Product Guide

McAfee MOVE AntiVirus 3.0.0

For use with ePolicy Orchestrator 4.6.0, 5.0.0 Software

Contents

Preface

Contents

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.

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

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

Task

1 Go to the McAfee Technical Support ServicePortal at http://mysupport.mcafee.com.

2 Under **Self Service**, access the type of information you need:

To access...	Do this...
User documentation	1 Click **Product Documentation**. 2 Select a product, then select a version. 3 Select a product document.
KnowledgeBase	• Click **Search the KnowledgeBase** for answers to your product questions. • Click **Browse the KnowledgeBase** for articles listed by product and version.

1 Introduction to McAfee® MOVE AntiVirus Agentless

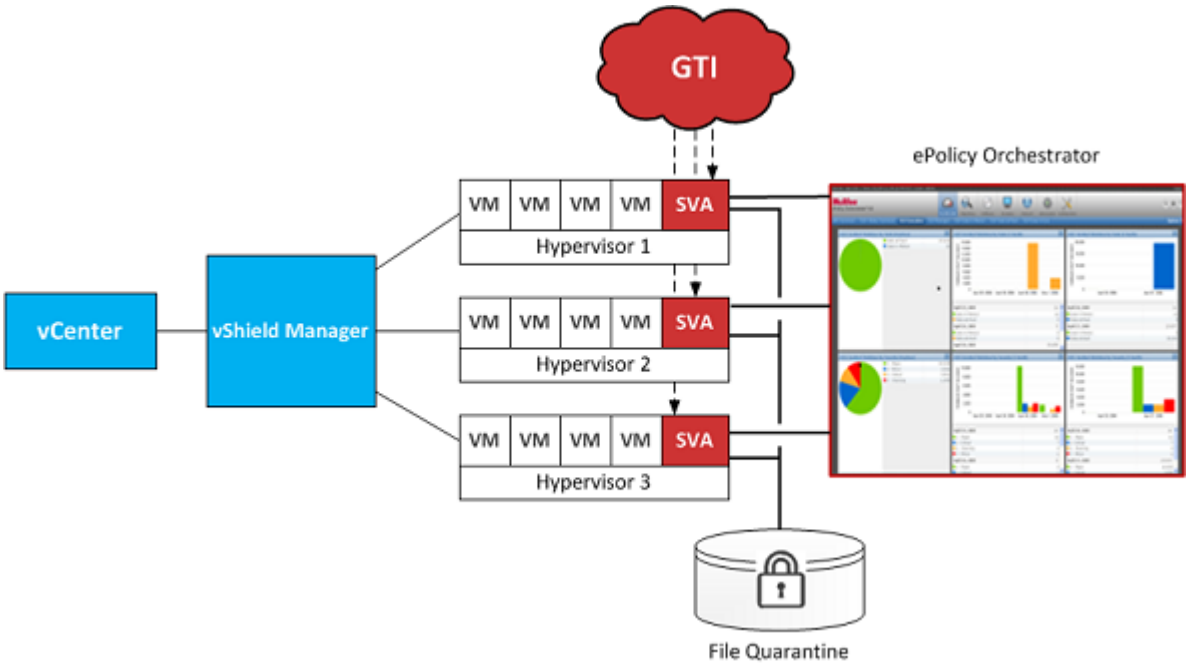
McAfee® MOVE AntiVirus Agentless provides virus protection for virtual machines (VMs) and contains a Security Virtual Appliance (SVA) delivered as an Open Virtualization Format (OVF) package.

The Agentless deployment option:

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

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.

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.

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* are embedded hypervisors for servers that run directly on server hardware without requiring an additional underlying operating system.

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, but you can install the McAfee Agent and other McAfee products on the VMs. McAfee® VirusScan® Enterprise for Linux, McAfee Agent 4.6, and McAfee MOVE AV Agentless comes pre-installed.

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

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

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

2 Installation and configuration

To set up your environment for McAfee 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 your environment includes these components, and that they meet these requirements.

