Product Guide

McAfee MOVE AntiVirus 2.5.0
For use with ePolicy Orchestrator® 4.5.0 and 4.6.0 Software
Copyright © 2012 McAfee, Inc. Do not copy without permission.

Trademark Attributions
McAfee, the McAfee logo, McAfee Active Protection, McAfee AppPrism, McAfee Artemis, McAfee CleanBoot, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Enterprise Mobility Management, Foundscore, Foundstone, McAfee NetPrism, McAfee Policy Enforcer, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, SmartFilter, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure, WormTraq are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

License Information
License Agreement
NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.
Contents

Preface
About this guide .................................. 7
Audience ..................................... 7
Conventions .................................... 7
Find product documentation . ............................. 8

McAfee MOVE AntiVirus Multi-Platform

1 Introduction to McAfee MOVE AntiVirus Multi-Platform 11
How the software works .................................... 11
Components and what they do ............................ 12
Before you start .................................. 13

2 Installation and configuration 15
Download McAfee MOVE AV Multi-Platform packages ............................. 15
Requirements ................................... 16
Install McAfee MOVE AV ................................ 16
Install the McAfee MOVE AV Multi-Platform Offload Scan Server ............. 17
Install the extension package ................................ 18
Add the deployment package to the Master Repository ..................... 18
Deploy the McAfee MOVE AV Agent ................................ 19
Deploy to clients using ePolicy Orchestrator 4.5 ..................... 19
Deploy to clients using ePolicy Orchestrator 4.6 ..................... 20
Deploy to VMware linked clones ................................ 21
Deploy in a XenDesktop 5 environment ................................ 22
Install the McAfee MOVE AV Agent manually ..................... 22
Upgrade McAfee MOVE AV Multi-Platform to 2.5 .......................... 23
Install the extension .................................. 23
Upgrade McAfee MOVE AV Multi-Platform Offload Scan Server to 2.5 .... 24
Install the agent package ................................ 24
Upgrade existing 2.0 agents using ePolicy Orchestrator .................. 25
Uninstall McAfee MOVE AV Multi-Platform ............................. 28
Uninstall the McAfee MOVE AV Agent with ePolicy Orchestrator 4.5 .... 28
Uninstall the McAfee MOVE AV Agent with ePolicy Orchestrator 4.6 .... 29
Uninstall the McAfee MOVE AV Offload Scan Server .................... 30
Uninstall the extension .................................. 30
Troubleshoot McAfee MOVE AV Multi-Platform installations ................ 31

3 Monitoring and managing 33
Integration with ePolicy Orchestrator ................................ 33
Policy management ..................................... 33
Configure a policy ..................................... 34
Create a policy ..................................... 34
Apply a policy ..................................... 35
Create a policy specifying Offload Scan Servers .......................... 36
8 Installation and configuration
Requirements ................................... 65
Download the McAfee MOVE AV Agentless packages ........................................... 66
Install VMware vShield Endpoint ................................................................. 67
Setting up the SVA .................................................................................... 67
  Configure the McAfee OVF certificate ....................................................... 67
  Deploy the OVF ....................................................................................... 68
  Configure the SVA .................................................................................... 68
  Install the McAfee MOVE AV Agentless extension ..................................... 69
  Install the VirusScan Enterprise for Linux extension .................................. 69

9 Monitoring and managing
Integration with ePolicy Orchestrator ........................................................... 71
Policy management ..................................................................................... 71
  Configuring policies .................................................................................. 72
Monitoring the SVA ..................................................................................... 74
  View the Threat Event Log ....................................................................... 74
  View the Health and Alarms page ............................................................. 75
Queries and reports ..................................................................................... 75

10 SVA security requirements

Index
Preface

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

**Agentless** — Integrates with VMware vShield 5.0 using VMware vShield Endpoint. This solution addresses the challenges of protecting your virtual environment and keeping it free of malware without an agent, resulting in easy deployment and setup. This option is described in Part II of this guide.

**Multi-Platform** — Removes the need to install an anti-virus application on every VM, and is the original agent-based deployment option. This option is described in Part I of this guide.

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.
- **Users** — People who use the computer where the software is running and can access some or all of its features.

**Conventions**

This guide uses the following typographical conventions and icons.

- **Book title or Emphasis** — Title of a book, chapter, or topic; introduction of a new term; emphasis.
- **Bold** — Text that is strongly emphasized.
- **User input or Path** — Commands and other text that the user types; the path of a folder or program.
- **Code** — A code sample.
- **User interface** — Words in the user interface including options, menus, buttons, and dialog boxes.
- **Hypertext blue** — A live link to a topic or to a website.
- **i** — **Note:** Additional information, like an alternate method of accessing an option.
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

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

<table>
<thead>
<tr>
<th>To access...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>User documentation</td>
<td>1 Click Product Documentation.</td>
</tr>
<tr>
<td></td>
<td>2 Select a product, then select a version.</td>
</tr>
<tr>
<td></td>
<td>3 Select a product document.</td>
</tr>
<tr>
<td>KnowledgeBase</td>
<td>• Click Search the KnowledgeBase for answers to your product questions.</td>
</tr>
<tr>
<td></td>
<td>• Click Browse the KnowledgeBase for articles listed by product and version.</td>
</tr>
</tbody>
</table>
McAfee MOVE AntiVirus Multi-Platform

The Multi-Platform deployment option removes the need to install an anti-virus application on every VM, and is the original agent-based deployment option. This option is described in Part I of this guide.

Chapter 1  Introduction to McAfee MOVE AntiVirus Multi-Platform
Chapter 2  Installation and configuration
Chapter 3  Monitoring and managing
Chapter 4  Upgrade McAfee MOVE AV Multi-Platform 1.5/1.6
Chapter 5  McAfee MOVE AV Multi-Platform Agent command-line interface reference
Chapter 6  McAfee MOVE AV Offload Scan Server command-line interface reference
Introduction to McAfee MOVE AntiVirus Multi-Platform

McAfee® MOVE AntiVirus Multi-Platform is an anti-virus solution for virtual environments that removes the need to install an anti-virus application on every virtual machine (VM). This document covers installation, configuration, and product usage information for McAfee MOVE AV Multi-Platform.

Contents
- How the software works
- Components and what they do
- Before you start

How the software works

Traditional security solutions for virtual environments run as an anti-virus application on every VM on the hypervisor. This model results in reduced VM density per hypervisor, and causes high disk, CPU, and memory usage.

The Multi-Platform deployment option offloads all on-access 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 results in improved performance related to anti-virus scanning and increased VM density per hypervisor.
Components and what they do

This diagram explains how each component performs specific functions to keep your environment protected.

- **ePolicy Orchestrator** — Communicates with the McAfee Agent, manages the Multi-Platform configuration, and provides reports on malware discovered within your virtual environment.

- **Hypervisor** — 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 system.

- **McAfee Agent** — Communicates with ePolicy Orchestrator.

- **McAfee MOVE AV Agent** — Allows end node systems to consult the Offload Scan Server for file scanning and malware detection. Enforces actions on the client when a threat is detected. Includes the mvadm command-line utility.

- **McAfee MOVE AV Offload Scan Server** — Provides offloaded scanning support for end node systems, which minimizes the performance impact on virtual desktops.

- **McAfee MOVE AV extension** — Provides policies and controls for configuring and managing McAfee MOVE AV behavior through ePolicy Orchestrator.

- **McAfee VirusScan Enterprise** — Provides anti-virus protection for VMs and communicates with the Offload Scan Server and the GTI servers.

For information on the other products in the solution, download their documentation from the McAfee Technical Support ServicePortal at http://mysupport.mcafee.com.
Before you start

Perform the following before starting installation and configuration of McAfee MOVE AV Agent software.

- Remove or disable any anti-virus application installed on the virtual machines, such as VirusScan Enterprise or Windows Defender, before deploying McAfee MOVE AV Agent software.

- If VirusScan Enterprise is installed, create a product deployment client task to uninstall VirusScan Enterprise from every virtual machine that receives the McAfee MOVE AV Agent.
Installation and configuration

To set up your environment for the Multi-Platform deployment option, you must download the McAfee MOVE AV Multi-Platform components, install the McAfee MOVE AV Offload Scan Server, and deploy the McAfee MOVE AV Agent.

Contents

- Download McAfee MOVE AV Multi-Platform packages
- Requirements
- Install McAfee MOVE AV
- Deploy the McAfee MOVE AV Agent
- Upgrade McAfee MOVE AV Multi-Platform to 2.5
- Uninstall McAfee MOVE AV Multi-Platform
- Troubleshoot McAfee MOVE AV Multi-Platform installations

Download McAfee MOVE AV Multi-Platform packages

You must download the McAfee MOVE AV Multi-Platform packages before they can be installed onto virtual systems or into ePolicy Orchestrator.

- From the McAfee download site, download these product packages:

<table>
<thead>
<tr>
<th>Package name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOVE-AV_Offload_Server_setup_x86.exe</td>
<td>Offload Scan Server installer</td>
</tr>
<tr>
<td>MOVE-AV_Agent_2500_WIN.zip</td>
<td>Deployment package</td>
</tr>
<tr>
<td>help_mov_av_250.zip</td>
<td>Help extension</td>
</tr>
<tr>
<td>MOVE-AV_Ext_2.5.0.zip</td>
<td>Product extension</td>
</tr>
<tr>
<td>MOVE-AV_Ext_2.5.0_License.zip</td>
<td>License extension; upgrades evaluation package to a fully licensed package</td>
</tr>
<tr>
<td>MOVE-AV_250_docs.ZIP</td>
<td>Documentation package</td>
</tr>
</tbody>
</table>
Requirements

McAfee MOVE AV Multi-Platform is an ePolicy Orchestrator managed product. Policies are maintained in ePolicy Orchestrator. File scanning is performed exclusively on deployed Offload Scan Servers rather than on the end nodes.

Software requirements

- ePolicy Orchestrator 4.5 or 4.6 — Installs client software, pushes out new policies, monitors client activity, creates reports, and stores and sends content and client updates to managed systems.
- McAfee Agent 4.5 or 4.6 — Acts as the intermediary between the end node system and ePolicy Orchestrator.
- VirusScan Enterprise 8.8 — Performs anti-virus scanning operations and must be present on the McAfee MOVE AV Offload Scan Server.

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

System requirements

The Offload Scan Server requires a dedicated virtual machine with VirusScan Enterprise 8.8 installed. The machine must meet these requirements:

- **Operating system**
  - Windows 2008 R2 SP1 or Windows 2008 SP2 (64-bit)
- **CPU**
  - 1 vCPU 2 GHz or higher
- **Memory**
  - 1 GB RAM or higher
- **Free disk space**
  - 8 GB or higher
- **Other requirements**
  - Static IP address

The McAfee MOVE AV Agent software requires one of these operating systems:

- Windows XP SP3
- Windows 7 (32-bit or 64-bit)
- Windows 8 Beta (32-bit or 64-bit)
- Windows 2003 R2 SP2 (32-bit)
- Windows 2008 SP2 (32-bit or 64-bit)
- Windows 2008 R2 SP1 (64-bit)
- Windows Vista (32-bit or 64-bit)

Windows XP virtual machines require 512 MB of RAM or more, all other operating systems require 1 GB of RAM or more.
Install McAfee MOVE AV

These installation tasks must be performed and can be completed in any order.

Tasks

- **Install the McAfee MOVE AV Multi-Platform Offload Scan Server on page 17**
  VirusScan Enterprise 8.8 must be installed on the virtual server before you install the McAfee MOVE AV Multi-Platform Offload Scan Server.

- **Install the extension package on page 18**
  The McAfee MOVE AV extension package must be installed in ePolicy Orchestrator before you can manage your virtual machines.

- **Add the deployment package to the Master Repository on page 18**
  Add the McAfee MOVE AV Agent deployment package into the Master Repository.

Install the McAfee MOVE AV Multi-Platform Offload Scan Server

VirusScan Enterprise 8.8 must be installed on the virtual server before you install the McAfee MOVE AV Multi-Platform Offload Scan Server.

**Before you begin**

- A copy of the McAfee MOVE AV Multi-Platform Offload Scan Server installation file (MOVE-AV_Server_Setup_x86.exe) must be accessible to the virtual machine where you want to install the McAfee MOVE AV Multi-Platform Offload Scan Server.

- Before you install the McAfee MOVE AV Multi-Platform Offload Scan Server on the virtual server, you must install VirusScan Enterprise 8.8 on the virtual server.

**Task**

For option definitions, click ? in the interface.

1. Run the McAfee MOVE AV offload scan server installation file (MOVE-AV_Offload_Server_Setup_x86.exe) in the folder you downloaded the file.

   
   ![](image1)
   
   McAfee recommends that you run the installation with elevated privileges.

2. Read the license agreement, select **Accept license agreement**, then click **Next**.

3. Enter the user name and organization, then click **Next**.

4. Specify the preferred port where the MOVE AV Server service will listen, then click **Next**.
   By default, the service is configured to listen on port 9053.
   
   ![](image2)
   
   The installer automatically makes an exception entry in the Windows Firewall settings on the McAfee MOVE AV Offload Server to allow communication on the specified port. If another firewall product is being used, configure it manually to allow communication on this port.

