Product Guide

McAfee MOVE AntiVirus (Agentless) 3.6.1
For use with McAfee ePolicy Orchestrator
COPYRIGHT
Copyright © 2015 McAfee, Inc., 2821 Mission College Boulevard, Santa Clara, CA 95054, 1.888.847.8766, www.intelsecurity.com

TRADEMARK ATTRIBUTIONS
Intel and the Intel logo are registered trademarks of the Intel Corporation in the US and/or other countries. McAfee and the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Evader, Foundscore, Foundstone, Global Threat Intelligence, McAfee LiveSafe, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee TechMaster, McAfee Total Protection, TrustedSource, VirusScan are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the US and other countries. Other marks 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

### 1 Introduction
- About MOVE AntiVirus (Agentless) ........................... 10
- Components and what they do ............................ 11
- Features ..................................... 12

### 2 MOVE AntiVirus (Agentless) configurations and deployment options
- Download the MOVE AntiVirus (Agentless) packages ................. 15
- Install the Data Center Connector for vSphere extension ............. 16
- Install the MOVE AntiVirus (Agentless) extension ..................... 16
- Install the VirusScan Enterprise for Linux extension .................. 17
- Setting up the SVM ................................ 18
  - MOVE SVM deployment options ........................... 18
  - Manually configure the MOVE SVM ........................ 19
- OVF properties ................................... 20

### 3 Deploying MOVE AntiVirus (Agentless) in an NSX environment
- Deploying the MOVE AntiVirus service (NSX) ....................... 23
- Requirements ................................... 24
- Download the MOVE AntiVirus (Agentless) packages ................. 26
- Register vCenter Server with NSX Manager .......................... 26
- Install the Data Center Connector for vSphere extension ............. 27
- Install the MOVE AntiVirus (Agentless) extension ..................... 28
- Register a VMware vCenter account with McAfee ePO .................. 28
- Set up a common configuration for McAfee ePO and MOVE SVM ....... 30
- Check in the MOVE SVM package to McAfee ePO ..................... 31
- Validate your NSX Manager using McAfee ePO ....................... 32
- Register the MOVE AntiVirus service on McAfee ePO ................. 34
  - MOVE AntiVirus (Agentless) policy export to NSX .................. 35
- Deploy the MOVE AntiVirus service using VMware vSphere Web Client .... 36
- Configuring the security group and security policy ................. 40
  - Create an NSX security policy ................................ 40
  - Create a global Security Group .............................. 42
  - Apply the NSX security policy to the NSX security group ............ 43
- Add hosts to your NSX cluster . ................................ 44
- Working with security tags .................................. 44
  - Enable NSX tagging through McAfee ePO ....................... 45
- Service Composer scenarios .................................. 46
  - Service Composer scenarios .............................. 46
4 Deploying MOVE AntiVirus in vCNS environment
Deploying the MOVE AntiVirus service (vCNS) ........................................ 51
Requirements ........................................................................ 51
Install the Data Center Connector for vSphere extension ................ 55
Install the MOVE AntiVirus (Agentless) extension ...................... 56
Register a VMware vCenter account with McAfee ePO ............... 56
Set up a common configuration for SVM deployment ................ 58
Check in the SVM package to McAfee ePO ............................. 59
Configure the IP Pool details .......................................... 59
Edit vShield Manager configuration .................................. 60
Deploy SVM using McAfee ePO ........................................ 62
View the SVM deployment details .................................... 66
Task type and status details ............................................. 67

5 Manual deployment of the SVM
Install VMware Endpoint .............................................. 69
Manually deploy the OVF .............................................. 69

6 Upgrading MOVE AntiVirus (Agentless)
Manual upgrade of the SVM ............................................ 71
Upgrade the extension ............................................... 71
Deploy a new MOVE SVM manually .................................. 72
Assign a policy ......................................................... 72
Upgrade MOVE AntiVirus (Agentless) in an NSX environment .... 73
Upgrade MOVE AntiVirus in vCNS environment ...................... 74

7 Uninstalling MOVE AntiVirus (Agentless)
Uninstalling MOVE AntiVirus (Agentless) 3.5.x or 3.6.0 in an NSX environment ........................................ 75
Remove MOVE AV service from the cluster ......................... 75
Remove the MOVE Guest Introspection Service from the security policy .......................... 75
Unregister the VMware NSX Manager from McAfee ePO ........... 76
Remove NSX Manager details from McAfee ePO .................... 76
Uninstall the extension .............................................. 76
Uninstall MOVE AntiVirus (Agentless) 3.6.1 in an NSX environment ........................................ 77
Remove MOVE AV service from the cluster ......................... 77
Remove the MOVE Guest Introspection Service from the security policy .......................... 77
Unregister the McAfee MOVE AV service using McAfee ePO ......................................................................................... 77
Uninstall the extension .............................................. 78
Uninstalling MOVE AntiVirus (Agentless) in a vCNS environment ........................................ 78
Remove SVM using McAfee ePO ........................................ 78
Uninstall the extension .............................................. 79