Software requirements

For optimal product reliability, performance and security in vShield Endpoint we highly recommend that you install the VMware ESXi 5.0 patch (ESXi500-201204001.zip) dated 4/12/2012, which is available from this portal: http://www.vmware.com/patchmgr/download.portal

- ePolicy Orchestrator 4.6 Patch 2 and later
- Security Virtual Appliance (SVA)
- VMware ESXi 4.1 Patch 3 (Optional)
- VMware ESXi 5.0, 5.1 (Optional)

  Patch ESXi500-201109402-BG: Updates tools-light

  Patch ESXi500-201109401-BG: Updates esx-base

- VMware vCenter 5.0, 5.1
- VMware vShield Manager 5.0, 5.1
- VMware vShield Endpoint 5.0, 5.1
- VMware vSphere Client 5.0, 5.1

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

SVA requirements

You must use the virtual machine we provide. This 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 VM must meet these minimum 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 10.4
Software	VirusScan Enterprise for Linux McAfee Agent 4.8 McAfee MOVE AV Agentless

Guest VM operating system requirements

- VMware Tools 5.0 (Patch 1 ESX500-201109402-BG)
- For information on 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

Download the McAfee MOVE AV Agentless packages

You must download these packages before they can be installed onto virtual systems or into ePolicy Orchestrator.

The OVF package and ePolicy Orchestrator extension 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_3.0.0.zip`)
- McAfee MOVE AV Agentless extension for ePolicy Orchestrator

Extension	Name
Main product extension	`MOVE-AV-AL_EXT_3.0.0.zip`
License extension	`MOVE-AV-AL_License_EXT_3.0.0.zip`

- McAfee MOVE AV Agentless help extension (`MOVE-AV_HELP_3.0.0.zip`)
- McAfee MOVE AV Agentless documentation package (`MOV-AV_DOCS_3.0.0.zip`)
- McAfee MOVE AV Agentless restore tool (`MOVE-AV-AL_RestoreTool_3.0.0.zip`)

- McAfee MOVE AV Agentless multiple OVF deployment tool (`MOVE-AV-AL_DeploySVA_3.0.0.zip`)
- McAfee MOVE AV Agentless ePolicy Orchestrator package (`MOVE-AV-AL_SVA_3.0.0.zip`)

If you have installed the ePolicy Orchestrator server 4.6.x using McAfee® Endpoint Advanced Suite Installer (McAfee EASI), these extensions are already installed and ready for use in McAfee ePO.

Install VMware vShield Endpoint

You must install vShield Manager (vShield 5.0, 5.1) on your virtual environment before you can install and configure the software.

If using ESX 4.1 make sure you upgrade the VMware Tools ISO image in ESXi 4.1. This ensures that a new VMware Tools installation on Windows virtual machines can support agentless protection.

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

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

Task

1. Install ESXi.
2. Install and configure vShield Manager.
3. Add component and vShield Endpoint licenses in vCenter.
4. Install vShield Endpoint on the hypervisor(s).
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 9

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 two deployment options: multiple OVF deployment and manual deployment. There are two configuration options: automatic configuration and manual configuration.

These are the deployment options:

- **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.

  This is the only option that supports clustered environments. This option also works for non-clustered environments.

- **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.

Deploy multiple OVFs

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

Before you begin

- From the McAfee download site, download and extract the contents of **MOVE-AV-AL_OVF_3.0.0.zip**.
- Install Java, Perl, and VMware OVF Tool on the system where you are running the deployment.
- VMware vShield Endpoint must be installed on the host or hypervisor.
- You must disable vMotion on the SVA. You can host the SVA on the hypervisor's local disk to avoid using vMotion.

Task

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

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

SVA	IP address
vShield 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 will result in failure to deploy the SVA.

This account must be a local admin account on the vCenter server (not a domain account).

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_DeploySVA_3.0.0.zip** file and open the CSV file.