5. Select the Global Threat Intelligence (GTI) level.
   This setting can be changed after installation using the McAfee MOVE AV Offload Server command-line interface (CLI). GTI is also known as Artemis, and more information on Artemis can be found in the McAfee VirusScan Enterprise Product Guide.

6. Verify the installation settings, then click **Install**.
7 Verify the installation:
   • Confirm that the MOVE AV Server service is running from Services control panel.
   • Confirm the following CLI access menu option has been added to the Windows Start menu: Start | Programs | McAfee | MOVE AV Server Command Prompt.

**Install the extension package**
The McAfee MOVE AV extension package must be installed in ePolicy Orchestrator before you can manage your virtual machines.
The extension file, MOVE-AV_Ext_2.5.0.zip, can be downloaded from the McAfee download site.

**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 the extension file, then click OK.
3 Verify that the product name appears in the Extensions list.

**Add the deployment package to the Master Repository**
Add the McAfee MOVE AV Agent deployment package into the Master Repository.

**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 MOVE-AV_Agent_2500_WIN.zip 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, this is usually Current.
   • Package signing — Specifies 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 Packages in Master Repository list in the Master Repository tab.
Deploy the McAfee MOVE AV Agent

After the McAfee MOVE AV package has been added to McAfee ePO, you must deploy the agent to virtual machines.

Tasks

- **Deploy to clients using ePolicy Orchestrator 4.5 on page 19**
  Deploy the McAfee MOVE AV Agent to virtual machines using ePolicy Orchestrator.

- **Deploy to clients using ePolicy Orchestrator 4.6 on page 20**
  Deploying McAfee MOVE AV Agent to clients from ePolicy Orchestrator requires two tasks. You must first create a deployment client task, then assign that task to virtual machines.

- **Deploy to VMware linked clones on page 21**
  When using VMware linked clones, extra steps are required to deploy the McAfee MOVE AV Agent properly.

- **Deploy in a XenDesktop 5 environment on page 22**
  When operating in a XenDesktop 5 environment, extra steps are required to deploy the McAfee MOVE AV Agent properly.

- **Install the McAfee MOVE AV Agent manually on page 22**
  It is possible to install the McAfee MOVE AV manually without deploying it from ePolicy Orchestrator.

Deploy to clients using ePolicy Orchestrator 4.5

Deploy the McAfee MOVE AV Agent to virtual machines using ePolicy Orchestrator.

Before you begin

You must have added the virtual machines to the System Tree in ePolicy Orchestrator, and deployed the McAfee Agent to those systems. For details, see the [McAfee ePolicy Orchestrator Installation Guide](#) and [McAfee Agent Product Guide](#).

This guide specifies only steps to perform on a single system. To perform these steps on multiple systems, select a group in the System Tree and choose Client Tasks.

Task

1. From the ePolicy Orchestrator console, click Menu | Systems | System Tree | Client Tasks, then click New Task.

2. On the description page of the Client Task Builder, type the name of the task, for example, Install MOVE AV Agents on VM clients, and add a description in Notes.

3. From the Type drop-down list, select Product Deployment | Send this task to all computers then select, then click Next.

4. On the configuration page of the Client Task Builder, next to Target platforms, select Windows.

5. From the Products and components list, select MOVE AV Agent 2.0.0.xx, change the following settings, then click Next.
   a. Set the Action to Install.
   b. Set the Language to English.
   c. Set Branch to Current.

6. On the schedule page of the Client Task Builder, select Enabled for the schedule status.
Select a Schedule type, select Run Immediately to deploy now, then click Next.

Review and verify the details on the Client Task Builder page, then click Save.

If you scheduled the task to run immediately, perform an agent wake-up call.

To confirm that the McAfee MOVE AV Agent was successfully installed:

a. Log on to the McAfee MOVE AV Agent machine as administrator.

b. Open the McAfee MOVE AV Agent command prompt and type this command:

```
mvadm status
```

You can also check that system information and McAfee MOVE AV properties are reported to the ePolicy Orchestrator console. For details, see the McAfee ePolicy Orchestrator Product Guide.

Deploy to clients using ePolicy Orchestrator 4.6

Deploying McAfee MOVE AV Agent to clients from ePolicy Orchestrator requires two tasks. You must first create a deployment client task, then assign that task to virtual machines.

Tasks

- Create a McAfee MOVE AV Agent deployment task on page 20
  Before a task can be assigned to systems, it must be created.
- Assign the McAfee MOVE AV Agent deployment task to virtual systems on page 21
  The McAfee MOVE AV Agent must be assigned to virtual systems to take effect.

Create a McAfee MOVE AV Agent deployment task

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

Task

For option definitions, click ? in the interface.

1. Open the Client Task Catalog: click Menu | Policy | Client Task Catalog.

2. In the left column under McAfee Agent, select Product Deployment.

3. Click Actions | New Task, select Product Deployment, then click OK.

4. Type the name of the task, for example, Install MOVE AV Agent on VM client, and add any descriptive information in the Description field.

5. Make sure that Windows is the only Target platform selected.

6. For Products and components:
   a. Select MOVE AV Agent 2.5.0 from the first drop-down list.
   b. Set the Action to Install, set the Language to Language Neutral, and set the Branch to Current.
   c. Leave the Command line setting blank.

7. Select the remaining options according to your environment's best practices, then click Save.

The newly created task appears in the Client Task Catalog.
Assign the McAfee MOVE AV Agent deployment task to virtual systems
The McAfee MOVE AV Agent must be assigned to virtual systems to take effect.

Before you begin
You must have already added the McAfee MOVE AV Agent to the Master Repository, and added your virtual systems to the System Tree.

Task
For option definitions, click ? in the interface.

1 Select a group in the System Tree.
2 Click Menu | Policy | Client Task Assignments, then click the Assigned Client Tasks tab.
3 Click Actions | New Client Task Assignment.
4 Select these settings, then click Next.
   • Product — McAfee Agent
   • Task Type — Product Deployment
   • Task Name — The name of the task you created earlier
5 On the Schedule tab next to Schedule type, select Run Immediately from the drop-down list, set the Options as appropriate, then click Next.
6 Examine the settings on the Summary tab, then click Save to assign the task.

The McAfee MOVE AV Agent is deployed to every system in the selected group in the System Tree.

Deploy to VMware linked clones
When using VMware linked clones, extra steps are required to deploy the McAfee MOVE AV Agent properly.

Before you begin
The McAfee Agent must already be installed on the parent virtual machine, and McAfee MOVE AV Agent must already be in the ePolicy Orchestrator Master Repository.

Task
1 Deploy McAfee MOVE AV Agent to the parent virtual machine, then verify it has been applied successfully on the vDisk.
2 Stop the McAfee Framework service.
3 Delete the registry value AgentGUID from the location determined by your Windows operating system.
   • 32-bit — HKEY_LOCAL_MACHINE\SOFTWARE\Network Associates\ePolicy Orchestrator\Agent (32-bit)
   • 64-bit — HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Network Associates\ePolicy Orchestrator\Agent (64-bit)
4 Shut down the virtual machine and take a snapshot.
5 From the VMware view manager, select the pool, then click Edit.
6 In the pool window, select vCenter settings.

7 Click Browse, then select the snapshot you just created.

8 Apply the new snapshot to all virtual machines in the pool.

These steps change with different versions of VMware View. Consult your VMware View Administrator Guide for details on recomposing linked clone desktops.

See also
Deploy to clients using ePolicy Orchestrator 4.5 on page 19
Deploy to clients using ePolicy Orchestrator 4.6 on page 20

Deploy in a XenDesktop 5 environment

When operating in a XenDesktop 5 environment, extra steps are required to deploy the McAfee MOVE AV Agent properly.

Before you begin

The McAfee Agent must already be installed on the master image, and the McAfee MOVE AV Agent must already be in the Master Repository.

Task

1 Deploy the McAfee MOVE AV Agent to the master image, then verify it has been applied successfully.

2 Configure and apply McAfee MOVE AntiVirus policies to the master image, then verify it has been applied successfully.

3 In the master image, delete the value for the registry key named AgentGUID from the location determined by your Windows operating system.
   • 32-bit — HKEY_LOCAL_MACHINE\SOFTWARE\Network Associates\ePolicy Orchestrator\Agent (32-bit)
   • 64-bit — HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Network Associates\ePolicy Orchestrator\Agent (64-bit)

4 Shut down the master image and clone all virtual machines from that master image.

Install the McAfee MOVE AV Agent manually

It is possible to install the McAfee MOVE AV manually without deploying it from ePolicy Orchestrator.

Before you begin

You must have downloaded the McAfee MOVE AV installer and store it in a location accessible from the system where it will be installed.

This procedure is used only in situations where you don’t want to use ePolicy Orchestrator to deploy the McAfee MOVE AV Agent to the target system.

Task

1 Extract the appropriate McAfee MOVE AV Agent installer based on your Windows operating system.
   • 64-bit — setup-win-amd64.exe.
   • 32-bit — setup-win-x86.exe.

2 Run the appropriate installer, then click Next in the Welcome screen.
3 In the License Agreement screen, accept the EULA, then click Next.

4 In the Customer information screen, enter a user name and organization and click Next.

5 In the Destination folder screen, choose the default location or specify a different location, then click Next.

6 In the Ready to install the program screen, click Install.

7 Click Finish to complete the installation.

8 To configure the manual installation, open the McAfee MOVE AV command prompt: click Start | Programs | McAfee | MOVE AV Agent Command Prompt, and run these commands.
   a Type mvadm status to verify the McAfee MOVE AV Agent installed correctly.
   b Type mvadm config serveraddress1=<IPv4 address of the primary offload scan server>
   c Type mvadm config serveraddress2=<IPv4 address of the secondary offload scan server>
   d Type mvadm enable to activate the McAfee MOVE AV Agent.

The McAfee MOVE AV Agent is now installed and running on the target system.

---

Upgrade McAfee MOVE AV Multi-Platform to 2.5

Upgrading McAfee MOVE AV Multi-Platform from version 2.0 to version 2.5 replaces the McAfee MOVE AV Agent and extension in ePolicy Orchestrator. The 2.0 agents can be managed by the 2.5 extension and are supported by the 2.5 Offload Scan Servers.

**Before you begin**

From the Software Manager or the McAfee download site, download these components:
- McAfee MOVE AV 2.5 extension (MOVE-AV_Ext_2.5.0.zip)
- McAfee MOVE AV 2.5 license (MOVE-AV_Ext_2.5.0_License.zip)
- McAfee MOVE AV 2.5 Offload Server (MOVE-AV_Offload_Server_setup_x86.exe)
- McAfee MOVE AV 2.5 Agent package (MOVE-AV_Agent_2500_WIN.zip)

**Tasks**

- **Install the extension on page 24**
  Version 2.5 of the McAfee MOVE AV extension replaces the 2.0 extension. Existing policies are automatically migrated to version 2.5.

- **Upgrade McAfee MOVE AV Multi-Platform Offload Scan Server to 2.5 on page 24**
  We recommend staggering Offload Scan Server upgrades so that protection is maintained on the supported end nodes. McAfee MOVE AV 2.0 Agents are supported by the 2.5 Offload Scan Servers.

- **Install the agent package on page 24**
  The agent package must be installed in ePolicy Orchestrator and deployed to end node systems before you can manage your virtual machines.

- **Upgrade existing 2.0 agents using ePolicy Orchestrator on page 25**
  Create a client task to install the McAfee MOVE AV Agent over the 2.0 version. We recommend using ePolicy Orchestrator Client Tasks to upgrade McAfee MOVE AV Agents.
Install the extension
Version 2.5 of the McAfee MOVE AV extension replaces the 2.0 extension. Existing policies are automatically migrated to version 2.5.

**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** | **Extension**.
2. When the **Extensions** page opens, click **Install Extension**.
3. Browse to and select the **MOVE-AV_Ext_2.5.0.zip** file, then click **OK**. This extension replaces the existing 2.0 extension.
4. After a confirmation message, click **OK**.

> The full extension consists of an evaluation extension and a licensing extension.

Upgrade McAfee MOVE AV Multi-Platform Offload Scan Server to 2.5
We recommend staggering Offload Scan Server upgrades so that protection is maintained on the supported end nodes. McAfee MOVE AV 2.0 Agents are supported by the 2.5 Offload Scan Servers.

**Task**
1. Download the McAfee MOVE AV Offload Scan Server installation file from the Software Manager:
   a. Copy the installation file (**MOVE AV_Server_Setup_x86.exe**) to the virtual machine.
   b. From the virtual server, run the installation file.
   c. Click **Yes** when prompted to confirm the upgrade. The Installation wizard opens.
   d. Click **Next** to start the upgrade.
   e. Select the **GTI Level** you chose for your 2.0 server.
   f. Click **Finish**.
2. Verify that the upgrade was successful:
   a. Confirm that the **MOVE AV Server** service is running by using the **Services** control panel.
   b. Open the McAfee MOVE AV Offload Scan Server command prompt and run this command to verify the version:

```bash
mvadm version
```

Install the agent package
The agent package must be installed in ePolicy Orchestrator and deployed to end note systems before you can manage your virtual machines.

**Before you begin**
Download the agent 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)**.
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.

### Upgrade existing 2.0 agents using ePolicy Orchestrator

Create a client task to install the McAfee MOVE AV Agent over the 2.0 version. We recommend using ePolicy Orchestrator Client Tasks to upgrade McAfee MOVE AV Agents.

ePolicy Orchestrator 4.5 and 4.6 require different steps for creating a client task.

