scan** policy, is enabled.
- The **Quarantine network share** configuration, which is present under the **SVA** policy, is mounted.
- A detection occurs.
- **Delete files automatically** is the primary action.

Quarantined files are automatically deleted after 28 days.

The restore tool at-a-glance

This diagram provides an overview of how the quarantine restore tool works.



The restore tool requires Java Runtime Environment (JRE) 1.6 or 1.7.

For JRE 1.7, you must modify `quarantine_restore.cmd` by adding `-Djava.net.preferIPv4Stack=true` to the JVMARGS variable.

1 Connect to a quarantine share.

2 View the list of quarantined files.

3 View the VMs corresponding to the selected file.

4 Save a file to your local system.

5 Restore a specific file to one or more selected VMs.

Restore a file

Restoring a quarantined file allows you to save to your local system or to a specific VM.

Before you begin

- Update the DATs on the SVA and the system where you run the restore.

  This is essential to successfully restore the file; otherwise the restored file is detected as a virus and deleted.

- Download **MOVE-AV-AL_RestoreTool.3.6.0.zip** from the McAfee download site and extract the contents.

The quarantine tool restores the guest VM files by accessing them via CIFS. The TCP Port 445 must be open on the guest VM's firewall before restoring the files.

Task

1 From the folder where you extracted **MOVE-AV-AL_RestoreTool.3.6.0.zip**, run `quarantine_restore.cmd` to launch the quarantine restore tool.

The **Connect** dialog box is automatically displayed.

2 Enter the location and credentials of the quarantine share, then click **OK**.

Use the **Connect** button to display the dialog and connect to another share.

3 From the list of quarantined files, select the file you want to restore.

The same file might be listed multiple times. This indicates that a file has been quarantined multiple times and the contents of the file are different.

4 Choose one of these two options:

To...	Do this...
Save the file to your local system	1 Select **Save File**. 2 Browse to the location, enter a file name, and click **OK**. The file is saved to the specified location. The quarantined file remains on the share.
Restore the file to selected VMs	1 Select the VMs where you want to restore the file, then click **Restore**. 2 Enter valid credentials to restore the file to all the selected VMs. The same file can be restored to multiple VMs by multi-selecting the VM hosts before you click **Restore**. The same credentials must be valid for all the selected VMs for this method to work. The file is restored to each selected VM. The quarantined file is removed from the share after it is successfully restored. When the restore is completed, the list of quarantined files and VMs are updated to reflect the current state.

The **RestoreTool.log** is where errors are logged.

Enabling the scan policy quarantine configuration

The **Quarantine** tab is located on the **Scan** policy page. Quarantine is only applicable if the on-access scan or on-demand scan primary action is Delete files automatically. If quarantine fails, the secondary action is applied.

Table 3-2 Quarantine settings

Settings	Description
Quarantine configuration	Enable or disable quarantine functionality.

Using the SVA policy quarantine settings

The **Quarantine settings** tab is located on the **SVA Policy** page. The malware that is detected on any virtual machine is quarantined only when you have enabled the **Quarantine configuration** option under **Scan policy**.

Table 3-3 Quarantine settings

Settings	Description
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. For details, see *Configure the quarantine folder*. Make sure that you enter the server name in a manner that can be resolved by the SVA. How this is entered depends on the environment and how the SVA is configured.
Network domain name	The domain used to access the specified share.
Network user name	The user name used to access the specified share.
Network password	The password used to access the specified share. After you save and re-open a scan policy, the network password appears blank. Even though it appears blank, it is saved in the policy settings. Click **Set password** to set/reset the password for the quarantine share.

See also

Configure the quarantine folder on page 53
Set permissions for shared folders on page 53

Configure the quarantine folder

You can limit access to the quarantine folder by configuring permissions.

Tasks

- *Set permissions for shared folders* on page 53
  Setting permission for the quarantine folder allows you to specify who has access to the share.