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

4 Save the CSV file, then run the **deploySVA.pl** script.

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

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

6 Power on the VM.

CSV file properties

If you deploy the OVF from the Perl Deployment package, then you must fill out a CSV file containing the SVA configuration information. We provide a CSV file template that contains these columns. Refer to the associated OVF property for more 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 you deploy the OVF to 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 is used by the McAfee ePO server 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
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. This option doesn't support clustered deployments.

Before you begin

- From the McAfee download site, download and extract the contents of the **MOVE-AV-AL_OVF_3.0.0.zip**. If you have installed the ePolicy Orchestrator server 4.6.x using McAfee® Endpoint Advanced Suite Installer (McAfee EASI), go to the **postInstall** directory in the unzipped package of EASI_DataCenter and extract the contents of the **MOVE-AV-AL_OVF_3.0.0.zip**.
- VMware vShield Endpoint must be installed on the hypervisor.
- Make sure that vMotion will not move the SVA from the selected hypervisor.

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.

The vSphere Client must be connected to a vCenter server to successfully deploy the OVF.

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 desired disk provisioning.
Network Mapping	Map the OVF networks to the existing networks on the selected hypervisor. 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.
Properties	If you specify the configuration information on 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.
Ready to Complete	Review the options you selected.

3 Click **Finish**.

Configuring the SVA

These are the available configuration options.

- If you choose the Multiple OVF Deployment option or provide the configuration information on the **Properties** page during manual deployment, the SVA is automatically configured.
- If you choose the Manual Deployment option and don't provide the configuration information on the **Properties** page, you must manually configure the SVA.

The MOVE AV Agentless Security Virtual Appliance (SVA) OVF (Open Virtualization Format) template has a pre-configured 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.

To reconfigure the Time Zone, DATE and Time for your local time, follow these steps:

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

2 Run this command:

```
sudo dpkg-reconfigure tzdata
```

3 Type your password, when prompted.

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

To configure the DATE and TIME, follow these steps:

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

2 Run this command:

```
sudo date -s "16 APR 2012 16:05:00"
```

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

3 Type your password, when prompted.

Manually configure the SVA

The first time you log on, the configuration script automatically runs. If you chose to provide the configuration information in the **Properties** setting and it isn't showing up in ePolicy Orchestrator, you must log on to the SVA and follow this task.

Before you begin

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

SVA	IP address
vShield 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.

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

Task

1 Power 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.

In some heavy load conditions, the default SVA configuration might be insufficient. If so, you can modify certain configuration parameters in the SVA configuration file. For details, see the KnowledgeBase article:

https://kc.mcafee.com/corporate/index?page=content&id=KB78947.

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	Username	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 need to enter any other network settings. The DNS servers must be automatically discovered. Any DNS servers specified overwrites the automatically discovered DNS servers.
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 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.
SVA	Hostname	The hostname of the SVA.
SVA	savaadmin Password	The password of the svaadmin account.
vShield Manager	IP Address	The IP address or DNS name of the vShield Manager.
vShield Manager	Password	The password used to register the SVA with the vShield Manager.
vShield Manager	Username	The username used to register the SVA with the vShield Manager.
* This is only applicable when the **Network Type** is **static**.		

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_3.0.0.zip`
License extension	`MOVE-AV-AL_License_EXT_3.0.0.zip`

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

Install the VirusScan Enterprise for Linux extension

You only need to install this extension if you want to manage the VirusScan Enterprise for Linux policy on the SVA. If you want to use the default settings you can don't need to perform this task.

VirusScan for Linux is only licensed for use on the SVA., and is not licensed for use in 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 Install these extensions:

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

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

Do this for each of these extensions:

Extension	File
McAfee Agent	**EPOAGENTMETA.ZIP**
McAfee VirusScan for Linux	**LYNXSHLD1900.ZIP**
McAfee VirusScan for Linux reports	**LYNXSHLD1900PARSER.ZIP**

3 Monitoring and managing

The Agentless deployment option monitors the status of virtual desktops and modifies 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 3.0.0**.
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 re-open 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.