#### Tasks

- **Upgrade the McAfee MOVE AV Agent using ePolicy Orchestrator 4.5 on page 25**
  > After the Offload Scan Server is upgraded, install the agent on all virtual machines using the Offload Scan Server.

- **Upgrade the McAfee MOVE AV Agent with ePolicy Orchestrator 4.6 on page 26**
  > Upgrading McAfee MOVE AV Agents from ePolicy Orchestrator requires two tasks. You must first create an upgrade client task, then assign that task to virtual machines.

### Upgrade the McAfee MOVE AV Agent using ePolicy Orchestrator 4.5

After the Offload Scan Server is upgraded, install the agent on all virtual machines using the Offload Scan Server.

#### Task

For option definitions, click ? in the interface.

1. From the ePolicy Orchestrator console, click **Menu | Systems | System Tree | Client Tasks**, then click **New Task**.
2. On the **Description** page of the Client Task Builder, type the name of the task — for example, **Install MOVE AV Agents on VM clients** — and add a description in **Notes**.
3. Select **Product Deployment** from the **Type** drop-down list, select **Send this task to all computers**, then click **Next**.
4. On the **Configuration** page next to **Target platforms**, select **Windows**.
For **Products and components**, select the following, then click **Next**.

- Select **MOVE AV Agent 2.5.0** from the first drop-down list.
- Set the **Action** to **Install**, set the **Language** to **English**, and set the **Branch** to **Current**.
- Leave the **Command line** setting blank.

On the **Schedule** page, select **Enabled** for the schedule status.

Select a **Schedule type**, then select **Run Immediately** to deploy now.

Review and verify the details on the **Summary** page, then click **Save**.

If you scheduled the task to run immediately, perform an agent wake-up call.

Confirm that the McAfee MOVE AV Agent has been successfully upgraded:

- Log on to the McAfee MOVE AV Agent machine as administrator.
- Open the MOVE AV Agent command prompt and execute the following command to verify the MOVE AV Agent version:

```
mvadm version
```

You can also check that system information and MOVE AV properties are reported to the ePolicy Orchestrator console. For details, see the **McAfee ePolicy Orchestrator Product Guide**.

---

**Upgrade the McAfee MOVE AV Agent with ePolicy Orchestrator 4.6**

Upgrading McAfee MOVE AV Agents from ePolicy Orchestrator requires two tasks. You must first create an upgrade client task, then assign that task to virtual machines.

**Tasks**

- **Create a McAfee MOVE AV Agent upgrade task** on page 26
  Before you can upgrade the McAfee MOVE AV Agent, you must create an upgrade client task.

- **Assign the McAfee MOVE AV Agent upgrade task to virtual systems** on page 27
  The upgrade task must be assigned to virtual systems to take effect.

**Create a McAfee MOVE AV Agent upgrade task**

Before you can upgrade the McAfee MOVE AV Agent, you must create an upgrade client task.

**Task**

For option definitions, click ? in the interface.

1. Open the Client Task Catalog: click **Menu | Policy | Client Task Catalog**.
2. In the left column under **McAfee Agent**, select **Product Deployment**.
3. Click **Actions | New Task**, then select **Product Deployment** and click **OK**.
4. Type the name of the task, for example, **Upgrade MOVE AV Agent on VM client**, and add information in the **Description** field.
5. Make sure that **Windows** is the only **Target platform** selected.
6 For Products and components:
   a Select MOVE AV Agent 2.5.0 from the first drop-down list.
   b Set the Action to Install, set the Language to Language Neutral, and set the Branch to Current.
   c Leave the Command line setting blank.

7 Select the remaining options according to your environment’s best practices, then click Save. The newly created task appears in the Client Task Catalog.

**Assign the McAfee MOVE AV Agent upgrade task to virtual systems**
The upgrade task must be assigned to virtual systems to take effect.

**Before you begin**
You must have already added the McAfee MOVE AV Agent to the Master Repository, and added your virtual systems to the System Tree.

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

1 Select a group in the System Tree.

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

3 Click Actions | New Client Task Assignment.

4 Select these settings, then click Next.
   - Product — McAfee Agent
   - Task Type — Product Deployment
   - Task Name — The name of the task you created earlier

5 On the Schedule tab next to Schedule type, select Run Immediately from the drop-down list, set the Options as appropriate, then click Next.

6 Examine the settings displayed on the Summary tab, then click Save to assign the task.

The McAfee MOVE AV Agent is upgraded on every system in the selected group in the System Tree.
Uninstall McAfee MOVE AV Multi-Platform

A full uninstall involves removing all components: McAfee MOVE AV Agent, McAfee MOVE AV Offload Scan Server, and the McAfee MOVE AV Multi-Platform extension.

Tasks

- **Uninstall the McAfee MOVE AV Agent with ePolicy Orchestrator 4.5 on page 28**
  As part of the uninstall, the agent must be removed from virtual machines.

- **Uninstall the McAfee MOVE AV Agent with ePolicy Orchestrator 4.6 on page 29**
  Uninstalling the McAfee MOVE AV Agent with ePolicy Orchestrator 4.6 requires two tasks. You must first create an uninstallation client task, then assign that task to virtual systems.

- **Uninstall the McAfee MOVE AV Offload Scan Server on page 30**
  Uninstall McAfee MOVE AV Offload Scan Server through the Windows Control Panel.

- **Uninstall the extension on page 30**
  Uninstall the McAfee MOVE AV Multi-Platform extension from ePolicy Orchestrator.

Uninstall the McAfee MOVE AV Agent with ePolicy Orchestrator 4.5

As part of the uninstall, the agent must be removed from virtual machines.

Task

For option definitions, click ? in the interface.

1. From the ePolicy Orchestrator console, click **Menu | Systems | System Tree | Client Tasks**, then click **New Task**.

2. On the **Description** page of the Client Task Builder, type the name of the task. For example, name the task **Uninstall MOVE AV Agents from VM clients and add information to Notes**.

3. From the **Type** drop-down list, select **Product Deployment**, then **Send this task to all computers**.

4. Click **Next**.

5. On the **Configuration** page next to **Target platforms**, select **Windows**.

6. From the **Products and components** list, select **MOVE AV Agent 2.5.0.xx**, change the following settings, then click **Next**.
   a. Set the **Action** to **Remove**.
   b. Set the **Language** to **English**.
   c. Set **Branch** to **Current**.

7. On the **Schedule** page, select **Enabled** for the schedule status.

8. Select a **Schedule type**, then select **Run Immediately** to deploy now.

9. Review and verify the details on the **Summary** page, then click **Save**.

10. If you scheduled the task to run immediately, perform an agent wake-up call.
Uninstall the McAfee MOVE AV Agent with ePolicy Orchestrator 4.6

Uninstalling the McAfee MOVE AV Agent with ePolicy Orchestrator 4.6 requires two tasks. You must first create an uninstallation client task, then assign that task to virtual systems.

Tasks
- Create the McAfee MOVE AV Agent uninstallation task on page 29
  You must first create an uninstallation task before you can apply it to systems and remove the software.
- Assign the McAfee MOVE AV Agent uninstallation task to virtual systems on page 29
  The uninstallation task must be assigned to virtual systems to take effect.

Create the McAfee MOVE AV Agent uninstallation task
You must first create an uninstallation task before you can apply it to systems and remove the software.

Task
For option definitions, click ? in the interface.

1  Open the Client Task Catalog: click Menu | Policy | Client Task Catalog.
2  In the left column under McAfee Agent, select Product Deployment.
3  Click Actions | New Task, select Product Deployment, then click OK.
4  Type the name of the task, like Uninstall MOVE AV Agent on VM client, and an optional Description.
5  Make sure that Windows is the only Target platform selected.
6  For Products and components, select the following, then click Next.
   a  Select MOVE AV Agent 2.5.0 from the first drop-down list.
   b  Set the Action to Remove, set the Language to Language Neutral, and set the Branch to Current.
   c  Leave the Command Line setting blank.
7  Select the remaining options according to your environment’s best practices, then click Save.

The newly created task appears in the Client Task Catalog.

Assign the McAfee MOVE AV Agent uninstallation task to virtual systems
The uninstallation task must be assigned to virtual systems to take effect.

Before you begin
You must have already added the McAfee MOVE AV Agent to the Master Repository and added your virtual systems to the System Tree.

Task
For option definitions, click ? in the interface.

1  Select a group in the System Tree.
2  Click Menu | Policy | Client Task Assignments, then click the Assigned Client Tasks tab.
3  Click Actions | New Client Task Assignment.
4 Select these settings, then click Next.

• Product — McAfee Agent
• Task Type — Product Deployment
• Task Name — The name of the task you created earlier

5 On the Schedule tab next to Schedule type, select Run Immediately from the drop-down list, set the Options as appropriate, then click Next.

6 Examine the settings displayed on the Summary tab, then click Save to assign the task.

The McAfee MOVE AV Agent is removed from every system in the selected group in the System Tree.

Uninstall the McAfee MOVE AV Offload Scan Server
Uninstall McAfee MOVE AV Offload Scan Server through the Windows Control Panel.

Task
1 Click Start | Control Panel | Programs and Features.
2 Select MOVE AV Server, then click Uninstall.
3 Click Yes to start uninstallation.
4 After the uninstall procedure is complete, verify MOVE AV Server no longer appears in the Program and Features list.

Uninstall the extension
Uninstall the McAfee MOVE AV Multi-Platform extension from ePolicy Orchestrator.

Task
For option definitions, click ? in the interface.
1 From the ePolicy Orchestrator console, click Menu | Software | Extensions.
2 From the Extensions tab under McAfee group, select MOVE AV.
3 Click Remove.

This now requires uninstalling both the base and license extensions. The license extension must be removed first.

Delete reports and queries manually after uninstalling the extension.
Troubleshoot McAfee MOVE AV Multi-Platform installations

Common operating issues encountered in a McAfee MOVE AV deployment can be resolved by performing these steps.

**Task**

1. Check that the **MOVE AV server** service is running and listening on the specified port. The default port is 9053.

2. Check that the McAfee MOVE AV Agent is able to communicate through any firewalls with the McAfee MOVE AV Offload Scan Server on the specified port.

3. Verify the McAfee MOVE AV Agent is enabled. Run the `mvadm status` command from a McAfee MOVE AV Agent command-line interface with administrator privileges.

4. Make sure that McAfee MOVE AV policy on ePolicy Orchestrator is configured correctly.
   - Protection State is Enabled
   - McAfee MOVE AV Offload Server IP addresses are configured correctly

5. Check that VirusScan Enterprise 8.8 is installed and working properly on the McAfee MOVE AV Offload Scan Server virtual machine, and that a recent DAT is present.
Installation and configuration
Troubleshoot McAfee MOVE AV Multi-Platform installations
Monitoring and managing

The Multi-Platform deployment option monitors the status of virtual machines to identify problems and modify behavior from the ePolicy Orchestrator console.

Contents

- Integration with ePolicy Orchestrator
- Policy management
- Configuring permissions sets
- Queries and reports
- Global Threat Intelligence
- Handling potentially malicious files
- Communication between virtual machines and Offload Scan Servers
- McAfee MOVE AV Multi-Platform alerts
- McAfee MOVE AV Multi-Platform self-protection

Integration with ePolicy Orchestrator

The McAfee MOVE AV deployment option uses the ePolicy Orchestrator framework to deliver and enforce policies.

This approach provides a single management solution that allows for mass deployment.

ePolicy Orchestrator communicates policy information to McAfee MOVE AV clients on a regular interval through the McAfee Agent. McAfee MOVE AV clients enforce policies, collect event information, and transmit the information back to ePolicy Orchestrator. Client-side management is available through a command-line interface (CLI) on Windows-based clients.

Policy management

Through the ePolicy Orchestrator console, you can configure policies from a central location.

How policies are enforced

When you change McAfee MOVE AV Multi-Platform policies in the ePolicy Orchestrator console, the changes take effect on the targeted managed systems at the next agent-server communication. To enforce policies immediately, send an agent wake-up call to the targeted systems from the ePolicy Orchestrator console.
 Policies and their categories

Policy information for the McAfee MOVE AV Agent is grouped into a single category: General. You can create, modify, or delete as many policies as needed under this category. ePolicy Orchestrator provides a preconfigured McAfee Default policy, which can’t 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. McAfee MOVE AV Multi-Platform, 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.

Policy tracking and tuning

The deployment and management of McAfee MOVE AV Multi-Platform clients are handled from ePolicy Orchestrator. Since McAfee MOVE AV policies apply only to virtual machines in the System Tree, you can group the virtual machines hierarchically by attributes.

McAfee recommends grouping the virtual machines by the McAfee MOVE AV Multi-Platform configuration criteria, including scan settings and use of the Offload Scan Server. Deploying McAfee MOVE AV Multi-Platform to thousands of systems is managed easily because most virtual machines fit into a few usage profiles. Managing a large deployment is reduced to maintaining a few policy rules. As a deployment grows, newly added virtual machines should fit one or more existing profiles, and can be placed under the correct group in the System Tree.

Configure a policy

You can configure the McAfee MOVE AV Multi-Platform Agent on-access scan behavior with policy settings.