Set permissions for shared folders

Setting permission for the quarantine folder allows you to specify who has access to the share.

Before you begin

Create the following:

- Quarantine folder
- Domain User Account — The account used by the SVA to quarantine files.
- Domain Local Security Group — This group has access to the Restore Tool.

Task

1 Right-click the quarantine folder, then select **Properties**.

2 Select the **Sharing** tab and click **Advanced Sharing**

3 In the **Advanced Sharing** dialog box, select **Share this folder**, then change **Share name** to `quarantine$`. The `$` symbol hides the share.

4 Click **Permissions**, select the default user name **Everyone**, click **Remove**, then click **Apply**.

5 Click **Add** to select an object type.

You can give permission only to administrators who require access to the quarantine folder.

a In **Select Users or Groups**, enter your Domain User account in the **object names** dialog box, then click **OK**.

b Select the user name you created earlier, select **Full Control**, then click **OK**.

6 Click **Add** to select an object type.

a In **Select Users or Groups**, enter your Domain Local Security Group in the **object names** dialog box, then click **OK**.

b With this group selected, select **Full Control**, then click **OK**.

How VM-based scan configuration works

Using the **VM-based scan configuration** setting, the McAfee ePO administrator can enforce unique scan policies to different groups, resource pool, or specific virtual machines protected by MOVE-SVA on a hypervisor, even when McAfee Agent is not deployed to the client systems.

The **Scan** policy can be applied to SVA systems or to a specific virtual machine, or group. When you enable the **VM-based scan configuration** setting, all VMs are protected by the **Scan** policy, which is assigned to VM or group. However, when this is disabled, the **Scan** policy that is assigned to SVA is enforced to individual virtual machines.

The **Scan** policy can be assigned to the system using system-based assignment or rule-based assignment in McAfee ePO.

Enable the VM-based scan configuration setting

When you install the McAfee MOVE AntiVirus Agentless extension, the default **Scan** policy is assigned to the **My Organization** group, and the same is enforced to every VM under this group. However, to enforce a unique **Scan** policy to individual virtual machines or group, you need to assign the unique **Scan** policy to a specific VM or group, then enable the **VM-based scan configuration** option present under the **SVA** policy.

Before you begin

- Make sure that you have appropriate permissions to perform this task.
- Make sure that you installed the extensions for Data Center and Data Center Connector for vSphere.

Task

For option definitions, click **?** in the interface.

1 Create a new **SVA** policy or edit an existing **SVA** policy and assign it to the target SVAs. For details see *Create an SVA policy*.

2 In the **Scan Settings** tab of the **Policy Settings** page of the newly-created or edited policy, select **VM-based scan configuration** and click **Save**. The **VM-based scan configuration** setting is now active. These policies are enforced to SVA within the default policy collection interval, which is 60 minutes.

Follow these steps to run the policy collection immediately:

a Click **Menu** | **Configuration** | **Server Settings**, then click **MOVE AV [Agentless]** under **Setting Categories**.

b Click **Run**. The **Policy collection completed successfully** message appears on successful collection of the policies.

Enabling the **Policy collector** option periodically updates the target SVAs with the latest **Scan** policies. You can change the policy enforcement interval by navigating to **Menu** | **Configuration** | **Server Settings** | **Setting Categories** | **MOVE AV [Agentless]** | **Edit**. You can also view the task log for policy collection by navigating to **Menu** | **Automation** | **Server Task Log**.

c Send an agent wake-up call to the target SVAs.

Scan diagnosis

You can run the scan diagnostic tool or use McAfee ePO to calculate and display frequently scanning files, extensions, and VMs, so that you can include these results in the path exclusion policies to exclude them from being scanned.

Create and run a scan diagnostic client task using McAfee ePO

Select an SVA or a group of SVA from the System Tree and assign a client task to calculate and display frequently scanning files, extensions, and VMs, so that you can include these results in the path exclusion policies to exclude them from being scanned.