8 Monitoring and managing your environment
Integration with ePolicy Orchestrator .................................. 81
Policy management ......................................................... 81
Configuring policies ...................................................... 82
Configuring role-based access control for policies and SVM deployment ........................................ 86
How quarantine works ..................................................... 87
The restore tool at-a-glance ............................................. 87
Restore a file ............................................................. 88
Enabling the scan policy quarantine configuration .................... 89
Using the SVA policy quarantine settings ............................... 89
Configure the quarantine folder ...................................... 90
Set permissions for shared folders ................................... 90
How VM-based scan configuration works ............................ 91
Enable the VM-based scan configuration setting .................... 91
### Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan diagnosis</td>
<td>92</td>
</tr>
<tr>
<td>Create and run a scan diagnostic client task using McAfee ePO</td>
<td>92</td>
</tr>
<tr>
<td>Run the scan diagnostic tool using command line</td>
<td>92</td>
</tr>
<tr>
<td>Monitoring the SVM</td>
<td>94</td>
</tr>
<tr>
<td>View the Threat Event Log</td>
<td>94</td>
</tr>
<tr>
<td>View the Health and Alarms page</td>
<td>94</td>
</tr>
<tr>
<td>9 Queries and reports</td>
<td>95</td>
</tr>
<tr>
<td>Predefined MOVE AntiVirus (Agentless) queries</td>
<td>95</td>
</tr>
<tr>
<td>View default queries</td>
<td>97</td>
</tr>
<tr>
<td>Predefined datacenter queries</td>
<td>97</td>
</tr>
<tr>
<td>Data Center and Public Cloud dashboards</td>
<td>100</td>
</tr>
<tr>
<td>A Additional information</td>
<td>109</td>
</tr>
<tr>
<td>SVM security requirements</td>
<td>110</td>
</tr>
<tr>
<td>Install a vSphere Distributed Switch</td>
<td>110</td>
</tr>
<tr>
<td>Prepare ESXi servers</td>
<td>111</td>
</tr>
<tr>
<td>Install the guest introspection service</td>
<td>112</td>
</tr>
<tr>
<td>Frequently asked questions</td>
<td>115</td>
</tr>
<tr>
<td>Index</td>
<td>121</td>
</tr>
</tbody>
</table>
Preface

This guide provides the information you need to work with your McAfee product.

Contents

- About this guide
- Find product documentation

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 these typographical conventions and icons.

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

On the ServicePortal, you can find Information about a released product, including product documentation, technical articles, and more.

**Task**

1. Go to the ServicePortal at http://support.mcafee.com and click the Knowledge Center tab.
2. In the Knowledge Base pane under Content Source, select Product Documentation.
3. Select a product and version, then click Search to display a list of documents.
Introduction

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

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

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

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

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

**Agentless**

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

The Agentless deployment option:

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

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

**Multi-Platform**

This solution removes the need to install an anti-virus application on every VM. It is the original agent-based deployment option and unique network-based offloading that works on any hypervisor platform (including VMware vSphere).
The Multi-Platform deployment option offloads all scanning to a dedicated VM — an offload scan server — that runs McAfee VirusScan Enterprise software. Guest VMs are no longer required to run anti-virus software locally, which improves performance for anti-virus scanning, and increases VM density per hypervisor.

The Multi-Platform deployment option:

• Uses McAfee ePO to manage the MOVE AntiVirus configuration on the client systems, offload scan server, and SVM Manager (OSS Manager).

• Leverages the McAfee Agent for policy and event handling.

• Uses McAfee ePO for reports on viruses that are discovered on the VMs.

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

Contents

› About MOVE AntiVirus (Agentless)
› Components and what they do
› Features

About MOVE AntiVirus (Agentless)

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

The Agentless solution:

• Uses the VMware vShield Endpoint API to receive scan requests from VMs on the hypervisor

• Relies on McAfee® VirusScan® Enterprise for Linux for SVM protection and updates

• Uses McAfee® ePolicy Orchestrator® (McAfee ePO®) to manage the SVM

• Leverages the McAfee Agent for policy and event handling

• Uses McAfee ePO to provide reports on viruses that are discovered on the VMs
Components and what they do

Each component performs specific functions to keep your environment protected.

**ePolicy Orchestrator** — Allows you to configure policies to manage MOVE AntiVirus (Agentless) and provides reports on malware discovered within your virtual environment.

**Security Virtual Machine (SVM)** — Provides anti-virus protection for VMs and communicates with the loadable kernel module on the hypervisor, ePolicy Orchestrator, and the GTI servers. The SVM is the only system directly managed by ePolicy Orchestrator. VirusScan Enterprise for Linux, McAfee Agent, and MOVE AntiVirus (Agentless) come preinstalled.

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

**GTI (Global Threat Intelligence)** — Classifies suspicious files that are found on the file system. When the real-time malware defense detects a suspicious program, it sends a DNS request for analysis to a central database server hosted by McAfee Labs.
VMware vCenter — Console that manages the ESXi servers, which host the guest VMs that require protection.

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

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

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

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

Features

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

Centralized management

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

Optimized scanning

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

Flexible deployment

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

- VMware vCloud Networking and Security Manager (vCNS)-based deployment
- NSX Manager-based deployment
- Manual deployment

VMware vCNS-based deployment-based deployment

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

NSX Manager-based deployment

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

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

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

**Endpoint Scan and Security reports**

With the Data Center Connector for vSphere software, you can quickly retrieve the Endpoint Scan Report and Endpoint Security Report of all registered endpoints. For details, see *Data Center Connector for vSphere Product Guide*. 
MOVE AntiVirus (Agentless) configurations and deployment options

To set up your environment for MOVE AntiVirus (Agentless) deployment, you install VMware vShield Endpoint, configure the Security Virtual Machine (SVM), and install the product extensions.