The policies can configure:

- Which McAfee MOVE AV Offload Scan Server a virtual machine uses
- When files are scanned
- Files and programs excluded from scanning
- Where to send alerts
- What to do when a threat is found
- How to handle quarantined files

Create a policy

Policies allow you to describe threat scanning behavior for specific virtual machines.
**Task**

For option definitions, click ? in the interface.

1. Open the Policy Catalog: click Menu | Policy | Policy Catalog.
2. In the Product drop-down list, select MOVE AV [Multi-Platform] 2.5.0. Because all policy settings in the Product drop-down list are grouped under one category (General), the policy is automatically selected in the Category drop-down list.
3. Click New Policy.
4. On the New Policy page, configure these policy settings, then click OK.
5. In the General tab of the Policy Settings page for the newly-created policy, configure these settings to control basic behavior.
6. In the Scan Items tab, configure the following settings to control which files are scanned.
7. In the Alerts tab, configure the Show threat events in setting to specify where alerts are shown: the Event Log (on the local system), in ePO for use in reports and queries, or as a Popup.
8. In the Actions tab, configure the behavior When a threat is found. 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.
9. In the Quarantine tab, select Enabled for the quarantine feature, specify where quarantined files are stored with the Quarantine Directory setting, and how long quarantined files are stored with the Quarantine data retention setting.
10. Click Save.

**Apply a policy**

You must apply a policy for it to take effect.

**Task**

For option definitions, click ? in the interface.

1. In the System Tree, select the group containing the virtual machines for which you want to apply the policy.
2. Click Menu | Systems | System Tree | Assigned Policies.
3. In the Product drop-down list, select MOVE AV [Multi-Platform] 2.5.0.
4. In the Actions column of the McAfee Default policy, select Edit assignments.
5. In the Inherit from list on the Policy Assignments page, select Break inheritance and assign the policy and settings below.
6. In the Assigned Policy list, select the policy you created earlier.
Create a policy specifying Offload Scan Servers
You can create a policy that specifies which Offload Scan Servers a group of virtual machines should use.

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

1. From the ePolicy Orchestrator console, click **Menu | Policy | Policy Catalog**, then select **MOVE AV [Multi-Platform] 2.5.0**.
2. Click **New Policy**.
3. Type a name for the new policy (for example, **MOVE AV Server Policy**), then click **OK**.
4. In the **General** tab on the **Policy Settings** page, configure options as appropriate, then click **Save** to commit your changes.
   - Select **Scan Configuration** to make sure that the protection state is enabled. The protection state is disabled by default.
   - Enter the **Primary MOVE AV Server IPv4 address** and **Primary MOVE AV Server port**. Enter the **Secondary MOVE AV Server IPv4 address** (if any).
   - Enter the **Secondary MOVE AV Server IPv4 address** and **Secondary MOVE AV Server port**.
   - Modify the **Scan Timeout**, **Cache Scan Result of File Size Up to**, and **Cache Expiration Time** settings if required.

After you create this policy, you must assign it before it takes effect.

Configuring permissions sets
A permission set is a group of permissions (or access rights) granted to a user account for specific features of a product. Permission sets only grant permissions — they never remove a permission.

All permissions to all products and features are assigned automatically to global administrators. Other users must have permission assigned manually. Global administrators can assign existing permission sets when creating or editing user accounts and when creating or editing permission sets.

For more information on permission sets, see the *McAfee ePolicy Orchestrator Product Guide*.

**McAfee MOVE AV Permission set**
The McAfee MOVE AV Multi-Platform software adds a **MOVE-AV 2.5 Policy Permission** section to the permission sets with one setting. This defines access rights to the software features. Global administrators must grant permissions to users to use the McAfee MOVE AV deployment option, because no permissions are granted by default.

**Other required permissions**
The global administrator needs to give ePolicy Orchestrator permissions to handle other areas that work with the McAfee MOVE AV including queries, dashboards, and the Threat Event Log.
For these features... | These permissions sets are required
---|---
Dashboards | Dashboards, Queries and Reports
Queries | Queries and Reports
Policies | System Tree access, Policy Assignment Rules
Events on virtual machines | Systems, System Tree access, Threat Event Log

### Configure permission sets

Update the read/write access permissions assigned to the user roles defined for your ePolicy Orchestrator environment.

**Task**

For option definitions, click ? in the interface.

1. From the ePolicy Orchestrator console, click **Menu | User Management | Permission Sets**
2. Select a user role from the **Permission Sets** list.
3. Next to **MOVE-AV 2.5 Policy Permission**, click **Edit**.
4. Select the permission level.
5. Click **Save**.

For more information on permission sets, see the *McAfee ePolicy Orchestrator Product Guide*.

### Queries and reports

From the ePolicy Orchestrator console, you can extract information about your McAfee MOVE AV Multi-Platform clients with several queries and reports.

- View events in the threat event log.
- Run default McAfee MOVE AV Multi-Platform queries that show important client information.
- Create reports using data sent by the McAfee MOVE AV Agents to the ePolicy Orchestrator database.

### Fix the VirusScan Enterprise compliance query results

VirusScan Enterprise software might report virtual machines that use McAfee MOVE AV Multi-Platform as noncompliant.

In general, we recommend that you use the VirusScan Enterprise Compliance report to determine compliance for systems that use the Offload Scan Server. Use the McAfee MOVE AV Agent status report to determine if client protection is enabled.

If virtual machines that use the Multi-Platform deployment option are being reported incorrectly as noncompliant in the VirusScan Enterprise 8.8 Compliance query, exclude those machines from its results.

**Task**

For option definitions, click ? in the interface.

1. From the ePolicy Orchestrator console, click **Menu | Queries and Reports**.
2. Click **Shared groups | VirusScan Enterprise | VSE version 8.8 Compliance**.
3 Click Edit, then click the Filters tab.

4 From Available Properties, select Products Property | Installed products.

5 Select does not contain from the comparison, and type MOVE-AV in the text box.

6 Click Save to modify the query.

**Default queries**

The McAfee MOVE AV deployment option adds several queries to your ePolicy Orchestrator environment.

<table>
<thead>
<tr>
<th>Query</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOVE-AV [Multi-Platform]: Agent Protection Status</td>
<td>Displays the status of all MOVE Agents being managed by the server.</td>
</tr>
<tr>
<td>MOVE-AV [Multi-Platform]: Summary of Threats Detected in the Last 24 Hours</td>
<td>Displays threats that have been detected in the last 24 hours.</td>
</tr>
<tr>
<td>MOVE-AV [Multi-Platform]: Threats Detected in the Last 24 Hours</td>
<td>Displays the number of threats detected in the last 24 hours by hour.</td>
</tr>
<tr>
<td>MOVE-AV [Multi-Platform]: Top 10 Computers with the Most Detections</td>
<td>Displays the top ten computers with the most threat detections in the last three months.</td>
</tr>
<tr>
<td>MOVE-AV [Multi-Platform]: Top 10 Detected Threats</td>
<td>Displays the top ten detected threats in the last three months.</td>
</tr>
<tr>
<td>MOVE-AV [Multi-Platform]: Top 10 Users with the Most Detections</td>
<td>Displays the top ten users with the most threat detections in the last three months.</td>
</tr>
</tbody>
</table>

You can add these queries to dashboards to more efficiently track your environment by displaying several queries at once. See the chapter on dashboards in the ePolicy Orchestrator Product Guide for information on managing dashboards.

The queries are constantly refreshed, or you can run them at a specified frequency. You can add them to reports that are run on specific schedules and re-tried as PDF files or email messages.

**Global Threat Intelligence**

*McAfee Global Threat Intelligence (GTI)*, previously known as Artemis, is a comprehensive, real-time, cloud-based file reputation service that enables McAfee products to protect customers against both known and emerging malware-based threats.

This cloud-based system receives billions of file reputation queries each month, and responds with a score that reflects the likelihood that the file in question is malware. The score is based not only on the collective intelligence from sensors querying the McAfee cloud and the analysis performed by McAfee Labs researchers and automated tools, but also on the correlation of cross-vector intelligence from web, email, and network threat data. The McAfee anti-malware engine — whether deployed as part of an endpoint anti-malware, gateway, or other solution — uses the score to determine action (such as block or quarantine) based on local policy.

These are the key benefits of GTI:

- Compresses the threat protection time period from days to milliseconds
- Increases malware detection rates
- Reduces downtime and remediation costs associated with malware attacks
Change the Global Threat Intelligence level

You can change the Global Threat Intelligence (GTI) sensitivity level when required.

The GTI sensitivity level can be changed only at a command prompt on a McAfee MOVE AV Multi-Platform Offload Scan Server. Higher sensitivity levels are more secure, but can degrade performance and might cause more false positive results.

**Task**

1. Open the McAfee MOVE AV Multi-Platform Offload Server command prompt: click **Start | Programs | McAfee | Move AV Server Command Prompt**.

2. Type `mvadm config set GTILevel=x` where `x` is a value of 0 (Disabled), or 1 (Very Low) through 5 (Very High).

   **Note:** If `x` is anything other than an integer between 0 and 5, an error message is displayed, and the GTI level is not changed.

The GTI level is changed as specified. If the new GTI level is more sensitive than before, all previously scanned files are flushed from the cache.

Handling potentially malicious files

Policy settings determine what happens to a file after a scan has determined it could be malicious.

There are three actions the McAfee MOVE AV deployment option can take when dealing with a potentially malicious file.

These policy settings determine which of these actions are taken.

<table>
<thead>
<tr>
<th>Primary action</th>
<th>Quarantine setting</th>
<th>Actions taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete files automatically</td>
<td>Enabled (default)</td>
<td>Back up the malicious file as a .VIR file in the quarantine folder, then delete the original file.</td>
</tr>
<tr>
<td>(default)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete files automatically</td>
<td>Disabled</td>
<td>Delete the file. Nothing appears in the quarantine folder.</td>
</tr>
<tr>
<td>Deny access to files</td>
<td>Enabled or Disabled</td>
<td>Deny access to the file. Nothing appears in the quarantine folder.</td>
</tr>
</tbody>
</table>

Isolating malicious files in quarantine

The McAfee MOVE AV deployment option provides methods for dealing with malicious files beyond events and notifications.

When an item is detected as a threat, an event is triggered that notifies administrators of the threat. In addition, the malicious file can also be isolated in a quarantine folder. This allows you to perform other processes, like remove and restore, on the quarantined items.

Quarantining is enabled by default, and quarantined items are placed in the `C:\Quarantine` folder on the system where the file was discovered. Quarantined items are sorted in the quarantine folder by threat category, and are automatically deleted after a configurable period of time. Quarantine behavior can be modified through policy changes.

Change threat quarantine behavior

Modify the default quarantine settings to suit your organizational policies.
**Task**
For option definitions, click ? in the interface.

1. Open the Policy Catalog: click Menu | Policy | Policy Catalog, then from the Product list select MOVE-AV 2.5.0.

2. Click the name of an existing policy to edit it, then click the Quarantine tab.

3. Change the threat quarantine behavior:
   - Disable the quarantine functionality by deselecting Enabled.
   - Change where quarantined items are stored by changing the Quarantine Directory setting.
     Mapped network drives and UNC network path names are not supported.
   - If you don’t want quarantined items deleted after a period of time, deselect Automatically delete quarantined data after the specified number of days.
   - If you want to change how long quarantined items are stored before they are deleted, change the Number of days to keep backed-up data in the quarantine directory setting.

4. Click Save to modify the policy.

The modified policy is applied after the next agent-server communication interval. If you want the policy applied immediately, perform an agent wake-up call on the systems where the newly-modified policy is assigned.

**Change the primary threat response**
You can modify how the Multi-Platform deployment option handles potentially malicious files after a threat is detected.

By default, McAfee MOVE AV Multi-Platform policy backs up a potentially malicious file to a quarantine folder as a .VIR file, then deletes the original. These steps change that behavior.

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

1. Open the Policy Catalog: click Menu | Policy | Policy Catalog, then from the Product list select MOVE-AV [Multi-Platform] 2.5.0.

2. Click the name of an existing policy to edit it, then click the Actions tab.

3. Change the Perform this action first setting to Delete files automatically or Deny access to files, depending on your requirements.

   The second action is set to Deny access to files if that is not the first action. Otherwise, there is no second action. If quarantine is on, a backup of the file is made in the quarantine folder before it is deleted.

4. Click Save.

Systems assigned this policy are updated at the next agent-server communication interval.

**Change when files are scanned**
You can modify the Multi-Platform deployment option policy to determine which files are scanned for threats and when.

By default, the Multi-Platform deployment option scans all executable files when read from or written to disk, or when opened for backup. The McAfee program files and Windows service are excluded from scans.
Task
For option definitions, click ? in the interface.

1. Open the Policy Catalog: click Menu | Policy | Policy Catalog, then from the Product list select MOVE-AV [Multi-Platform] 2.5.0.
2. Click the name of an existing policy to edit it, then click the Scan Items tab.
3. Change the file scanning behavior in one of these ways:
   - Change when files are scanned by selecting any combination of When writing to disk, When reading from disk, On network drives, and Opened for backup.
     - Selecting On network drives can degrade network performance depending on your environment.
   - Change which files are scanned by selecting All files to scan all executable files, or Following only to specify a list of file extensions to scan.
   - Wildcards are not supported, and exact matches are required. Do not include the period when specifying extensions.
   - Specify paths and processes that you want to exclude from scans by adding them to the Path Exclusions and Process Exclusions lists.
4. Click Save to modify the policy.