Before you begin

Make sure that you have installed the MOVE AV (Agentless) 3.6.0 extension.

Task

For option definitions, click **?** in the interface.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Select **Menu** | **Policy** | **Client Task Catalog** .

3 From **Client Task Types**, select **MOVE AV [Agentless] 3.6.0** | **Scan Diagnostics**.

4 Click the name of an existing client task or click **New Task** and confirm the task type.

5 Configure these settings on each tab and click **Save**.

Tab	Description
Task Name	Specifies a unique user-friendly name for the task.
Description	Specifies some user-friendly description about the task.
Diagnosis Time	Specifies the time period, in minutes, set for calculating the frequently scanned files. for example 1-10 minutes.

6 Click **Assign**, specify the SVA where you want to assign the task, then click **OK**.

7 Click **2 Schedule** to schedule the task. At the end of specified minutes, the McAfee ePO completes the analysis and displays the results. The default allowed time limit is 10 minutes.

8 Click **Menu** | **Reporting** | **Queries & Reports** and select **MOVE AV [Agentless]** under **McAfee Groups** to view and run these scan diagnostic queries:

- **MOVE AV [Agentless]: Top 10 Scanned File Extensions for each SVA** — Lists the top 10 file extensions scanned by the SVA.
- **MOVE AV [Agentless]: Top 10 Scanned Files for each SVA** — Lists the top 10 files scanned by the SVA.
- **MOVE AV [Agentless]: Top 10 Scanned Virtual Machines for each SVA** — Lists the top 10 virtual machines that are sending maximum scan and checksum request.

Run the scan diagnostic tool using command line

Use the scan diagnostic tool to calculate and display frequently scanning files, extensions, and VMs, so that you can include these results in the path exclusion policies to exclude them from being scanned.

Before you begin

Make sure that the user is a root user, or has sudo permissions.

Access the command-line interface (CLI) of the SVA to create and display this report.

Task

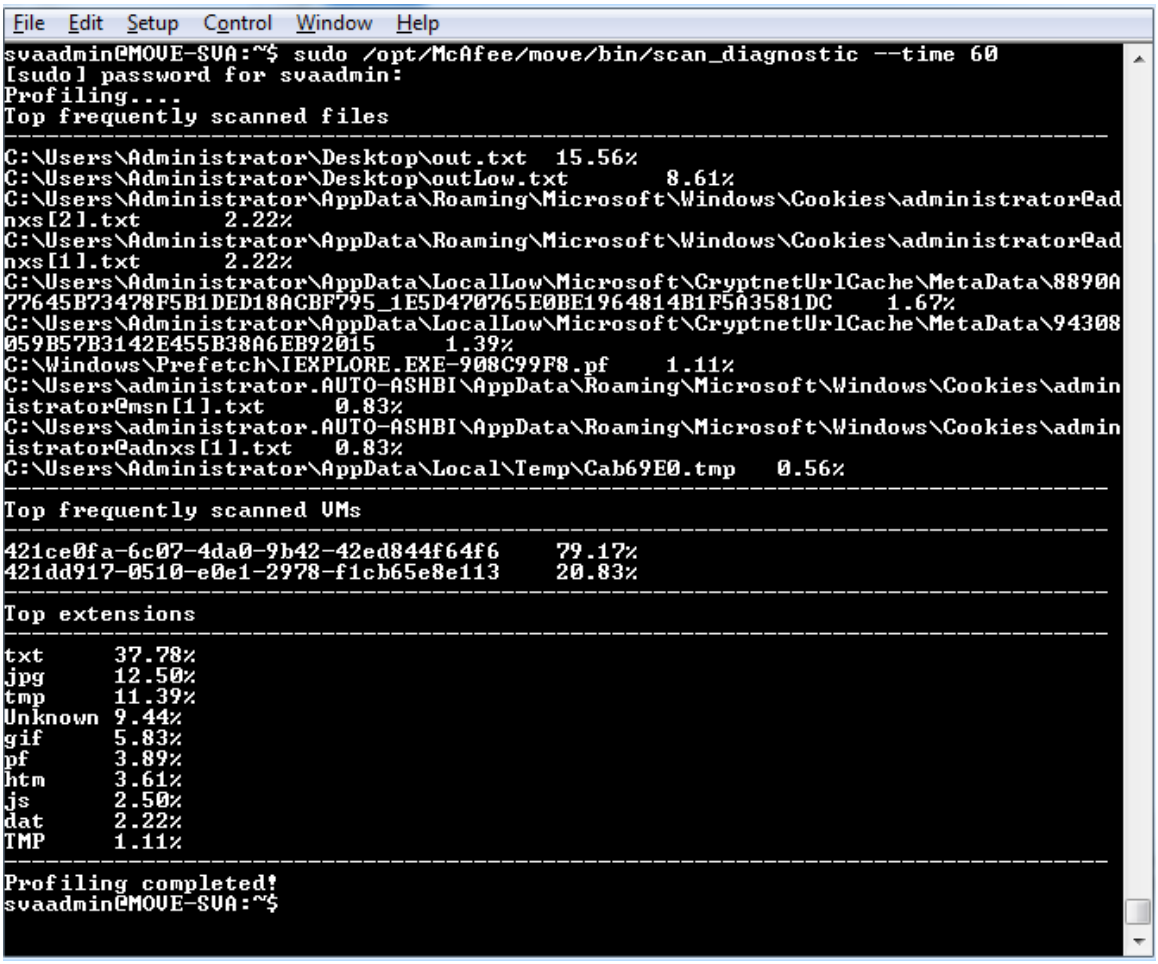
To list the available Help options, run the tool with the "--help" option.