VMware vShield Endpoint is installed on an ESXi host:
- As a loadable kernel module within the hypervisor
- As a filter driver within the guest VM

One SVM is required for each ESX hypervisor. Because of the architecture of vShield Endpoint, each ESX host must have access to the disk subsystem.

Contents
- Download the MOVE AntiVirus (Agentless) packages
- Install the Data Center Connector for vSphere extension
- Install the MOVE AntiVirus (Agentless) extension
- Install the VirusScan Enterprise for Linux extension
- Setting up the SVM
- Configure the MOVE SVM
- OVF properties

Download the MOVE AntiVirus (Agentless) packages

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

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

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

- MOVE AntiVirus (Agentless) OVF (MOVE-AV-AL_OVF_3.6.1.Zip)
- MOVE AntiVirus (Agentless) extension for ePolicy Orchestrator:
  - Main product extension — MOVE-AV-AL_EXT_3.6.1.Zip
  - License extensions — MOVE-AV-AL_License_EXT_3.6.1.Zip
- MOVE AntiVirus (Agentless) documentation package (MOV-AV-AL_DOCS_3.6.1.Zip)
- MOVE AntiVirus (Agentless) restore tool (MOVE-AV-AL_RestoreTool_3.6.1.Zip)

Install the Data Center Connector for vSphere extension

Download and install the Data Center Connector for vSphere extension on the McAfee ePO server to be able to discover the VM information and import it to the System Tree.

Before you begin

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

From the McAfee download site (http://www.mcafee.com/us/downloads/), you can download the extension for vSphere connector.

<table>
<thead>
<tr>
<th>Connector</th>
<th>Suite</th>
<th>Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Center Connector for vSphere</td>
<td>McAfee Server Security Advanced</td>
<td>vSphere_Ext_3.6.1.zip</td>
</tr>
<tr>
<td></td>
<td>McAfee Server Security Essential</td>
<td>vSphere_Ext_3.6.1.zip</td>
</tr>
</tbody>
</table>

Task

For details about product features, usage, and best practices, click ? or Help.

1 Log on to McAfee ePO as an administrator.
2 Select Menu | Software | Extensions | Install Extension.
3 Browse to and select the extension file for vSphere connector, then click OK.
4 Review the extension details and click OK.

Install the MOVE AntiVirus (Agentless) extension

A product's extension must be installed before McAfee ePO can manage the product.

Before you begin

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

Task

For option definitions, click ? in the interface.

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

<table>
<thead>
<tr>
<th>Extension</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main product extension</td>
<td>MOVE-AV-AL_EXT_3.6.1.Zip</td>
</tr>
<tr>
<td>License extension</td>
<td>MOVE-AV-AL_License_EXT_3.6.1.Zip</td>
</tr>
</tbody>
</table>

2 Log on to McAfee ePO as an administrator.
3 Select Menu | Software | Extensions | Install Extension.
Install the VirusScan Enterprise for Linux extension

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

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

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

Task

For option definitions, click ? in the interface.

1 Log on to McAfee ePO as an administrator.

2 Select Menu | Software | Extensions | Install Extension.

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

<table>
<thead>
<tr>
<th>Extension</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee Agent</td>
</tr>
<tr>
<td>McAfee VirusScan Enterprise for Linux</td>
</tr>
<tr>
<td>McAfee VirusScan Enterprise for Linux reports</td>
</tr>
</tbody>
</table>

For product package and extension details, see the product documentation for your version of McAfee Agent and McAfee VirusScan Enterprise for Linux.

4 Verify that the product name appears in the Extensions list.
Setting up the SVM

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

MOVE SVM deployment options

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

There are three MOVE SVM deployment options.

• **VMware vCloud Networking and Security Manager-based deployment** - You can check in the SVM and deploy it using McAfee ePO to one or more clusters. You can select one or more hosts, a group of hosts or an entire vCenter to deploy and specify the schedule for deployment. This deployment method allows you to deploy the SVM with all prerequisites necessary for a successful deployment of SVM.

• **VMware NSX Manager-based deployment** — You can register the SVM with VMware NSX Manager and deploy it automatically to one or more clusters. You can select one or more Network and Security services to deploy and specify the schedule for deployment.

• **Manual deployment** — You can manually deploy the SVM to each hypervisor from the vSphere Client. The vSphere Client must be connected to a vCenter server, and not directly to a hypervisor.

> The manual deployment of the SVM is a legacy method. So, we recommend that you use the McAfee ePO wizard-based deployments.

There are two configuration options.

• Automatic configuration

• Manual configuration

For details on different deployment and configuration options, see the relevant section in this document.

Configure the MOVE SVM

There are two MOVE SVM configuration options: automatic configuration and manual configuration.

• The MOVE SVM is automatically configured when you select any of these deployment options:
  • VMware vCloud Networking and Security Manager-based deployment
  • VMware NSX Manager-based deployment
  • Manual (Multiple OVF) deployment
  • When you provide the configuration information about the Properties page during manual deployment.

• If you select the Manual Deployment option and don’t provide the configuration information about the Properties page, you must manually configure the MOVE SVM.