Communication between virtual machines and Offload Scan Servers

The McAfee MOVE AV Agent and the Offload Scan Server communicate through a specific port to isolate and secure their communication channel.

In order to make sure communication between the McAfee MOVE AV Agent and the Offload Scan Server is isolated from all other network traffic, a specific network port is used. This port must be opened up on any firewalls between the systems to allow this communication to occur.

By default, the Multi-Platform deployment option uses port 9053. This port is not generally used by other applications. If your network has other requirements, you can change this communication port by modifying the policy.

Change the Offload Scan Server port

The port used by the Offload Scan Server can be changed after installation if your network environment requires the Multi-Platform deployment option use a different port.

Task
For option definitions, click ? in the interface.

1. On the Offload Scan Server, open the command prompt: click Start | Programs | McAfee | Move AV Server Command Prompt.
2. Change the port by typing this command: mvadm config set serverport1=<portnum>.
3. Restart the Offload Scan Server.
4. From the ePolicy Orchestrator console, modify the policy assigned to the group of virtual machines using this Offload Scan Server to reflect the new port number.

   See the McAfee ePolicy Orchestrator Product Guide for details on modifying policies.

5. Perform an agent wake-up call to push the modified policy to appropriate virtual machines.

---

**McAfee MOVE AV Multi-Platform alerts**

There are three situations important enough for McAfee MOVE AV Multi-Platform to generate alerts. This is when protection is enabled or disabled, or when a threat is detected.

These alerts can be displayed in any of three locations: the local system’s Windows Event Log, the ePolicy Orchestrator threat event log, or on the local system as a McAfee System Tray pop-up.

You can configure these alerts by changing the policy.

### Change the alert behavior

The default alert locations can be modified to suit your organizational policies.

By default, McAfee MOVE AV Multi-Platform displays alerts in the local system’s Windows Event Log, and the ePolicy Orchestrator threat event log. Alert notification locations can be changed by modifying the McAfee MOVE AV Multi-Platform policy.

#### Task

For option definitions, click ? in the interface.

1. Open the Policy Catalog: click **Menu | Policy | Policy Catalog**, then from the Product list select **MOVE-AV [Multi-Platform] 2.5.0**.

2. Click the name of an existing policy to edit it, then click the **Alerts** tab.

3. Change the threat alert behavior by selecting or deselecting the following locations:
   - **Event Log** — The local system’s Windows Event Log
   - **ePO** — The ePolicy Orchestrator threat event log
   - **Popup** — A pop-up alert in the McAfee System Tray icon

4. Click **Save** to modify the policy.

The modified policy is applied after the next agent-server communication interval. If you want the policy applied immediately, perform an agent wake-up call on the systems where the newly-modified policy is assigned.

### McAfee MOVE AV Multi-Platform alert messages list

McAfee MOVE AV Multi-Platform displays one of these messages when the triggering event occurs.

<table>
<thead>
<tr>
<th>Events</th>
<th>Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection enabled</td>
<td>MOVE AV Agent protection is enabled. Reason <code>&lt;reason&gt;</code>.</td>
</tr>
<tr>
<td>Protection disabled</td>
<td>MOVE AV Agent protection is disabled. Reason <code>&lt;reason&gt;</code>.</td>
</tr>
<tr>
<td>Threat detected</td>
<td>Detected threat <code>&lt;threat name&gt;</code> of type <code>&lt;threat type&gt;</code> in file <code>&lt;filename&gt;</code>. The file is <code>&lt;action&gt;</code>.</td>
</tr>
</tbody>
</table>

When the message is displayed, every word in angled brackets (for example, `<reason>`) is replaced by an appropriate phrase.
**McAfee MOVE AV Multi-Platform self-protection**

The self-protection feature defends files, service, and registry keys on virtual machines. Use the VirusScan Enterprise access protection rules for self-protection of the Offload Scan Server.

The self-protection feature is designed to prevent malicious attacks on McAfee MOVE AV Multi-Platform software components. This keeps your virus protection active and stable.

<table>
<thead>
<tr>
<th>Protection type</th>
<th>Protection effects</th>
</tr>
</thead>
<tbody>
<tr>
<td>File protection</td>
<td>These files and all parent folders are protected against deletion and renaming.</td>
</tr>
<tr>
<td></td>
<td>• &lt;install_dir&gt;mvadm.exe</td>
</tr>
<tr>
<td></td>
<td>• &lt;install_dir&gt;mvmctraypl.dll</td>
</tr>
<tr>
<td></td>
<td>• &lt;install_dir&gt;mvagtsvc.exe</td>
</tr>
<tr>
<td></td>
<td>• &lt;systemroot&gt;\system32\drivers\mvagtdrv.sys</td>
</tr>
<tr>
<td></td>
<td>• &lt;install_dir&gt;mvagntpl.dll</td>
</tr>
<tr>
<td>Registry protection</td>
<td>These registry keys, all subkeys, and all values under them are protected.</td>
</tr>
<tr>
<td></td>
<td>• services\mvagtdrv</td>
</tr>
<tr>
<td></td>
<td>• services\mvagtsvc</td>
</tr>
<tr>
<td></td>
<td>• services\EventLog\Application\MOVE AV Agent</td>
</tr>
<tr>
<td></td>
<td>All parent keys starting from services are protected from deletion and rename.</td>
</tr>
<tr>
<td>Service stop protection</td>
<td>The mvagtsvc service cannot be stopped.</td>
</tr>
</tbody>
</table>

The self-protection feature is controlled by the `IntegrityEnabled` configuration parameter. By default, the parameter is set to 0x7, and all components of the feature are enabled.

The configuration parameter accepts values from 0–7, which is a decimal representation of a 3-bit binary value.

<table>
<thead>
<tr>
<th>Decimal value</th>
<th>Binary value</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>000</td>
<td>Protection disabled</td>
</tr>
<tr>
<td>1</td>
<td>001</td>
<td>File protection</td>
</tr>
<tr>
<td>2</td>
<td>010</td>
<td>Registry protection</td>
</tr>
<tr>
<td>3</td>
<td>011</td>
<td>File and registry protection</td>
</tr>
<tr>
<td>4</td>
<td>100</td>
<td>Service protection</td>
</tr>
<tr>
<td>5</td>
<td>101</td>
<td>Service and file protection</td>
</tr>
<tr>
<td>6</td>
<td>110</td>
<td>Service and registry protection</td>
</tr>
<tr>
<td>7</td>
<td>111</td>
<td>Service, registry, and file protection</td>
</tr>
</tbody>
</table>

For example, to enable file and registry protection, set the parameter to 3 (0b011) with this command:

```
mvadm config set IntegrityEnabled=3
```

To enable file and service stop protection, but not registry protection, set the parameter to 5 (0b101) with this command:

```
mvadm config set IntegrityEnabled=5
```
To disable the self-protection feature, set the parameter to 0 with this command:

```
mvadm config set IntegrityEnabled=0
```

When service stop protection is enabled (by setting the highest bit to 1), the `mvagtsvc` service does not accept stop commands. File protection and registry protection require the agent driver to be loaded, but service stop protection does not. Use these command to load or unload the driver.

```
mvadm enable
mvadm disable
```

### McAfee MOVE AV Multi-Platform Offload Scan Server

We recommend using the following VirusScan Enterprise access protection rules for self-protection of the offload scan server. These must be configured manually after installation.

<table>
<thead>
<tr>
<th>Protection type</th>
<th>Protection effects</th>
</tr>
</thead>
<tbody>
<tr>
<td>File protection (via VirusScan Enterprise access protection)</td>
<td>Create a File/Folder Access Protection Rule that excludes the <code>mvserver.exe</code> process, and blocks the <code>C:\Program Files (x86)\McAfee\MOVE AV Server\**</code> folder. Set File actions to prevent to Write access to files, New files being created and Files being deleted, as shown here.</td>
</tr>
<tr>
<td></td>
<td><strong>File/Folder Access Protection Rule</strong></td>
</tr>
<tr>
<td></td>
<td>Rule name:</td>
</tr>
<tr>
<td></td>
<td>MVFile</td>
</tr>
<tr>
<td></td>
<td>Processes to include:</td>
</tr>
<tr>
<td></td>
<td>*</td>
</tr>
<tr>
<td></td>
<td>Processes to exclude:</td>
</tr>
<tr>
<td></td>
<td><code>mvserver.exe</code></td>
</tr>
<tr>
<td></td>
<td>File or folder name to block: (Wildcards are allowed)</td>
</tr>
<tr>
<td></td>
<td><code>C:\Program Files (x86)\McAfee\MOVE AV Server\**</code></td>
</tr>
<tr>
<td></td>
<td>File actions to prevent:</td>
</tr>
<tr>
<td></td>
<td>☑ Read access to files</td>
</tr>
<tr>
<td></td>
<td>☑ Write access to files</td>
</tr>
<tr>
<td></td>
<td>☑ Files being executed</td>
</tr>
<tr>
<td></td>
<td>☑ New files being created</td>
</tr>
<tr>
<td></td>
<td>☑ Files being deleted</td>
</tr>
<tr>
<td></td>
<td>See the <code>VirusScan Enterprise Product Guide</code> for details.</td>
</tr>
</tbody>
</table>

 Registry protection (VirusScan Enterprise access protection)

These registry keys and all keys and values under them must be protected:

- HKCCS/Service/mvserver
- HKCCS/Service/mvserver/Parameters
There are two approaches for upgrading McAfee MOVE AV Multi-Platform. The first requires greater resource overhead, the second potentially results in a short non-protection window for virtual machines that are being upgraded.

- **Persistent Virtual Machine** — Use this approach if you have an environment where virtual machines are persistent and require constant anti-virus protection.

- **Non-Persistent Virtual Machine** — Use this approach for environments with non-persistent virtual machines, but carefully plan Offload Scan Server downtime because virtual machines lose virus protection for a period of time during the upgrade process.

### Upgrade persistent virtual machines

This approach provides nearly seamless virus protection, but requires the overhead of duplicate Offload Scan Servers for the duration of the upgrade process.

We recommend this method for environments comprised of primarily persistent virtual machines.

#### Task

For option definitions, click ? in the interface.

1. Install the 2.5 package and extension on ePolicy Orchestrator.

   These components will coexist with previous versions of the components within ePolicy Orchestrator.

2. Create a new virtual server and install VirusScan Enterprise 8.8 on that server.

3. Install the Offload Scan Server version 2.5 on the virtual server.

4. Create a new McAfee MOVE AV Multi-Platform policy that references the Offload Scan Server you created in the previous step, and assign it to the virtual machines being upgraded.

5. Create an ePolicy Orchestrator client task to upgrade the McAfee MOVE AV Agents to version 2.5.

   As the upgrade task is executed on virtual machines, the VMs begin to use the new offload scanner for file scanning.
6 Shut down the version 1.5/1.6 Offload Scan Servers. McAfee MOVE AV extension can be removed from ePolicy Orchestrator.
7 Remove the version 1.5/1.6 McAfee MOVE AV Multi-Platform extension from ePolicy Orchestrator.

**Upgrade non-persistent virtual machines**

This approach does not require creating additional Offload Scan Servers, 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**

For option definitions, click ? in the interface.

1 Install the 2.5 package and extension to ePolicy Orchestrator.

   These components coexist with previous versions of the components within ePolicy Orchestrator.

2 Upgrade VirusScan Enterprise on all offload scan servers from version 8.7 to version 8.8.

   See the VirusScan Enterprise Installation Guide for more information.

3 Manually upgrade all Offload Scan Servers to version 2.5.

   Virtual machines serviced by upgraded Offload Scan Servers do not have anti-virus protection until after this task is completed.

4 Modify the master or golden image by deploying version 2.5 of the McAfee MOVE AV Agent from ePolicy Orchestrator.

**Upgrade McAfee MOVE AV Multi-Platform**

You must perform the upgrade tasks in a specific order to successfully upgrade the software.

Upgrading from 1.5/1.6 to 2.5 requires uninstalling the McAfee MOVE AV Agent as a separate client task prior to installing 2.5. Refer to the appendix for information on upgrades from 1.5/1.6.

- McAfee MOVE AV package and extension versions 1.6 and 2.5 can both reside within ePolicy Orchestrator simultaneously.
- Version 2.5 of the McAfee MOVE AV Agent and McAfee MOVE AV Offload Server software packages upgrades over version 1.6. Both versions cannot reside on the same virtual machine.
- Version 2.5 offload scan servers do not connect with version 1.6 Agents, and version 1.6 offload scan servers do not connect with version 2.5 Agents.
- Version 2.5 of the McAfee MOVE AntiVirus Offload Scan Server software package requires that VirusScan Enterprise version 8.8 is installed on the virtual server before installation can continue.
Tasks

• **Upgrade McAfee MOVE AV Offload Scan Server** on page 47
  Complete these steps on the virtual machine where the server is installed to upgrade the offload scan server from a prior version.

• **Install the extension package** on page 47
  Version 2.5 of the McAfee MOVE AV ePolicy Orchestrator extension can coexist with 1.5/1.6 extension versions.

• **Migrate existing policies to McAfee MOVE AV Multi-Platform 2.5** on page 48
  You can migrate policies you created with earlier versions of McAfee MOVE AV Multi-Platform using a server task that is available after installing the new extension.