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 are 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, select **Menu** | **Policy** | **Policy Catalog**.

2 From the **Product** drop-down list, select **MOVE AV Agentless 3.0.0**.

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 the settings to control which files are scanned.

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.

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

Wildcards are supported, however, environment variables aren't supported.

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 25

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 3.0.0**.
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 your VMs are protected.

Before you begin

- Make sure the policy is configured and has been delivered to the client prior to 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 29

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 machine. For details on assigning the **Scan** policy to specific virtual machine, 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.

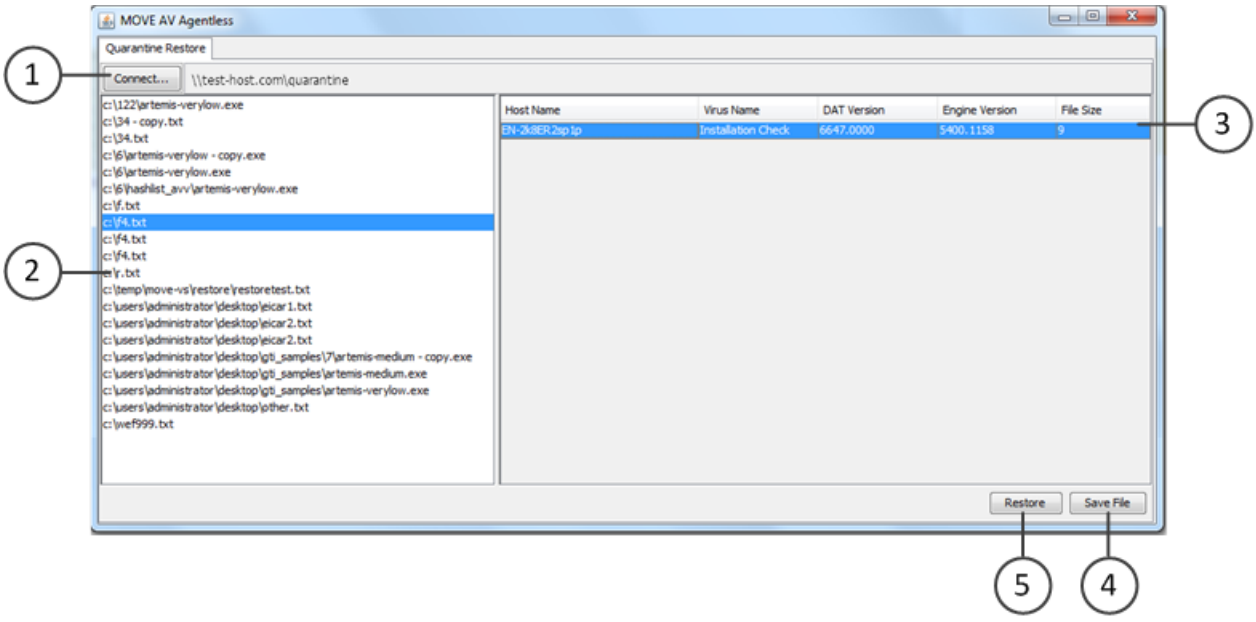
A file is quarantined when:

- 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.3.0.0.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.3.0.0.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 desired location, enter a file name, and click **OK**. The file is saved to the specified location. The quarantine file remains on the share.
Restore the file to selected VMs	1 Select the VMs that you want to restore the file to and 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 3-1 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 3-2 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 more 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 is dependent 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 26
Set permissions for shared folders on page 26
Set permissions for shared files on page 26

Configure the quarantine folder

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

Tasks

- *Set permissions for shared folders* on page 26
  Setting permission for the quarantine folder allows you to specify who has access to the share.
- *Set permissions for shared files* on page 26
  Setting permission for shared files allows you to limit the permissions of those who can access 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**.

Set permissions for shared files

Setting permission for shared files allows you to limit the permissions of those who can access 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, select **Properties**, then click the **Security** tab.

2 Click **Edit**.

a Select and remove the users group.