The MOVE AntiVirus (Agentless) Security Virtual Machine (SVM) OVF (Open Virtualization Format) template has a preconfigured time zone, date, and time, using default values. So, the scheduled on-demand scans in MOVE AntiVirus (Agentless) start at a different time than what you have configured.
Task
1. Log on to the MOVE SVM using `svmadmin` account.
2. Run the command `sudo dpkg-reconfigure tzdata` to reconfigure the time zone.
3. When prompted, type your password.
4. Select your local geographic region and time zone from the list.
5. Run the command `sudo date -s "16 APR 2012 16:05:00"` to configure the date and time.
   
   * In this example, the date and time is configured to be: 16 April 2012 4:05 PM.
6. When prompted, type your password.

Tasks
- **Manually configure the MOVE SVM on page 19**
  The first time you log on, the configuration script automatically runs.

**Manually configure the MOVE SVM**
The first time you log on, the configuration script automatically runs.

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

<table>
<thead>
<tr>
<th>SVM</th>
<th>vCloud Networking and Security Manager</th>
<th>vCenter</th>
<th>ePolicy Orchestrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>IP address or DNS name</td>
<td>User name and password</td>
<td>Server IP address and console-to-application server communication port is required (default is 8443)</td>
</tr>
</tbody>
</table>

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

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

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

**Task**
1. Turn on the VM.
2. From the vSphere Client, open the console.
3. At the prompt, log on with these credentials:
   - User name: `svaadmin`
   - Password: `admin`
The configuration script runs automatically the first time you log on.

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

## OVF properties

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

<table>
<thead>
<tr>
<th>Category</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>Primary Server</td>
<td>The IP address of the primary DNS server.</td>
</tr>
<tr>
<td>DNS</td>
<td>Secondary Server</td>
<td>The IP address of the secondary DNS server.</td>
</tr>
<tr>
<td>ePolicy Orchestrator</td>
<td>FIPS Mode</td>
<td>Specified if FIPS mode is enabled on the ePolicy Orchestrator server.</td>
</tr>
<tr>
<td>ePolicy Orchestrator</td>
<td>IP Address</td>
<td>The IP address or DNS name of the ePolicy Orchestrator server.</td>
</tr>
<tr>
<td>ePolicy Orchestrator</td>
<td>Password</td>
<td>The user’s password.</td>
</tr>
<tr>
<td>ePolicy Orchestrator</td>
<td>Port</td>
<td>The console-to-application server communication port used when connecting to the ePolicy Orchestrator server. Default is 8443.</td>
</tr>
<tr>
<td>ePolicy Orchestrator</td>
<td>User name</td>
<td>The user name used to access the ePolicy Orchestrator server.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Category</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Type</td>
<td>How to configure the MOVE SVM's IP address for the management network (DHCP or static). Default is DHCP. When DHCP is specified, you don’t require to enter any other network settings. The DNS servers must be automatically discovered. Any DNS server specified overwrites the automatically discovered DNS server.</td>
</tr>
<tr>
<td>Network</td>
<td>Broadcast Address</td>
<td>The SVM's broadcast address.*</td>
</tr>
<tr>
<td>Network</td>
<td>Gateway</td>
<td>The MOVE SVM's default gateway.*</td>
</tr>
<tr>
<td>Network</td>
<td>IP Address</td>
<td>The static IP Address of the MOVE SVM.*</td>
</tr>
<tr>
<td>Network</td>
<td>Netmask</td>
<td>The netmask for the MOVE SVM's management network.*</td>
</tr>
<tr>
<td>Network</td>
<td>Network</td>
<td>The network for the MOVE SVM's static IP address.*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This property is optional. If this setting remains blank, it is created from the IP address and the Netmask.</td>
</tr>
<tr>
<td>SVA</td>
<td>Domain</td>
<td>The MOVE SVM's domain name and the default domain name for DNS queries.</td>
</tr>
<tr>
<td>SVA</td>
<td>Host name</td>
<td>The host name of the MOVE SVM.</td>
</tr>
<tr>
<td>SVA</td>
<td>savaadmin Password</td>
<td>The password of the savaadmin account.</td>
</tr>
<tr>
<td>Category</td>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>vCloud Networking and Security Manager</td>
<td>IP Address</td>
<td>The IP address or DNS name of the vCloud Networking and Security Manager.</td>
</tr>
<tr>
<td>vCloud Networking and Security Manager</td>
<td>Password</td>
<td>The password used to register the MOVE SVM with the vCloud Networking and Security Manager.</td>
</tr>
<tr>
<td>vCloud Networking and Security Manager</td>
<td>User name</td>
<td>The user name used to register the MOVE SVM with the vCloud Networking and Security Manager.</td>
</tr>
</tbody>
</table>

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

If you are deploying McAfee MOVE AV in an NSX environment, make sure that you leave the NSX-specific deployment parameters blank under **SVM**.
MOVE AntiVirus (Agentless) configurations and deployment options

OVF properties
Deploying MOVE AntiVirus (Agentless) in an NSX environment

Using McAfee ePO and vSphere Web Client, you can register the MOVE SVM with VMware NSX Manager, configure it, and deploy it to one or more clusters. This deployment automatically provides virus protection for virtual machines on a new hypervisor from the moment the hypervisor is added to the cluster.