- To calculate the frequently scanned files, run the command: `>cd /opt/McAfee/move/bin>sudo ./scan_diagnostic` or `sudo /opt/McAfee/move/bin/scan_diagnostic` .

  These parameters are available:

  - `--help` — Shows how to use the command and its options.
  - `--time arg` — Specifies the time period, in seconds, set for calculating the frequently scanned files. For example 60 seconds.
  - `--elements arg` — Specifies the number of entries to be captured and displayed in the result.
  - `--path arg` — Specifies the output folder path. The default path is `/opt/McAfee/move/log`.

At the end of specified minutes, the tool completes the analysis and displays the results. The default allowed time limit is 1 minute.



You can also change the time limit by editing the `svaconfig.xml` file present at `/opt/McAfee/move/etc/`.

To stop the scan diagnostic tool while it is collecting the data, use the `Ctrl+C` keys.

This diagnostic tool captures these details:

- Top 10 file scan requests
- Top 10 file extensions
- Top 10 virtual machines that are sending maximum scan and checksum request.

The name of the VM is resolved only when the vCenter is successfully registered in the Scan policy using McAfee ePO. Otherwise, only the VM ID appears.

Monitoring the SVA

Monitor the status of the SVA using the Threat Event Log in ePolicy Orchestrator, or the Health and Alarms feature in VMware vShield Endpoint.

View the Threat Event Log

Use the Threat Event Log to quickly view and sort through events in the database. You can choose which columns are displayed in the sortable table. Depending on which products you are managing, you can also take certain actions on the events.

Task

For option definitions, click **?** in the interface.

1. From the ePolicy Orchestrator console, click **Menu** | **Reporting** | **Threat Event Log**.
2. Click any of the column titles to sort the events. You can also click **Actions** | **Choose Columns**.
3. From the **Available Columns** drop-down list, select table columns as needed, then click **Save**.
4. Select events in the table, then click **Actions** and select **Show Related Systems** to see the details for the systems that sent the selected events.

View the Health and Alarms page

Check the status of the SVA from the **Health and Alarms** page.

Task

1. From the vSphere Client, select **Inventory** | **Hosts and Clusters**.
2. From the resource tree, select a data center, cluster, or ESXi host resource.
3. Click the **vShield** tab.
4. Click **Endpoint**.