• **Upgrade the McAfee MOVE AV Agent using ePolicy Orchestrator 4.5** on page 25
  After the Offload Scan Server is upgraded, install the agent on all virtual machines using the Offload Scan Server.

• **Upgrade the McAfee MOVE AV Agent with ePolicy Orchestrator 4.6** on page 26
  Upgrading McAfee MOVE AV Agents from ePolicy Orchestrator requires two tasks. You must first create an upgrade client task, then assign that task to virtual machines.

**Upgrade McAfee MOVE AV Offload Scan Server**
Complete these steps on the virtual machine where the server is installed to upgrade the offload scan server from a prior version.

In environments that are made up of primarily persistent images, creating new additional version 2.0 Offload Scan Servers might be preferable to upgrading existing Offload Scan Servers.

Task
For option definitions, click ? in the interface.

1. Install the McAfee MOVE AV Offload Scan Server on the virtual server.
   a. Upgrade the VirusScan Enterprise instance on the Offload Scan Server to version 8.8.
   b. Copy the McAfee MOVE AV Offload Scan Server installation file (**MOVE AV_Server_Setup_x86.exe**) to the virtual machine.
   c. From the virtual server, run the McAfee MOVE AV Offload Scan Server installation file.
   d. Click **Yes** when prompted to confirm the upgrade.
   e. Click **Next** to start the upgrade, then click **Finish** when prompted.

2. Verify that the upgrade was successful:
   a. Confirm that the MOVE AV Server service is running by using the **Services** control panel.
   b. Open the McAfee MOVE AV Offload Scan Server command prompt and execute the following command to verify the version:
      ```
      mvadm version
      ```

**Install the extension package**
Version 2.5 of the McAfee MOVE AV ePolicy Orchestrator extension can coexist with 1.5/1.6 extension versions.

**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_Ext_2.5.0.zip` file, then click **OK**.
4. After a confirmation message, click **OK**.

Migrate existing policies to McAfee MOVE AV Multi-Platform 2.5
You can migrate policies you created with earlier versions of McAfee MOVE AV Multi-Platform using a server task that is available after installing the new extension.

**Before you begin**
The McAfee MOVE AV Multi-Platform extension version 2.5 must be installed before migrating policies.

Offload Scan Server policy settings and policy assignments are not migrated. Offload Scan Server policy 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: Migrate Policy from MOVE-AV 1.5/1.6 to MOVE-AV 2.5.0**.
3. In the **Actions** column, click **Run**.
4. Open the **Server Task Log**: click **Menu | Automation | Server Task Log**.
5. Verify the task finished.

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

If version 2.5 policies exist with the same name as version 1.5/1.6 policies, the migration server task fails.

Upgrade the McAfee MOVE AV Agent using ePolicy Orchestrator 4.5
After the Offload Scan Server is upgraded, install the agent on all virtual machines using the Offload Scan Server.

Task
For option definitions, click ? in the interface.

1. From the ePolicy Orchestrator console, click **Menu | Systems | System Tree | Client Tasks**, then click **New Task**.
2. On the **Description** page of the Client Task Builder, type the name of the task — for example, **Install MOVE AV Agents on VM clients** — and add a description in **Notes**.
3. Select **Product Deployment** from the **Type** drop-down list, select **Send this task to all computers**, then click **Next**.
4 On the Configuration page next to Target platforms, select Windows.

5 For Products and components, select the following, then click Next.
   a Select MOVE AV Agent 2.5.0 from the first drop-down list.
   b Set the Action to Install, set the Language to English, and set the Branch to Current.
   c Leave the Command line setting blank.

6 On the Schedule page, select Enabled for the schedule status.

7 Select a Schedule type, then select Run Immediately to deploy now.

8 Review and verify the details on the Summary page, then click Save.

9 If you scheduled the task to run immediately, perform an agent wake-up call.

10 Confirm that the McAfee MOVE AV Agent has been successfully upgraded:
    a Log on to the McAfee MOVE AV Agent machine as administrator.
    b Open the MOVE AV Agent command prompt and execute the following command to verify the MOVE AV Agent version:

```
mvadm version
```

You can also check that system information and MOVE AV properties are reported to the ePolicy Orchestrator console. For details, see the McAfee ePolicy Orchestrator Product Guide.

Upgrade the McAfee MOVE AV Agent with ePolicy Orchestrator 4.6

Upgrading McAfee MOVE AV Agents from ePolicy Orchestrator requires two tasks. You must first create an upgrade client task, then assign that task to virtual machines.

Tasks
   • Create a McAfee MOVE AV Agent upgrade task on page 26
     Before you can upgrade the McAfee MOVE AV Agent, you must create an upgrade client task.
   • Assign the McAfee MOVE AV Agent upgrade task to virtual systems on page 27
     The upgrade task must be assigned to virtual systems to take effect.

Create a McAfee MOVE AV Agent upgrade task

Before you can upgrade the McAfee MOVE AV Agent, you must create an upgrade client task.

Task
   For option definitions, click ? in the interface.

1 Open the Client Task Catalog: click Menu | Policy | Client Task Catalog.

2 In the left column under McAfee Agent, select Product Deployment.

3 Click Actions | New Task, then select Product Deployment and click OK.

4 Type the name of the task, for example, Upgrade MOVE AV Agent on VM client, and add information in the Description field.

5 Make sure that Windows is the only Target platform selected.
6 For Products and components:
   a Select MOVE AV Agent 2.5.0 from the first drop-down list.
   b Set the Action to Install, set the Language to Language Neutral, and set the Branch to Current.
   c Leave the Command line setting blank.

7 Select the remaining options according to your environment's best practices, then click Save. The newly created task appears in the Client Task Catalog.

**Assign the McAfee MOVE AV Agent upgrade task to virtual systems**
The upgrade task must be assigned to virtual systems to take effect.

**Before you begin**
You must have already added the McAfee MOVE AV Agent to the Master Repository, and added your virtual systems to the System Tree.

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

1 Select a group in the System Tree.

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

3 Click Actions | New Client Task Assignment.

4 Select these settings, then click Next.
   • Product — McAfee Agent
   • Task Type — Product Deployment
   • Task Name — The name of the task you created earlier

5 On the Schedule tab next to Schedule type, select Run Immediately from the drop-down list, set the Options as appropriate, then click Next.

6 Examine the settings displayed on the Summary tab, then click Save to assign the task.

The McAfee MOVE AV Agent is upgraded on every system in the selected group in the System Tree.
You can access the McAfee MOVE AV Multi-Platform Agent command-line interface (CLI) on the agent virtual machine to perform basic maintenance tasks.

The CLI is a series of commands you can issue to the `mvadm` utility. Each command has zero or more arguments that can be appended to the command to modify the command’s behavior. This reference lists each command available in `mvadm`, and all possible argument variations.

### Access the McAfee MOVE AV Agent command-line interface

A shortcut to the McAfee MOVE AV Multi-Platform command-line interface (CLI) is added to the Windows start menu during installation.

- Open the McAfee MOVE AV Multi-Platform CLI: click **Start | Programs | McAfee | MOVE AV Agent command prompt**.

  This command prompt has administrator privileges.

At this command prompt, you can type commands that activate the `mvadm` utility to perform administration tasks on the virtual machine.

### config

Use the `config` command to display and edit the configuration settings that are applied to current installation.

```
mvadm config set NAME=VALUE
```

```
mvadm config show
```

<table>
<thead>
<tr>
<th>Arguments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set NAME=VALUE</td>
<td>Sets the value of the configuration setting <code>NAME</code> to <code>VALUE</code>.</td>
</tr>
<tr>
<td>show</td>
<td>Lists the configuration settings.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AllowNetworkScan</td>
<td>0 (off) or 1 (on).</td>
<td>Enables or disables scanning of files residing on a network path.</td>
</tr>
<tr>
<td>ConnTimeout</td>
<td>A positive integer value. Defaults to 0 (no timeout).</td>
<td>Sets the connection timeout in milliseconds.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>EventSink</td>
<td>An integer between 0 (no notifications) and 14 (all notifications). Defaults to 14.</td>
<td>Determines where threat events are sent. The total combines the values for Windows Event Viewer log (2), ePolicy Orchestrator Threat Event Log (4), and McAfee System Tray pop-up (8).</td>
</tr>
<tr>
<td>IntegrityEnabled</td>
<td>An integer between 0 (no self-protection) and 7 representing a binary value. Defaults to 7 (all self-protections).</td>
<td>Determines the active self-protections. The total combines the values for file (1), registry (2), and services (4).</td>
</tr>
<tr>
<td>LogFileNum</td>
<td>A positive integer value. Defaults to 4.</td>
<td>Limits the number of log files allowed before they are rotated.</td>
</tr>
<tr>
<td>LogFileSize</td>
<td>An integer greater than 1024. Defaults to 2048.</td>
<td>Limits the size (in KB) of an individual log file.</td>
</tr>
<tr>
<td>MaxFileSize</td>
<td>A positive integer value. Defaults to 40.</td>
<td>Limits the size (in MB) of files where scan results are cached. Files up to this size are transferred completely to the offload scan server for scanning.</td>
</tr>
<tr>
<td>QuarantineEnabled</td>
<td>0 (off) or 1 (on). Defaults to 1.</td>
<td>Enables or disables quarantine services.</td>
</tr>
<tr>
<td>QuarantineFolder</td>
<td>A valid file path. Defaults to C:\Quarantine.</td>
<td>Determines where quarantined files are stored. Cannot be a mapped network drive or UNC file path.</td>
</tr>
<tr>
<td>QuarantineDays</td>
<td>A positive integer. Defaults to 28.</td>
<td>Determines the number of days quarantined files are stored before being deleted. Submitting a 0 turns off quarantined file deletion.</td>
</tr>
<tr>
<td>RTEMode</td>
<td>0 (off) or 1 (on). Defaults to 0.</td>
<td>Indicates protection status on the virtual machine. This value cannot be changed through the config command.</td>
</tr>
<tr>
<td>ScanAllFileTypes</td>
<td>0 (specific extensions) or 1 (all files). Defaults to 1.</td>
<td>Determines whether to scan all files or only specific extensions.</td>
</tr>
<tr>
<td>ScanFlags</td>
<td>An integer between 0 (no operations scanned) and 7 representing a binary value. Defaults to 7 (all operations scanned).</td>
<td>Determines which operations trigger scanning. The total combines the values for Read (1), Write (2), and Backup (4).</td>
</tr>
<tr>
<td>ScanTimeout</td>
<td>A positive integer. Defaults to 45000.</td>
<td>Limits the time (in milliseconds) allowed for file scans after which the file can be accessed.</td>
</tr>
<tr>
<td>ServerAddress1</td>
<td>An IPv4 address. No default.</td>
<td>Specifies the IPv4 address of the primary offload scan server used by the virtual machine.</td>
</tr>
<tr>
<td>ServerAddress2</td>
<td>An IPv4 address. No default.</td>
<td>Specifies the IPv4 address of the secondary offload scan server used by the virtual machine.</td>
</tr>
<tr>
<td>ServerPort1</td>
<td>Between 1024 and 65535. Defaults to 9053.</td>
<td>Specifies the port used to communicate with the primary offload scan server.</td>
</tr>
<tr>
<td>ServerPort2</td>
<td>Between 1024 and 65535. Defaults to 9053.</td>
<td>Specifies the port used to communicate with the secondary offload scan server.</td>
</tr>
<tr>
<td>ThreatAction1</td>
<td>0 (delete) or 1 (deny access). Defaults to 0.</td>
<td>Determines the primary action taken when a threat is detected.</td>
</tr>
<tr>
<td>ThreatAction2</td>
<td>0 (delete) or 1 (deny access). Defaults to 1.</td>
<td>Determines the secondary action taken when a threat is detected.</td>
</tr>
</tbody>
</table>
**disable**

Use the `disable` command to disable the McAfee MOVE AV Agent on the virtual machine.

```
mvadm disable
```

<table>
<thead>
<tr>
<th>Arguments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Disables the McAfee MOVE AV Agent on the virtual machine.</td>
</tr>
</tbody>
</table>

This removes virus protection from the virtual machine.

**enable**

Use the `enable` command to enable the McAfee MOVE AV Agent on the virtual machine when it was earlier disabled.

```
mvadm enable
```

<table>
<thead>
<tr>
<th>Arguments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Enables the McAfee MOVE AV Agent. This restores anti-virus protection to the virtual machine.</td>
</tr>
</tbody>
</table>

**excludopath**

Use the `excludopath` command to specify paths to be skipped during anti-virus scanning.

```
mvadm excludopath add path
mvadm excludopath remove path
mvadm excludopath list
mvadm excludopath flush
```

<table>
<thead>
<tr>
<th>Arguments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add path</td>
<td>Specifies the path to be excluded from anti-virus scanning.</td>
</tr>
<tr>
<td>remove path</td>
<td>Removes the path from the list of paths to be excluded from anti-virus scanning.</td>
</tr>
<tr>
<td>list</td>
<td>Lists the path exclusion rules defined using the <code>add</code> argument.</td>
</tr>
<tr>
<td>flush</td>
<td>Removes all user-defined path exclusion rules defined using the <code>add</code> argument.</td>
</tr>
</tbody>
</table>

**ftypes**

Use the `ftypes` command to display and edit the list of file extensions to be sent for anti-virus scanning.

```
mvadm ftypes add extn
mvadm ftypes remove extn
mvadm ftypes list
```

Wildcards are not supported by the `ftypes` command, and extensions must be an exact match. Issuing a `mvadm ftypes add doc` command will not cause `.DOCX` files to be scanned.
Arguments | Description
---|---
add extn | Causes the files with extension `extn` to be included for anti-virus scanning.
remove extn | Removes the files with extension `extn` from the list of files to be included for anti-virus scanning.
list | Lists the file extensions to be included for anti-virus scanning.