Contents

- Deploying the MOVE AntiVirus service (NSX)
- Requirements
- Download the MOVE AntiVirus (Agentless) packages
- Register vCenter Server with NSX Manager
- Install the Data Center Connector for vSphere extension
- Install the MOVE AntiVirus (Agentless) extension
- Register a VMware vCenter account with McAfee ePO
- Set up a common configuration for McAfee ePO and MOVE SVM
- Check in the MOVE SVM package to McAfee ePO
- Validate your NSX Manager using McAfee ePO
- Register the MOVE AntiVirus service on McAfee ePO
- Deploy the MOVE AntiVirus service using VMware vSphere Web Client
- Configuring the security group and security policy
- Add hosts to your NSX cluster
- Working with security tags
- Service Composer scenarios

Deploying the MOVE AntiVirus service (NSX)

The extensions for Data Center Connector for vSphere and MOVE AntiVirus (Agentless) are installed on the McAfee ePO server, so that you can register the vCenter account and set up the NSX requirements. You must complete this process before deploying the MOVE AV service and configuring the policies.

For details about how to configure, monitor, and maintain the VMware NSX system with NSX Manager and vSphere Web Client, see NSX Administration Guide available at http://pubs.vmware.com/NSX-6/index.jsp.

Overview of the deployment process

The overall MOVE AV service deployment in an NSX environment consists of the following tasks.

The entire deployment process is only for an NSX environment and not for VMware vCloud Networking and Security (vCNS) environment.
1. Register vCenter Server with NSX Manager.

2. Install the extensions for Data Center Connector for vSphere and MOVE AntiVirus (Agentless) on McAfee ePO in this order:
   - Data Center Connector for vSphere
   - MOVE AntiVirus (Agentless)

3. Register a VMware vCenter account with McAfee ePO.

4. Set up a common configuration for McAfee ePO and SVM on the McAfee ePO server.

5. Check in the SVM package to McAfee ePO.

6. Test the NSX Manager connection to the McAfee ePO server by validating the credentials of the NSX Manager. You can view the registration status of the NSX Manager and register it, if required.

7. Register the MOVE AV service on the McAfee ePO server.

8. Verify the policy export details in vSphere Web Client.


10. Apply the NSX Security Policy to the NSX Security Group.

11. Deploy the MOVE AV service using vSphere Web Client.

12. Apply MOVE AntiVirus (Agentless) protection to your VMs.

### Requirements

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

#### SVM requirements

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

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

The McAfee Security Virtual Machine (SVM) 3.6.1 package must be checked in to McAfee ePO. The SVM VM is built to meet these minimum hardware requirements:

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

These items come preinstalled:

- **Operating system**: Ubuntu 12.04.5
- **Software**: VirusScan Enterprise for Linux 2.0.2.29099
  - McAfee Agent 4.8
  - MOVE AntiVirus (Agentless)

![We recommend that you set the SVM's time zone, date, and time to match your McAfee ePO server. Otherwise, the on-demand scan (ODS) does not start at the time that you specify.]
**VMware requirements**

You must be running this VMware software:

- VMware vSphere
  - VMware vCenter 5.5 U2 or 6.0
  - VMware ESXi 5.5 U2 or 6.0
- VMware NSX Manager 6.1.2, 6.1.4 or later

⚠️ Your NSX Manager account must have administrative permissions.

Your NSX datacenter must meet these configuration requirements:

- The datacenter must be using a vSphere Distributed Switch (vDS). For details about installing this switch, see *Install a vSphere Distributed Switch in Additional information*.
- ESXi servers must be connected to the vDS.
- Your ESXi servers must be grouped into clusters, even if you have only a single ESXi in a single cluster. The ESXi servers must be connected to the vDS before they are moved into clusters.
- Your ESXi servers must be prepared by installing the drivers that allow network traffic inspection. For details about host preparation, see *Prepare ESXi servers in Additional information*.
- Guest Introspection service must be installed on all ESXi servers. For details, see *Install the Guest Introspection Service in Additional information*.
- Virtual machines must belong to an NSX Security Group.
- Virtual machines must have the latest VMware Tools installed, including the VMware Endpoint Driver.

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

For information about the Guest VM operating systems that are supported for VMware vShield Endpoint, see the VMware 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)

**McAfee ePO requirements**

- McAfee ePO 4.6.8, 5.1.0, 5.1.1, or 5.3.0

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

**Data Center Connector for vSphere requirements**

- Data Center Connector for vSphere 3.6.1

⚠️ Version 3.6.1 extension of Data Center Connector for vSphere is a minimum requirement for upgrading to MOVE AntiVirus (Agentless) 3.6.1 in an NSX environment.
Download the MOVE AntiVirus (Agentless) packages

Download these packages before they can be installed on virtual systems or the McAfee ePO server.

The OVF package and McAfee ePO extensions are required. The Help extension and documentation package are optional.

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

- MOVE AntiVirus (Agentless) OVF (MOVE-AV-AL_OVF_3.6.1.Zip)
- MOVE AntiVirus (Agentless) extension for McAfee ePO:
  - Main product extension — MOVE-AV-AL_EXT_3.6.1.Zip
  - License extension — MOVE-AV-AL_License_EXT_3.6.1.Zip
  - Help extension — MOVE-AV-AL_HELP_EXT_3.6.1.Zip
- MOVE AntiVirus (Agentless) documentation package (MOV-AV-AL_DOCS_3.6.1.Zip)
- MOVE AntiVirus (Agentless) restore tool (MOVE-AV-AL_RestoreTool_3.6.1.Zip)

Register vCenter Server with NSX Manager

Log on to the NSX Manager virtual appliance console to register a vCenter Server and review the settings specified during installation.