You must prevent the folder from inheriting permissions to successfully remove the group.

b Click **Add**, enter the Domain User account, then click **OK**.

This is the account the SVA uses to store quarantined files.

c Click **Add**, enter the name of the Local Security Group you created earlier, then click **OK**.

3 Close the dialog box and right-click the folder to open it's Properties page.

4 Click the **Security** tab, **Advanced** | **Change Permissions**, then select the Domain Local User account used by the SVA to store quarantined files, then click **Edit**.

5 Select **This folder, subfolders and files**.

6 Select all the available permissions except **Change permissions** and **Take ownership**, then click **OK**.

7 Deselect **Include inheritable permissions** from this object's parent, then select **Add**.

8 Select the Domain Local Security group of users with rights to restore quarantined files, then click **Edit**.

9 From the **Apply** drop-down list in the Permission Entry dialog box:

a Select **This folder, subfolder, and files**.

b Select these permissions:

- **Traverse folder/execute file**
- **List folder/read data**
- **Read attributes**
- **Read extended attributes**
- **Delete subfolders and files**
- **Delete**
- **Read permissions**

10 Click **OK**, then click **Close**.

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

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 SVA(s). 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 if you want to run the policy collection immediately:

   1. Click **Menu** | **Configuration** | **Server Settings**, then click **MOVE AV [Agentless]** under **Setting Categories**.
   2. Click **Run**. The **Policy collection completed successfully** message appears on successful collection of the policies.

      Enabling the **Policy collector** option periodically updates the target SVA(s) 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**.

   3. Send an agent wake-up call to the target SVA(s).

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 datacenter, 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 Upgrade McAfee MOVE AV Agentless

There are two approaches for upgrading McAfee MOVE AV Agentless, you can deploy a new SVA or upgrade an existing SVA. You must perform these upgrade steps in a specific order to successfully upgrade the software.

- **Deploy a new SVA** — This approach requires you to unregister an existing 2.6 SVA, then deploy the 3.0 SVA to the hypervisor. This option ensures that you have the latest security updates.
- **Upgrade an existing SVA** — This approach upgrades McAfee MOVE AV Agentless on the existing 2.6 SVA with an ePolicy Orchestrator deployable package, and results in a short non-protection window for the protected VMS on the hypervisor.

Review this list before upgrading your environment.

- The 3.0 ePolicy Orchestrator extension doesn't upgrade the 2.6 extension. Both extensions can simultaneously reside within ePolicy Orchestrator.
- 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.

See also

Deploy a new SVA on page 32
Upgrade an existing SVA on page 33

Contents

Install the extension

Version 3.0 of the McAfee MOVE AV Agentless ePolicy Orchestrator extension can coexist with the 2.6 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_3.0.0.zip file, then click **OK**.

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

Migrate existing policies

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.

Before you begin
The McAfee MOVE AV Agentless extension version 3.0 must be installed before migrating policies.

Quarantine settings and policy assignments are not migrated. Quarantine settings need to be redefined after migration and policies need to be reassigned.

Task

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

1 Open the Server Tasks page: click **Menu** | **Automation** | **Server Tasks**.

2 Select the task named **MOVE AV [Agentless]: Migrate Policy from MOVE-AV 2.6 [Agentless] to MOVE AV [Agentless] 3.0**.

3 In the **Actions** column, click **Run**.

4 Open the **Server Task Log**: click **Menu** | **Automation** | **Server Task Log**.

5 Verify the task finished.

6 If failures are reported in the **Server Task Log**, take corrective action and run this task again.

If version 3.0 policies exist with the same name as version 2.6 policies, the migration server task will skip the duplicate name policies and migrate the remaining policies.

Deploy a new SVA

You must unregister the 2.6 SVA before deploying the new 3.0 SVA.

Task

1 From the Software Manager or the McAfee download site, download **MOVE-AV-AL_OVF_3.0.0.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 vShield Manager.

5 Enter `u` to unregister.

6 Power off the SVA.

Do not delete this SVA until the 3.0 version is successfully deployed. This SVA can be used to help troubleshoot deployment issues.