**help**

Use the `help` command to display usage information for the `mvadm` utility.

```
mvadm help
mvadm help command
```

Arguments | Description
---|---
default | Lists the summary description for the McAfee MOVE AV Agent CLI commands.
command | Lists the detailed help for the provided command.

**loglevel**

Use the `loglevel` command to view and edit the log level of the McAfee MOVE AV Agent modules.

```
mvadm loglevel
mvadm loglevel enable {MODULE_NAME | ALL} {TYPES... | ALL}
mvadm loglevel disable {MODULE_NAME | ALL} {TYPES... | ALL}
```

Arguments | Description
---|---
default | Lists the current log level of each module that is part of the McAfee MOVE AV Agent. Use this form to get a full list of modules for use with other forms of the `loglevel` command.

```
enable (MODULE_NAME | ALL) {TYPES... | ALL}
disable (MODULE_NAME | ALL) {TYPES... | ALL}
```

Sets the log level for module `MODULE_NAME` or all modules to the specified log level types or to all types.

Clears the specified log level types or all types for module `MODULE_NAME` or for all modules.

These are the supported log level types:

- Error
- Warning
- System
- Info
- Detail
- Fnentry
- Fnexit
pp

Use the `pp` command to specify trusted processes. All files acted upon by a trusted process are excluded from scans.

```
mvadm pp list

mvadm pp add <process base name>

mvadm pp remove <process base name>

mvadm pp set <process base name>
```

<table>
<thead>
<tr>
<th>Arguments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list</td>
<td>Displays a list of all the trusted processes.</td>
</tr>
</tbody>
</table>
| add <process base name> | Adds the specified process (or processes) as a trusted process. As an example:  
mvadm pp add userprofilemanager.exe  
All files acted upon by the `userprofilemanager.exe` file are excluded from the scan. |
| remove <process base name> | Removes the specified process (or processes) as a trusted process.         |
| set <process base name> | Removes all existing trusted processes and adds the specified process (or processes) as trusted processes. |

q

Use the `q` command to change McAfee MOVE AV Multi-Platform quarantine behavior.

```
mvadm q list

mvadm q restore <detected as>

mvadm q remove <detected as>
```

<table>
<thead>
<tr>
<th>Arguments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list</td>
<td>Lists the currently quarantined files and their detection type.</td>
</tr>
<tr>
<td>restore &lt;detected as&gt;</td>
<td>Restores all <code>.VIR</code> files from the currently configured quarantine folder with the specified <code>&lt;detected as&gt;</code> category.</td>
</tr>
<tr>
<td>remove &lt;detected as&gt;</td>
<td>Deletes all <code>.VIR</code> files from the currently configured quarantine folder with the specified <code>&lt;detected as&gt;</code> category.</td>
</tr>
</tbody>
</table>

status

Use the `status` command to display the current status of the McAfee MOVE AV Agent in terms of operational mode (enabled or disabled) and its McAfee MOVE AV Multi-Platform Offload Scan Server details.

```
mvadm status
```

<table>
<thead>
<tr>
<th>Arguments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Lists the current McAfee MOVE AV Agent status.</td>
</tr>
</tbody>
</table>
Example

C:\Program Files\McAfee\MOVE AV Agent>mvadm status
Scan Configuration: Enabled
Driver Status: Driver is loaded
Primary Server: 172.25.196.64:9054 [Active]
Secondary Server: 172.25.196.65:9053 [Standby]
Protection Status: Enabled

version

Use the version command to display the version of the McAfee MOVE AV Agent installed on the virtual machine.

mvadm version

<table>
<thead>
<tr>
<th>Arguments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Displays the version of the McAfee MOVE AV Agent installed on the virtual machine. This is most useful for verifying an upgrade operation is complete, or checking if an upgrade is needed.</td>
</tr>
</tbody>
</table>
McAfee MOVE AV Offload Scan Server
command-line interface reference

You can access the Offload Scan Server command-line interface (CLI) on the Offload Scan Server virtual machine to perform basic maintenance tasks.

The CLI is a series of commands you can issue to the `mvadm` utility. Each command has zero or more arguments that can be appended to the command to modify the command’s behavior. This reference lists each command available in `mvadm`, and all possible argument variations.

Access the McAfee MOVE AV Offload Scan Server command-line interface

A shortcut to the McAfee MOVE AV Offload Scan Server command-line interface (CLI) is added to the Windows start menu during installation.

Task

- Open the McAfee MOVE AV Offload Scan Server CLI: click Start | Programs | McAfee | MOVE AV Server command prompt.

This command prompt has administrator privileges.

At this command prompt, you can type commands that activates the `mvadm` utility to perform administration tasks on the Offload Scan Server.

cache

Use the `cache` command to perform operations on the Offload Scan Server's scan cache.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mvadm cache save cfilename</code></td>
<td>Save the current set of checksums from the trusted checksum cache to the file cfilename.</td>
</tr>
<tr>
<td><code>mvadm cache load cfilename</code></td>
<td>Load the checksums from file cfilename into the trusted checksum cache.</td>
</tr>
<tr>
<td><code>mvadm cache list</code></td>
<td></td>
</tr>
<tr>
<td><code>mvadm cache flush</code></td>
<td></td>
</tr>
<tr>
<td><code>mvadm cache info</code></td>
<td></td>
</tr>
</tbody>
</table>

Arguments                  | Description                                           |
---------------------------|-------------------------------------------------------|
save cfilename             | Save the current set of checksums from the trusted checksum cache to the file cfilename. |
load cfilename             | Load the checksums from file cfilename into the trusted checksum cache. |
Arguments | Description
--- | ---
list | List the checksums available in the trusted checksum cache.
flush | Remove all checksums from the trusted checksum cache.
info | Print details of the trusted checksum cache.

**config**

Use the `config` command to display and edit the configuration settings that are applied to current installation.

```
mvadm config set NAME=VALUE
```

```
mvadm config show
```

Arguments | Description
--- | ---
set NAME=VALUE | Sets the value of the configuration setting `NAME` to `VALUE`.
show | Lists the configuration settings.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ComputeCksum</td>
<td>0 (server) or 1 (agent). Defaults to 1.</td>
<td>Determines whether to use the server-computed checksum of the file or the checksum sent by the McAfee MOVE AV Agent.</td>
</tr>
<tr>
<td>ConnTimeout</td>
<td>A positive integer value. Defaults to 0 (no timeout).</td>
<td>Sets the connection timeout in milliseconds.</td>
</tr>
<tr>
<td>GTILevel</td>
<td>Between 0 (disabled) and 5 (Very High). Defaults to 1 (Very Low).</td>
<td>Sets the Global Threat Intelligence level (previously known as Artemis.).</td>
</tr>
<tr>
<td>IntegrityEnabled</td>
<td>0 (off) or 1 (on). Defaults to 1.</td>
<td>Enables or disables the self-protection feature.</td>
</tr>
<tr>
<td>LogFileNum</td>
<td>A positive integer value. Defaults to 4.</td>
<td>Limits the number of log files allowed before they are rotated.</td>
</tr>
<tr>
<td>LogFileSize</td>
<td>An integer greater than 1024. Defaults to 2048.</td>
<td>Limits the size (in KB) of an individual log file.</td>
</tr>
<tr>
<td>MaxCacheItems</td>
<td>A positive integer value. Defaults to 1,000,000.</td>
<td>Limits the number of items that can exist in the cache.</td>
</tr>
<tr>
<td>NumThreads</td>
<td>Between 0 and 500. Defaults to 300.</td>
<td>Limits the number of available scan request threads.</td>
</tr>
<tr>
<td>ScanArchiveFiles</td>
<td>0 (off) or 1 (on). Defaults to 0.</td>
<td>Enables or disables scanning inside archive files.</td>
</tr>
<tr>
<td>ScanPUPS</td>
<td>0 (off) or 1 (on). Defaults to 0.</td>
<td>Enables or disables checking for potentially unwanted programs (PUPs). Scan behavior is determined by VirusScan Enterprise settings.</td>
</tr>
<tr>
<td>ServerPort1</td>
<td>Between 1024 and 65535. Defaults to 9053.</td>
<td>Determines the port on which the server listens for client requests.</td>
</tr>
</tbody>
</table>

**help**

Use the `help` command to display usage information for the `mvadm` utility.

```
mvadm help
```

```
mvadm help command
``
Arguments | Description
--- | ---
default | Lists the summary description for the McAfee MOVE AV Offload Scan Server CLI commands.
command | Lists the detailed help for command command.

**loglevel**

Use the loglevel command to view and edit the log level of the McAfee MOVE AV Offload Scan Server modules.

```bash
mvadm loglevel
```

```bash
mvadm loglevel enable {MODULE_NAME | ALL} {TYPES... | ALL}
```

```bash
mvadm loglevel disable {MODULE_NAME | ALL} {TYPES... | ALL}
```

<table>
<thead>
<tr>
<th>Arguments</th>
<th>Description</th>
</tr>
</thead>
</table>
default | Lists the current log level of each module in the McAfee MOVE AV Offload Scan Server. Use this form to get a full list of modules for use with the other forms of the loglevel command.|

| enable {MODULE_NAME | ALL} {TYPES... | ALL} | Sets the log level for module MODULE_NAME or all modules to the specified log level types or to all types. |
| disable {MODULE_NAME | ALL} {TYPES... | ALL} | Clears the specified log level types or all types for MODULE_NAME or for all modules. |

These are the supported log level types:

- Error
- Detail
- Warning
- Fnentry
- System
- Fnexit
- Info

**stats**

Use the stats command to display the current statistics of the McAfee MOVE AV Offload Scan Server.

```bash
mvadm stats
```

<table>
<thead>
<tr>
<th>Arguments</th>
<th>Description</th>
</tr>
</thead>
</table>
default | Displays current usage and performance statistics for the McAfee MOVE AV Offload Scan Server. The statistics are collected in real-time, and the displayed data is a snapshot of the information at the time the command was invoked. The full list of reported statistics is shown in the example output. |

<table>
<thead>
<tr>
<th>Example output</th>
</tr>
</thead>
</table>
C:\>mvadm stats
Total number of cksum req: 13125
Total number of file transfer req: 11825
Total number of smart file req: 14
Cksum cache hit: 1300
Total av scan req: 11825
Total av scan failure: 0
Data recv failure: 0
Resp send failure: 0

McAfee MOVE AntiVirus 2.5.0  Product Guide  59
version

Use the `version` command to display the version of the McAfee MOVE AV Offload Scan Server application installed on the server virtual machine.