   The vShield Endpoint Health and Alarms page displays the status of the items.

Queries and reports

Use ePolicy Orchestrator queries to view events, run default queries, and create reports.

- View events in the Threat Event Log.
- Run default queries that show important client information.
- Create reports using data sent by the McAfee Agent to the ePolicy Orchestrator database.

For information on how to run a query or report, see the ePolicy Orchestrator product guide.

Queries are questions that you ask ePolicy Orchestrator, which returns answers as charts and tables. You can export, download, combine queries into reports, and use most queries as dashboard monitors.

You can use predefined queries as is, edit predefined queries, or create queries from events and properties stored in the ePolicy Orchestrator database. To create custom queries, your assigned permission set must include the ability to create and edit private queries.

Reports enable you to package one or more queries into a single PDF document, for access outside of ePolicy Orchestrator.

To create reports, your assigned permission set must include the ability to create and edit reports. You can restrict access to reports using groups and permission sets exactly as you restrict access to queries. Reports and queries can use the same groups, and because reports primarily consist of queries, this allows for consistent access control.

McAfee Agent isn't installed on each VM. Only the SVA appears in the ePolicy Orchestrator console, which means you don't see each VM. vShield Manger provides a report that validates the protection status of each VM.

McAfee MOVE AV Agentless provides the following predefined queries:

Query	Description
MOVE AV Agentless: Computers with Threats Detected per Week	MOVE AV Agentless: Threats Detected Over the Previous 2 Quarters
MOVE AV Agentless: Detection Response Summary	MOVE AV Agentless: Threats Detected per Week
MOVE AV Agentless: Summary of Threats Detected in the Last 24 Hours	MOVE AV Agentless: Top 10 Computers with the Most Detections
MOVE AV Agentless: Summary of Threats Detected in the Last 7 Days	MOVE AV Agentless: Top 10 Detected Threats
MOVE AV Agentless: Threat Count by Severity	MOVE AV Agentless: Top 10 Threats per Threat Category
MOVE AV Agentless: Threat Names Detected per Week	MOVE AV Agentless: Unwanted Programs Detected in the Last 24 Hours
MOVE AV Agentless: Threats Detected in the Last 24 Hours	MOVE AV Agentless: Unwanted Programs Detected in the Last 7 Days
MOVE AV Agentless: Threats detected in the Last 7 Days	

4 Managing the SVAs

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

Review this list before unregistering the existing SVA and deploying the new SVA in your environment.

- The 3.6.0 ePolicy Orchestrator extension upgrades the 3.5.x extension. The ePolicy Orchestrator server can manage both versions simultaneously.
- You can migrate policies you created with earlier versions of McAfee MOVE AV (Agentless) using a server task that is available after installing the new extension.
- Quarantine settings and policy assignments are not migrated. Quarantine settings need to be redefined after migration and policies need to be reassigned.
- You must import the SVA IP query file to McAfee ePO and download the output file (.CSV), so that it can be used for unregistering the SVAs.

See also

Deploy a new SVA manually on page 65

Contents

Import the SVA IP query file

You must import the SVA IP query file to the McAfee ePO server, so that you can download the CSV file, which is required for unregistering the SVA.

Before you begin

- Download `MOVE-AV-AL_SVA_Deployment_3.6.0.zip` from the McAfee download site and extract the contents.

Task

For option definitions, click **?** in the interface.

1. Log on to McAfee ePO as an administrator.
2. Click **Menu** | **Queries and Reports** | **Actions** | **Import Definitions** to open the **Import Queries** page.
3. Click **Choose File** to browse and select the `MOVE_AV_Query_SVA_IPs.xml` file from the folder where you extracted `MOVE-AV-AL_SVA_Deployment_3.6.0.zip`.
4. Under **Group**, create a group or select an existing group, then click **Save** to open the **Import Queries** page.
5. Click **OK**.
6. From the **Query** tab, select the group and click **Run** from the **MOVE_AV_Query_SVA_IPs** query to open the **MOVE_AV_Query_SVA_IPs** page.
7. Click **Actions** | **Export Table**. The **Export** page appears.
8. Select the CSV format of the exported file, then click **Export**.
9. From the **Export** page, click the link to open the file, or right-click the link to download and save the file.
10. Copy the CSV file to the folder where you extracted `MOVE-AV-AL_SVA_Deployment_3.6.0.zip`.