7 Deploy a new SVA to the hypervisor.

Upgrade an existing SVA

This upgrade approach does not require creating an additional SVA, and can create a short window of time when virtual machines are unprotected. In most environments, we recommend you perform this upgrade during scheduled downtime.

Task

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

Package name	Description
`MOVEAVAgentless.3.0.0.163-SVA`	ePolicy Orchestrator package
`EPOAGENTMETA.zip`	McAfee Agent package

Upgrading McAfee VirusScan for Linux and McAfee Agent are not required, but new versions are available. If you're interested in upgrading, see *McAfee VirusScan for Linux Installation Guide* and *McAfee Agent Installation Guide*.

2 Deploy the new SVA software package.

Tasks

- *Import the MOVE AV package* on page 33
  The SVA software package must be checked in to ePolicy Orchestrator and deployed to the virtual machines that is currently running the 2.6 SVA before you can manage your systems.
- *Create a product deployment task* on page 34
  Before a task can be assigned to systems, it must be created.
- *Assign a product deployment task* on page 34
  The McAfee Agent must be assigned to virtual systems to take effect.

See also

Install the McAfee MOVE AV Agentless extension on page 18

Import the MOVE AV package

The SVA software package must be checked in to ePolicy Orchestrator and deployed to the virtual machines that is currently running the 2.6 SVA before you can manage your systems.

Before you begin

Download the SVA software package from the McAfee download site.

Task

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

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

2 On the Master Repository page, select **Actions** | **Check In Package**.

3 Select the package type as **Product or Update (.zip)**.

4 Browse to and select the **MOVEAVAgentless.3.0.0.163-SVA** file.

5 Click **Next**.

6 On the **Package Options** page:

- **Package Info** — Confirm that this is the correct package.
- **Branch** — Select the branch for new products, usually **Current**.
- **Package signing** — Specify if the package is signed by McAfee or is a third-party package.

7 Click **Save** to check in the package.

The new package appears in the **Packages in Master Repository** list on the **Master Repository** tab.

Create a product deployment task

Before a task can be assigned to systems, it must be created.

> **Before you begin**
> You must check in the extension packages before you can create a client task.

Task

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

1 Click **Menu** | **Policy** | **Client Task Catalog**.

2 Select **Product Deployment** from the Client Task Types menu, then click **Actions** | **New Task** to open the Client Task Builder wizard.

3 Select **Product Deployment** from the list, then click **OK**.

4 Type a name for the task you are creating, and add any descriptive information in the **Description** field.

5 Make sure that **Linux** is the only **Target platform** selected.

6 For **Products and components**:

- Select **MOVE AV Agentless 3.0.0** from the drop-down list.
- Set the **Action** to **Install**, set the **Language** to **Language Neutral**, and set the **Branch** to **Current**.
- Leave the **Command line** setting blank.

7 Review the task settings, then click **Save**.

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

Assign a product deployment task

The McAfee Agent must be assigned to virtual systems to take effect.

> **Before you begin**
> You must check in the MOVE AV Agentless package before you can run a product deployment task.

Task

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

1 Click **Menu** | **Policy** | **Client Task Assignments**, then click the **Assigned Client Tasks** tab.

2 Click **Actions** | **New Client Task Assignment**.

3 Select these settings, then click **Next**.

- **Product** — **McAfee Agent**
- **Task Type** — **Product Deployment**
- **Task Name** — The name of the task you used when you created the client task.

4 On the **Schedule** tab, enter the information appropriate to the task you are creating.

5 Examine the settings on the **Summary** tab, then click **Save** to assign the task.

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] 3.0.0**.

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**.

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** by using 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 the process has made outside of its profile. For more information, visit this website: https://help.ubuntu.com/10.04/serverguide/C/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 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/files/pdf/techpaper/VMW-TWP-vSPHR-SECRTY-HRDNG-USLET-101-WEB-1.pdf

Index

T

V