```
mvadm version
```

<table>
<thead>
<tr>
<th>Arguments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Displays the McAfee MOVE AV Offload Scan Server version number. This is most useful for verifying an update has completed successfully, or checking if an update is needed.</td>
</tr>
</tbody>
</table>
McAfee MOVE AntiVirus Agentless

The Agentless deployment option integrates with VMware vShield 5.0 using VMware vShield Endpoint. This solution addresses the challenges of protecting your virtual environment and keeping it free of malware without an agent, resulting in easy deployment and setup. This option is described in Part II of this guide.

Chapter 7  Introduction to McAfee MOVE AntiVirus Agentless
Chapter 8  Installation and configuration
Chapter 9  Monitoring and managing
Chapter 10 SVA security requirements
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 (Management for Optimized Virtualization Environments) configuration on the SVA
- Leverages the McAfee Agent for policy and event handling
- Provides reports on viruses that are discovered on the VMs 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.
**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.
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 kernal module within the hypervisor.
- As a filter driver within the guest VM.

Contents
- Requirements
- Download the McAfee MOVE AV Agentless packages
- Install VMware vShield Endpoint
- Setting up the SVA

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
- Security Virtual Appliance (SVA)
- VMware ESXi 5.0
  - Patch ESXi500-201109402-BG: Updates tools-light
  - Patch ESXi500-201109401-BG: Updates esx-base
- VMware vCenter 5.0
- vShield Manager 5.0
- vShield Endpoint 5.0
- vSphere Client 5.0

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 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 4.6
  - 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](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/](http://www.mcafee.com/us/downloads/)), download these product packages:

- McAfee MOVE AV Agentless OVF (*move-sva.ovf*)
- McAfee Public CA v1 certificate (*McAfee_CA.cer*)
- McAfee MOVE AV Agentless extension for ePolicy Orchestrator

<table>
<thead>
<tr>
<th>Extension</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main product extension</td>
<td>MVAGNTLS2500.zip</td>
</tr>
<tr>
<td>License extension</td>
<td>MVALSLIC2500.zip</td>
</tr>
</tbody>
</table>

- McAfee MOVE AV Agentless help extension (*help_mov_av_250.zip*)
- McAfee MOVE AV Agentless documentation package (*MOV-AV_250_docs.zip*)
Install VMware vShield Endpoint

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


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

Task
1. Install ESXi 5.0.
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 as administrator.
   d. Select Custom, then click Next.
   e. Expand VMware Device Drivers | VMCI Drivers.
   f. Select vShield Drivers, then This feature will be installed on local hard drive.

Setting up the SVA

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

Configure the McAfee OVF certificate

In order for the McAfee OVF certificate to appear as trusted while deploying the OVF, the McAfee Public CA v1 certificate must be installed in the Intermediate Certification Authorities certificate store on the system running the vSphere client.

Before you begin
To deploy the OVF without trusting the McAfee OVF certificate, see Deploy the OVF.

Task
For option definitions, click ? in the interface.

1. Install the Certificates Snap-in to an MMC.exe.
2 Import the McAfee Public CA v1 certificate:
   a From MMC.exe, navigate to Certificates (Local Computer) | Intermediate Certification Authorities | Certificates.
   b Right-click the Certificates folder, then select All Tasks | Import.
      Browse to McAfee_CA.cer to import it.

Deploy the OVF
As part of the SVA set up and configuration, you must deploy the OVF.

Before you begin
- VMware vShield Endpoint must be installed on the host or hypervisor before deploying the OVF.
- You must disable vMotion on the SVA. You can host the SVA on the hypervisor's local disk to avoid using vMotion.

Task
1 From the vSphere Client, click File | Deploy OVF Template to open the installation wizard.
2 Browse to and select the move-sva.ovf file.
3 Click Open | Next to run through the wizard, then change the default settings as needed.
   - The VM Network port group must be mapped to the port group that the ePolicy Orchestrator server is on.
   - The vmservice-vshield-pg port group must be mapped to the vShield port group.
4 Click Finish.
   Depending on the size of your environment, McAfee recommends increasing the number of CPUs.

Configure the SVA
The first time you log on the configuration script automatically runs.
Use this command to manually run the configuration script: sudo/opt/McAfee/move/bin/sva-config

Task
1 Gather this information, which you’ll need when you run the configuration script:
   - SVA IP address
     - vShield Manager user name and password
     - vCenter IP address
     - ePolicy Orchestrator IP address or DNS name
       - user name and password

2 Power on the VM.
3 From the vSphere Client, open the console.
4 At the prompt, log on with these credentials:
   • User name: svaadmin
   • Password: admin

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

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

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

2 Browse to and select the **moveAVAgentlessLicensed.zip** file, then click **OK**.

**Install the VirusScan Enterprise for Linux extension**

As part of the installation and configuration of the Agentless deployment option, you must install the VirusScan Enterprise for Linux extension using ePolicy Orchestrator, and create an update task to keep your software up to date with the latest anti-virus definitions (DATs).

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:

<table>
<thead>
<tr>
<th>Extension</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee Agent</td>
<td>EPOAGENTMETA.ZIP</td>
</tr>
<tr>
<td>McAfee VirusScan for Linux</td>
<td>LYNXSHLD1700.ZIP</td>
</tr>
<tr>
<td>McAfee VirusScan for Linux reports</td>
<td>LYNXSHLD1700PARSER.ZIP</td>
</tr>
</tbody>
</table>

4 After you install the extension, create a product update task.
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
- Policy management
- Monitoring the SVA
- Queries and reports

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 2.5.0**.
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 IP address or the fully qualified domain name 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.
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.

**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 2.5.0.
3. From the Category drop-down list, select Scan.
4. Click New Policy.
5. On the New Policy page, configure these policy settings, then click OK.
6. In the General tab of the Policy Settings page for the newly-created policy, configure these settings to control basic behavior.
7. In the Scan Items tab, configure these 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 path.
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.

Apply a policy
You must apply a policy for it to take effect. McAfee MOVE AV Agentless policies differ from traditional ePolicy Orchestrator policies because they are applied to the SVA instead of the system on which the policy is enforced.

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 2.5.0.
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 entire policy is configured prior to testing.
- The On Access Scanner (OAS) must be enabled.
- This must happen on the client VM.

Task
For option definitions, click ? in the interface.

1 To create an EICAR test file, copy and paste this line into a new file in your text editor:
\[X5O!P %@AP\{4\PZX54 (P^)7CC)7\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H^*\]

2 Save the file as EICAR.txt.
   This file is deleted as soon as it’s saved.

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

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

5 View the Threat Event Log: Click Menu | Reporting | Threat Event Log.

See also
View the Threat Event Log on page 74

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 MOVE AV Agentless provides the following predefined queries:

- MOVE AV Agentless: Computers with Threats Detected per Week
- MOVE AV Agentless: Detection Response Summary
- MOVE AV Agentless: Summary of Threats Detected in the Last 24 Hours
- MOVE AV Agentless: Summary of Threats Detected in the Last 7 Days
- MOVE AV Agentless: Threat Count by Severity
- MOVE AV Agentless: Threat Names Detected per Week
- MOVE AV Agentless: Threats Detected Over the Previous 2 Quarters
- MOVE AV Agentless: Threats Detected per Week
- MOVE AV Agentless: Top 10 Computers with the Most Detections
- MOVE AV Agentless: Top 10 Detected Threats
- MOVE AV Agentless: Top 10 Threats per Threat Category
- 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
## SVA security requirements

The following security measures are implemented on the SVA.

<table>
<thead>
<tr>
<th>Security measure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>apparmor</strong></td>
<td>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, msvc, contains this profile: <code>/etc/apparmor.d/opt.McAfee.move.bin.msvc</code>. There are two apparmor modes: <strong>complain</strong> and <strong>enforce</strong>. By default, msvc is in enforce mode. You can change the mode to complain by using the <code>aa-complain msvc</code> command. To enable enforce mode, use the <code>aa-enforce msvc</code> command. While in complain mode, you can use the command <code>aa-logprof</code> to analyze any requests the process has made outside of its profile. For more information, visit this website: <a href="https://help.ubuntu.com/10.04/serverguide/C/apparmor.html">https://help.ubuntu.com/10.04/serverguide/C/apparmor.html</a></td>
</tr>
<tr>
<td><strong>iptables</strong></td>
<td>The <code>sva-firewalls</code> script enables the built-in firewall. Usage is `sva-firewalls: start</td>
</tr>
</tbody>
</table>
| **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`  
## Index

### A
about this guide 7
agent
  - assign deployment task 21
  - assign uninstall task 29
  - assign upgrade task 27, 50
  - create deployment task 20
  - create uninstall task 29
  - create upgrade task 26, 49
  - deploy to VMware 21
  - deploy to XenDesktop 22
  - deploy with ePolicy Orchestrator 4.5 19
  - deploy with ePolicy Orchestrator 4.6 20, 21
  - install manually 22
  - uninstall 29
  - upgrade in ePolicy Orchestrator 4.5 25, 48
  - upgrade with ePolicy Orchestrator 4.6 27, 50
agent command-line reference
  - config 51
  - disable command 53
  - enable command 53
  - excludepath command 53
  - ftypes command 53
  - help command 54
  - loglevel command 54
  - pp command 55
  - q command 55
  - status command 55
  - version command 56
agent deployment
  - overview 19
agent deployment package
  - add to Master Repository 18
Agentless deployment option
  - install extension 69
  - integration with ePolicy Orchestrator 71
  - policy management 71
alerts
  - changing behavior 42
  - message list 42
  - overview 42
anti-virus software
  - pre-installation issues 13
Artemis 38

### C
cache command 57
client tasks
  - agent deployment 20
  - assign agent deployment task 21
  - assign agent uninstall task 29
  - assign agent upgrade task 27, 50
  - create agent uninstall task 29
  - create agent upgrade task 26, 49
command-line reference
  - accessing agent 51
  - accessing offload scan server 57
  - agent config command 51
  - agent disable command 53
  - agent enable command 53
  - agent excludepath command 53
  - agent ftypes command 53
  - agent help command 54
  - agent loglevel command 54
  - agent pp command 55
  - agent q command 55
  - agent status command 55
  - agent version command 56
  - offload scan server config command 58
  - offload scan server help command 58
  - offload scan server loglevel command 59
  - offload scan server stats command 59
  - offload scan server version command 60
  - offload server cache command 57
communication
  - changing ports 41
  - default port 41
components
  - defined 63
  - overview 63
config command
  - agent 51
  - offload scan server 58
configuration
  - policy overview 33
  - SVA 68
conventions and icons used in this guide 7
Index

D
dashboards
  McAfee MOVE AntiVirus queries 38
deploy agent
ePolicy Orchestrator 4.5 19
deployment
  overview 12
  OVF 68
  strategy 12
disable command 53
documentation
  audience for this guide 7
  product-specific, finding 8
  typographical conventions and icons 7
download locations 15

E
enable command 53
ePolicy Orchestrator
  installation 18
  integration 33
  integration with Agentless 71
  restrictions 33
ePolicy Orchestrator extension
  upgrade 47
example
  creating a policy 36
excludepath command 53
extension
  uninstall 30
extensions
  Agentless deployment option 69
  VirusScan for Linux 69

F
file protection 43
ftypes command 53

G
Global Threat Intelligence
  benefits 38
  changing sensitivity 39
  overview 38
H
Health and Alarms page
  view 75
help command
  agent 54
  offload scan server 58
I
installation
  add agent package to Master Repository 18
  agent deployment overview 19
  assign agent upgrade task 27, 50
  assign deployment task 21
  common problems 31
  create agent deployment task 20
  create agent upgrade task 26, 49
  deploy agent with ePolicy Orchestrator 4.5 19
  deploy to VMware 21
  deploy to XenDesktop 22
  download software 15
  ePolicy Orchestrator 18
  manual agent install 22
  McAfee MOVE AntiVirus Offload Server 17
  overview 17
  requirements 13
  strategy 12
  test 74
  troubleshoot 31
  upgrade agent in ePolicy Orchestrator 4.5 25, 48
  upgrade ePolicy Orchestrator extension 47
  upgrade offload scan server 47
  upgrade overview 46
  upgrade scenario 45, 46
  VirusScan for Linux extension 69
  VMware Tools 67
  VMware vShield Endpoint 67
  vShield Manager 67

L
loglevel command
  agent 54
  offload scan server 59

M
Master Repository
  add agent deployment package 18
McAfee MOVE AntiVirus
  communication with ePolicy Orchestrator 33
  communication with offload scan server 41
  self-protection 43
  software packages 15
  uninstall 28
  upgrade strategies 45
McAfee MOVE AntiVirus Offload Scan Server
  installation 17
  uninstall 30
McAfee ServicePortal, accessing 8
messages
  list 42
  overview 42
mvadm
  cache command 57
  config command 39, 41, 51, 58
  disable command 53
  enable command 53
  excludepath command 53
  ftypes command 53
  help command 54, 58
  loglevel command 54, 59
  pp command 55
  q command 55
  stats command 59
  status command 55
  version command 56, 60

O
offload scan server
  changing communication port 41
  self-protection 43
  upgrade 47

offload scan server CLI
  config command 58
  help command 58
  loglevel command 59
  stats command 59
  version command 60

offload server CLI
  cache command 57
  open virtualization format
    deploy 68

P
policies
  Actions tab 34
  Agentless 71
  Alerts tab 34, 42
  application 33
  applying 35, 73
  categories 33
  changing quarantine behavior 39
  configuration overview 34
  configuring for Agentless 72
  create new 34
  creating a Scan policy 72
  creating an SVA policy 72
  enforcement 33
  example 36
  General tab 34, 36, 41
  inheritance 33
  options summary 34
  overview 33, 34
  Quarantine tab 34
  Scan 72
  Scan Items tab 34

Q
policies (continued)
  SVA 72
  tracking and tuning 33
  pp command 55
  prerequisites
    operating systems 16

Q
  q command 55
  quarantine
    changing behavior 39
    command-line access 55
    default behavior 39
    overview 39
  queries
    Compliance 37
    list 38
    McAfee MOVE AV queries 38
    reports 75
    VirusScan Enterprise 37

R
registry protection 43
  reports
    supplied queries 38
  requirements
    installation 13
    operating systems 65
    software 16, 65
    supported 16

S
security virtual appliance
  configure 68
  create a policy 72
  monitoring 74
  view status 75
  service protection 43
  ServicePortal, finding product documentation 8
  software compatibility 16
  stats command 59
  status command 55
  system requirements 16
  System Tray icon 42

T
Technical Support, finding product information 8
  threat event log 42, 74
  troubleshoot
    installation 31
U
uninstall process
  agent in ePolicy Orchestrator 4.6  29
  assign agent task  29
  create agent uninstall task  29
  ePolicy Orchestrator 4.5  28
  extension  30
  McAfee MOVE AntiVirus  28
  McAfee MOVE AntiVirus Offload Scan Server  30
 upgrade scenarios
  agent in ePolicy Orchestrator 4.5  25, 48
  create agent upgrade task  26, 49
  ePolicy Orchestrator extension  47
  higher downtime scenario  46
  higher resource scenario  45
  non-persistent VM  46
  offload scan server  47
  overview  46
  persistent VM  45
 upgrade scenarios (continued)
  strategy  45

V
version command
  agent  56
  offload scan server  60
 VMware
  deploy agents  21
  VMware vShield Endpoint
    deploy the SVA  67
    installation  67

W
Windows Event Log  42

X
XenDesktop
  deploy agent  22