Unregister the SVAs from vCloud Networking and Security Manager

Before upgrading the SVA, you must unregister the existing SVA from the vCloud Networking and Security Manager.

Before you begin

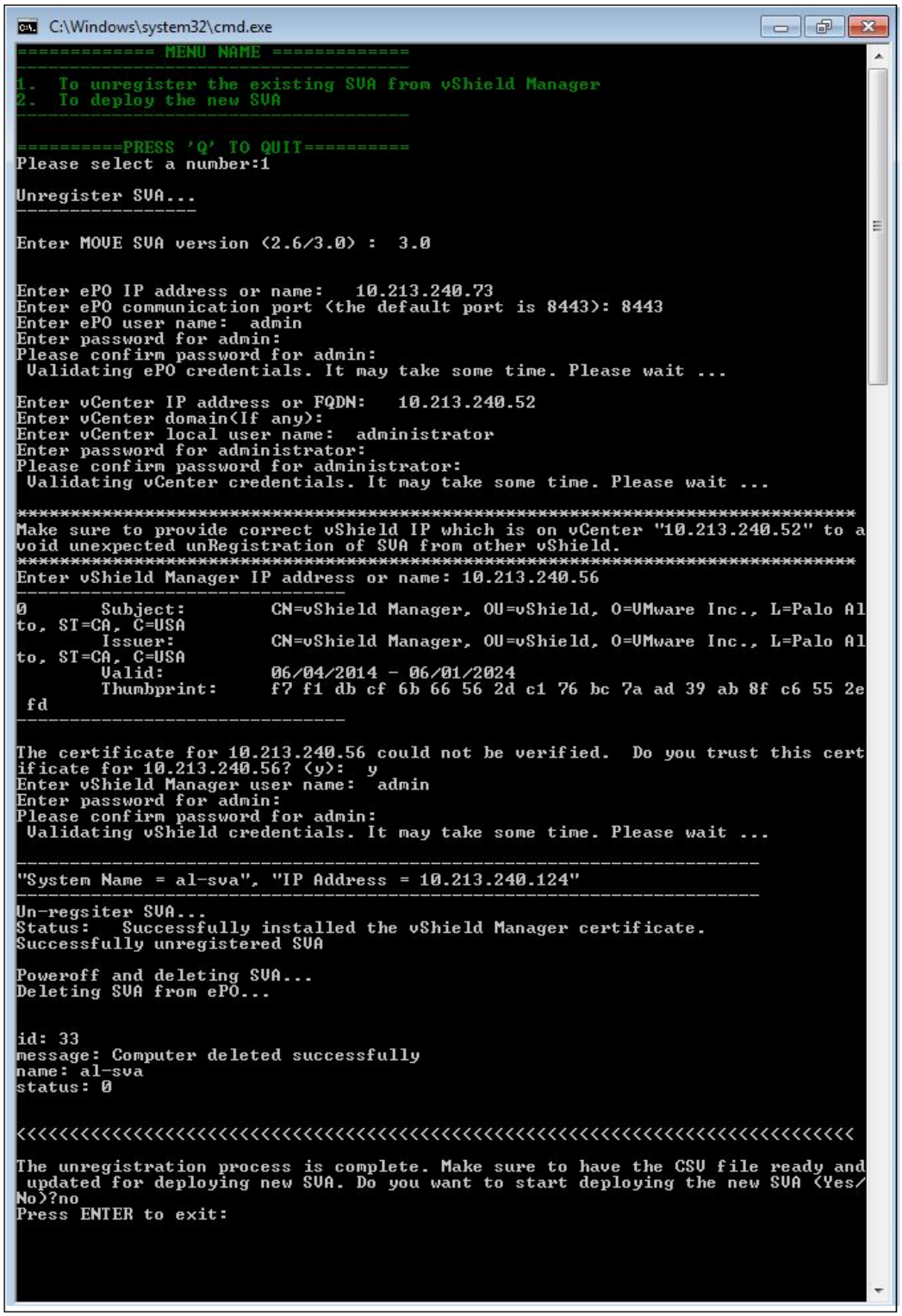
- Download `MOVE-AV-AL_SVA_Deployment_3.6.0.zip` from the McAfee download site and extract the contents.
- Make sure that you imported the SVA IP query file `MOVE_AV_Query_SVA_IPs.xml` to the McAfee ePO server and downloaded the `MOVE_AV_Query_SVA_IPs.csv` file.