Before you begin

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

Task

1. Log on to the NSX Manager virtual appliance console as an administrator.
2. Under NSX Manager Virtual Appliance Management, click Manage Appliance Settings.
3. From the left panel, select NSX Management Service and click Edit next to vCenter Server.
4 Type the IP address, vCenter user name, and password of the vCenter Server, then click **OK**.

5 Confirm that the vCenter Server status is **Connected**.

---

**Install the Data Center Connector for vSphere extension**

Download and install the Data Center Connector for vSphere extension on the McAfee ePO server to be able to discover the VM information and import it to the **System Tree**.

**Before you begin**

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

This extension, together with the MOVE AntiVirus (Agentless) extension, automatically detects and sends the details of your NSX Managers to the McAfee ePO server. However, these NSX Managers are not registered with McAfee ePO.

From the McAfee download site (http://www.mcafee.com/us/downloads/), you can download the extension for vSphere connector.

<table>
<thead>
<tr>
<th>Connector</th>
<th>Suite</th>
<th>Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Center Connector for vSphere</td>
<td>McAfee Server Security Advanced</td>
<td>vSphere_Ext_3.6.1.zip</td>
</tr>
<tr>
<td></td>
<td>McAfee Server Security Essential</td>
<td>vSphere_Ext_3.6.1.zip</td>
</tr>
</tbody>
</table>

Version 3.6.1 extension of Data Center Connector for vSphere is a minimum requirement for installing MOVE AntiVirus (Agentless) 3.6.1 in an NSX environment.
Task
For details about product features, usage, and best practices, click ? or Help.

1 Log on to McAfee ePO as an administrator.
2 Select Menu | Software | Extensions | Install Extension.
3 Browse to and select the extension file for vSphere connector, then click OK.
4 Review the extension details and click OK.

Install the MOVE AntiVirus (Agentless) extension
A product’s extension must be installed before McAfee ePO can manage the product.

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

Task
For option definitions, click ? in the interface.

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

<table>
<thead>
<tr>
<th>Extension</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main product extension</td>
<td>MOVE-AV-AL_EXT_3.6.1.Zip</td>
</tr>
<tr>
<td>License extension</td>
<td>MOVE-AV-AL_license_EXT_3.6.1.Zip</td>
</tr>
</tbody>
</table>

2 Log on to McAfee ePO as an administrator.
3 Select Menu | Software | Extensions | Install Extension.
4 Browse to and select the extension file, then click OK.
5 Verify that the product name appears in the Extensions list.

Register a VMware vCenter account with McAfee ePO
To enable and manage the security of the virtual machines in your datacenter with MOVE AntiVirus (Agentless), you must first add the vCenter to the McAfee ePO server. This is the same vCenter account that you already registered with NSX Manager.

Before you begin
Make sure that you have configured your VMware vCenter server that manages the ESXi servers, which host the guest VMs.
Task
For details about product features, usage, and best practices, click ? or Help.

1 Log on to McAfee ePO as an administrator.

2 Select Menu | Configuration | Registered Cloud Accounts, then click Add Cloud Account to open the Add Cloud Account page.

3 From the Choose Connector drop-down list on the Description page, select VMware vSphere, then click OK.

4 On the vCenter Account Details page, type these details:
   - **Account Name** — A name for the VMware vCenter account in McAfee ePO. Account names can include characters a–z, A–Z, 0–9, and [_.-], without space.
   - **Server Address** — (Required) IP address or the host name of the available VMware vCenter.
   - **vCenter User Name** — (Required) User name of the available VMware vCenter account.
     - This user’s minimum role can be read-only.
     - This user can be a domain account.
     - This user can also be a Single-Sign-On (SSO) user.
   - **vCenter Password** — (Required) Password of the available VMware vCenter account.
   - **Connection Protocol** — The protocol required to establish the connection with the VMware vCenter.
   - **Sync Interval (In Minutes)** — Specify the interval for running the next vCenter discovery. The default value is 5 minutes.
   - **Port No** — The port number required to establish the connection with the available VMware vCenter.
   - **Tag** — The administrator specifies this to identify the VMs. Tag name can include characters a–z, A–Z, 0–9, and [_.-], with space.
5 Click **Test Connection** to validate VMware vCenter account details and verify the connection to the VMware vCenter, then click **Next** to open the Validate Certificate page.

6 Click **Accept** to validate the certificate, then click **Finish**.

7 When prompted to confirm, click **OK** to register the vCenter account.

This action registers the VMware vCenter and imports all discovered virtual machines, which are unmanaged, into the System Tree. The instances are imported with the similar structure and hierarchy present in VMware vCenter.

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

8 View the imported VMs: select **Menu | Systems | System Tree** in McAfee ePO.

After the discovery, you can find your vCenter account under the group **vSphere**. The clusters and hosts from vCenter are logically grouped under each datacenter group in McAfee ePO.

---

### Set up a common configuration for McAfee ePO and MOVE SVM

Before deploying MOVE SVM, complete this common configuration on the McAfee ePO server, so that these settings are retrieved and used for every MOVE SVM deployment.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1 Log on to McAfee ePO as an administrator.