Task

1 Gather this information, which you need to run the unregister script:

ePolicy Orchestrator	Server IP address and port User name and password
	You must have a valid ePolicy Orchestrator user name that uses ePolicy Orchestrator authentication.
vCenter	IP address or DNS name User name and password
vCloud Networking and Security Manager	IP address or DNS name User name and password

2 From the folder where you extracted `MOVE-AV-AL_SVA_Deployment_3.6.0.zip`, run `launch.bat` to start the command prompt.



3 Enter `1` to unregister the existing SVA from the selected vCloud Networking and Security Manager.

You can enter `2` to deploy the new SVA. For details about deploying the SVA, see *Setting up the SVA*.

4 Enter the MOVE SVA version `3.5.0` or `3.5.1`.

5 Follow the prompts and answer the questions as they apply to your environment.

Make sure that you provide the IP address of the correct vCloud Networking and Security Manager on a vCenter, so that the correct target SVA is unregistered.

The script parses the CSV file and unregisters the SVA.

Upgrade the extension

Version 3.6.0 of the McAfee MOVE AV (Agentless) extension upgrades the 3.5.x extension.

Before you begin

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

Task

For option definitions, click **?** in the interface.

1 From the ePolicy Orchestrator console, click **Menu** | **Software** | **Extensions**.

2 When the **Extensions** page opens, click **Install Extension**.

3 Browse to and select the MOVE-AV-AL_EXT_3.6.0.zip file, then click **OK**.

4 After a confirmation message, click **OK**.

5 Browse to and select the MOVE-AV-AL_License_EXT_3.6.0.zip file, then click **OK**.

6 After a confirmation message, click **OK**.

All policies created in version 3.5.x exist after you upgrade to version 3.6.0.

Deploy a new SVA manually

You must unregister the 3.5.x SVA before deploying the new 3.6.0 SVA.

Task

1 From the Software Manager or the McAfee download site, download **MOVE-AV-AL_OVF_3.6.0.zip**.

2 Log on to the existing SVA.

3 Run **sudo /opt/McAfee/move/bin/sva-config**.

4 Enter `Yes` to register or unregister this SVA with vCloud Networking and Security Manager.

5 Enter `u` to unregister.

6 Turn off the SVA.

> Do not delete this SVA until the 3.6.0 version is successfully deployed. This SVA can be used to help troubleshoot deployment issues.

7 Deploy a new SVA to the hypervisor.

For details about other methods to deploy the SVA, see *Setting up the SVA*.

Assign a policy

Assign a policy to a specific group of the System Tree. You can assign policies before or after a product is deployed.

Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Systems** | **System Tree** | **Assigned Policies**, then select **MOVE AV [Agentless] 3.6.0**.

Each assigned policy per category appears in the details pane.

2 Locate the policy category that you want, then click **Edit Assignment**.

3 If the policy is inherited, select **Break inheritance and assign the policy and settings below** next to **Inherited from**.

4 Select a policy from the **Assigned policy** drop-down list.

> From this location, you can also edit the selected policy's settings, or create a new policy.

5 Choose whether to lock policy inheritance.

Locking policy inheritance prevents any systems that inherit this policy from having another one assigned in its place.

6 Click **Save**.

Upgrade the SVA using NSX Manager

Follow these steps to upgrade version 3.5 SVA to version 3.6 SVA if you have used McAfee ePO and VMware vCenter Web Client to configure the SVA with VMware NSX Manager and deploy it to one or more clusters.

Before you begin

- The MOVE SVA must be registered with VMware NSX Manager.
- The McAfee MOVE AV (Agentless) extension is installed on the McAfee ePO server.

Task

For option definitions, click **?** in the interface.

1 Log on to the VMware vCenter Web Client as an administrator.

2 Click **Networking & Security** | **Installation** | **Service Deployments** to open the **Networking & Security Service Deployment** page.

3 Delete the version 3.5 SVA from the cluster in the vCenter.

4 Remove all McAfee MOVE AV policy from Security policies in the VMware vCenter Web Client console.

5 Unregister the registered NSX Manager using McAfee ePO.

   a Log on to the McAfee ePO server as an administrator.

   b Click **Menu** | **Configuration** | **MOVE Service Registration**. This action lists all NSX Managers registered in McAfee ePO.

   c Click the **Unregister** link next to the registered NSX Manager.

6 Delete the existing SVA package from McAfee ePO.

   a Log on to the McAfee ePO server as an administrator.

   b Click **Menu** | **Configuration** | **MOVE repository** to open the **MOVE SVA repository configuration** page.

   c From **Actions**, click **Delete** to remove an existing SVA from McAfee ePO as it is not registered with NSX Manager. For details, see *Check in the SVA package to McAfee ePO*.

7 Install the McAfee MOVE AV (Agentless) 3.6.0 extension. For details, see *Upgrade the extension.*

8 Check in the version 3.6 SVA package to McAfee ePO. For details, see *Check in the SVA package to McAfee ePO*.

9 Register the version 3.6 SVA with VMware NSX Manager.

10 Deploy the version 3.6 SVA using VMware NSX Manager. For more information, see *VMware NSX Manager-based deployment*.

A SVA security requirements

The following security measures are implemented on the SVA.

Security measure	Description
apparmor	apparmor is a kernel module that envelops processes and limits their system access to predefined items as defined in their profile. The MOVE scanning process, mvsvc, contains this profile: `/etc/apparmor.d/opt.McAfee.move.bin.mvsvc`. There are two apparmor modes: **complain** and **enforce**. By default, mvsvc is in enforce mode. You can change the mode to **complain** with the `aa-complain mvsvc` command. To enable enforce mode, use the `aa-enforce mvsvc` command. While in **complain** mode, you can use the command `aa-logprof` to analyze any requests that the process has made outside of its profile. For more information, visit this website: https://help.ubuntu.com/12.04/serverguide/apparmor.html
iptables	The sva-firewalls script enables the built-in firewall. Usage is sva-firewalls: **start** | **stop** | **restart**. By default, the firewall rules allow: • TCP port 22 (SSH) • TCP port 8081 (McAfee Agent default port) • UDP 67, 68 (DHCP) The script name is sva-firewall. It is located at `etc/init.d/` and starts automatically.

SVA .vmx configuration file settings	Add these options to harden the SVA from a VM perspective:
	`isolation.tools.diskWiper.disable=TRUE`
	`isolation.tools.diskShrink.disable=TRUE`
	`isolation.device.connectable.disable=TRUE`
	`isolation.device.edit.disable=TRUE`
	`RemoteDisplay.maxConnections=1`
	`vmci0.unrestricted=FALSE`
	`log.rotateSize=1000000`
	`log.keepOld=10`
	
	For more information, visit this website: http://www.vmware.com/security/hardening-guides

Index

O

P

Q

R

S

T

U

V