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

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

   **Table 3-1  McAfee ePO credentials**

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Type the password of the McAfee ePO console that the administrator has currently logged on.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Retype the password.</td>
</tr>
</tbody>
</table>
Table 3-2  MOVE SVM configuration

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>Type a unique prefix that is added to the host name of the MOVE SVM. The prefix can include characters a–z, A–Z, 0–9, and [-], without space.</td>
</tr>
<tr>
<td>Prefix</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>Type a password to be used as the MOVE SVM password during deployment.</td>
</tr>
<tr>
<td></td>
<td>• The password must be at least 6 characters long.</td>
</tr>
<tr>
<td></td>
<td>• The password must contain at least one uppercase letter (A–Z) and one numeral (0–9).</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Retype the password.</td>
</tr>
<tr>
<td>NSX tagging</td>
<td>• <strong>NSX Virus Found Tag</strong> — Enable this option so that the VM is tagged with the ANTI_VIRUS.VirusFound.threat=high tag on detecting malware.</td>
</tr>
<tr>
<td></td>
<td>Here is the sequence of untagging:</td>
</tr>
<tr>
<td></td>
<td>1 The ANTI_VIRUS.VirusFound.threat=high tag is automatically removed from the VMs when the first on-demand scan starts after tagging.</td>
</tr>
<tr>
<td></td>
<td>2 If malware is detected during the on-demand scan, an action is taken as defined in the policy.</td>
</tr>
<tr>
<td></td>
<td>3 The VM is again tagged with ANTI_VIRUS.VirusFound.threat=high.</td>
</tr>
<tr>
<td></td>
<td>4 The same VM is again untagged when the next on-demand scan starts. It remains untagged if no malware is found.</td>
</tr>
<tr>
<td></td>
<td>• <strong>NSX Unprotected Tag</strong> — Enable this option to automatically retrieve the details of the unprotected VMs, tag them with MCAFEE.MOVE.unprotected=yes, and display them on NSX Manager. This tag resource indicates that these VMs are not protected by MOVE AntiVirus (Agentless). By default, this option is enabled.</td>
</tr>
<tr>
<td></td>
<td>The MCAFEE.MOVE.unprotected=yes tag is automatically removed from the VMs when they are protected.</td>
</tr>
</tbody>
</table>

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

---

### Check in the MOVE SVM package to McAfee ePO

Check in and host the MOVE SVM package in McAfee ePO, so that it is available with VMware NSX Manager to deploy it to the cluster. You can view and delete the MOVE SVM package using McAfee ePO.

**Before you begin**

• Verify that you installed the MOVE AntiVirus (Agentless) extension.

~!~ For a successful check-in, do not change the file name of the MOVE SVM package.
Task
For details about product features, usage, and best practices, click ? or Help.

1  Log on to McAfee ePO as an administrator.

2  Select Menu | Automation | MOVE AV Agentless.

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

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVM Name</td>
<td>Name of the MOVE SVM package checked in to McAfee ePO.</td>
</tr>
<tr>
<td>SVM Version</td>
<td>Version of the MOVE SVM package checked in to McAfee ePO.</td>
</tr>
<tr>
<td>SVM Use Count</td>
<td>Specifies the number of hypervisors that are using this MOVE SVM.</td>
</tr>
<tr>
<td>Action</td>
<td>• Delete — To remove an existing MOVE SVM when it is not registered with any NSX Manager.</td>
</tr>
</tbody>
</table>

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

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

⚠️ You can check in up to three versions of MOVE SVM starting from 3.5.

Validate your NSX Manager using McAfee ePO
The Data Center Connector for vSphere extension, together with the MOVE AntiVirus (Agentless) extension, automatically detects and sends the details of your NSX Managers to the McAfee ePO server. However, these NSX servers are not registered with McAfee ePO.

Before you begin
- You have created and configured NSX Manager.
- You have registered the vCenter account with NSX Manager.

Using this configuration available on the McAfee ePO server, you can edit the details and validate the credentials of your NSX Manager. From here, you can also register your vCenter server with NSX Manager.

Task
For details about product features, usage, and best practices, click ? or Help.

1  Log on to McAfee ePO as an administrator.

2  Select Menu | Automation | MOVE AV Agentless.
3. From the Configuration tab, click NSX Manager. The NSX Manager: Registration page appears with these details.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Manager Address</td>
<td>Displays the IP address or the host name of your NSX Manager.</td>
</tr>
<tr>
<td>NSX Manager Name</td>
<td>Displays the name of your NSX Manager.</td>
</tr>
<tr>
<td>vCenter Account</td>
<td>Displays the name of the registered vCenter account.</td>
</tr>
<tr>
<td>Action</td>
<td>Edit — Click to edit and validate the credentials and other details of the NSX Managers, which are automatically detected and sent to McAfee ePO.</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Account</td>
<td>Specifies the name of the registered vCenter account.</td>
</tr>
<tr>
<td>NSX Manager Name</td>
<td>Specifies the name of the available NSX Manager.</td>
</tr>
<tr>
<td>NSX Manager Address</td>
<td>Type the IP address or the host name of the available NSX Manager.</td>
</tr>
<tr>
<td>NSX Manager Port</td>
<td>Specifies the port number of NSX Manager.</td>
</tr>
<tr>
<td>NSX Manager Username</td>
<td>Type the user name of the available NSX Manager.</td>
</tr>
<tr>
<td>NSX Manager Password</td>
<td>Type the password of the available NSX Manager.</td>
</tr>
</tbody>
</table>

- Make sure that the credentials have administrative permissions.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Account:</td>
<td>SK-vc-1</td>
</tr>
<tr>
<td>NSX Manager Name:</td>
<td>SK-NSX-511</td>
</tr>
<tr>
<td>NSX Manager Address:</td>
<td>10.213.14.5</td>
</tr>
<tr>
<td>NSX Manager Port:</td>
<td>443</td>
</tr>
<tr>
<td>NSX Manager Username:</td>
<td>admin</td>
</tr>
<tr>
<td>NSX Manager Password:</td>
<td>*******</td>
</tr>
</tbody>
</table>

5. Click Validate to verify the credentials of the NSX Manager and check that the connection to the NSX Manager works.

6. Click Save to store the NSX Manager account details.
Register the MOVE AntiVirus service on McAfee ePO

After registering your vCenter account details to NSX Manager and McAfee ePO, you must enable the registration of MOVE AntiVirus (Agentless) as a service within NSX Manager using McAfee ePO. The details of the registered vCenter, SVM, and NSX Manager are automatically retrieved and displayed on the McAfee ePO server. However, you must register the MOVE AntiVirus service with the vCenter account using McAfee ePO. This registration permits the deployment of the MOVE AntiVirus service to the ESXi servers, which is the next task.

Task
For details about product features, usage, and best practices, click ? or Help.

1. Log on to McAfee ePO as an administrator.

2. Select Menu | Automation | MOVE AV Agentless.

3. From the Service tab, click NSX Manager to open the MOVE Service Registration page with these details.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Manager Name</td>
<td>Displays the name of the registered NSX Manager.</td>
</tr>
<tr>
<td>NSX Manager Address</td>
<td>Displays the IP address of your NSX Manager.</td>
</tr>
<tr>
<td>vCenter Account</td>
<td>Displays the name of the vCenter account that is registered with NSX Manager and McAfee ePO.</td>
</tr>
<tr>
<td>Registered SVM Version</td>
<td>Displays the version of the SVM checked in to McAfee ePO.</td>
</tr>
<tr>
<td>Service Registration Status</td>
<td>Displays these registration status values:</td>
</tr>
<tr>
<td></td>
<td>• Registered — Indicates that the MOVE AntiVirus service is registered and ready for deployment.</td>
</tr>
<tr>
<td></td>
<td>• Not Registered — Indicates that the MOVE AntiVirus service is not registered.</td>
</tr>
<tr>
<td></td>
<td>• Registration Failed — Indicates that the MOVE AntiVirus service failed.</td>
</tr>
<tr>
<td></td>
<td>• Register — Click to select the latest SVM and register it to the vCenter that is added to your NSX Manager.</td>
</tr>
<tr>
<td></td>
<td>• Unregister — Click to unregister the MOVE AntiVirus service and to remove it from the vCenter that is added to your NSX Manager.</td>
</tr>
<tr>
<td></td>
<td>• Upgrade — Click to upgrade the MOVE AntiVirus service.</td>
</tr>
<tr>
<td>Action</td>
<td>Make sure that you have checked in the latest SVM required for the upgrade.</td>
</tr>
</tbody>
</table>

4. Click Register under Actions to open the MOVE Service registration dialog box.
5 Select the latest MOVE SVM and click OK. The MOVE AntiVirus service is now registered with the vCenter account that is registered with your NSX Manager.

6 Verify that the MOVE AntiVirus service is now available under Networking & Security | Service Definitions in the VMware vSphere Web Client console.

![Image of vSphere Web Client console]

The MOVE AntiVirus (Agentless) Scan policies are exported from McAfee ePO to NSX in real time.

**MOVE AntiVirus (Agentless) policy export to NSX**

After you register the MOVE AntiVirus service in on McAfee ePO server, the MOVE AntiVirus (Agentless) Scan policies are exported from McAfee ePO to NSX in real time.

The exported policies are available in Profile Configurations under Networking & Security | Service Definitions | McAfee MOVE AV | Actions | Edit settings | Manage | Profile Configurations with a policy ID and description.

![Image of Profile Configurations]

Only the Scan policies are exported from McAfee ePO to NSX Manager.

When you create or change a MOVE AntiVirus (Agentless) policy in McAfee ePO, it is immediately exported to Profile Configurations in vSphere Web Client. This real-time policy export helps the VMware administrator understand the different set of policies created and changed by the administrator.

![Image of MOVE AV Agentless policies on McAfee ePO]

Changes to MOVE AntiVirus (Agentless) policy names in McAfee ePO are not updated in NSX. You must manually update the name changes in NSX.

When you delete a MOVE AntiVirus (Agentless) Scan policy from McAfee ePO, it is deleted from NSX Manager if it is not included in any of the NSX security policies.

We recommend that you verify the security policy in NSX before deleting any MOVE AntiVirus (Agentless) Scan policy from McAfee ePO.
You cannot delete the MOVE AntiVirus (Agentless) policy in NSX Manager when it is included in any NSX security policy. You must remove all configuration referring to this policy before deleting it.

**Deploy the MOVE AntiVirus service using VMware vSphere Web Client**

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

**Before you begin**

- The host, where you are deploying the SVM using NSX Manager, must be part of a cluster.
- The datacenter must be using a vSphere Distributed Switch (vDS). For details, see *Install a vSphere Distributed Switch in Additional information*.
- Guest Introspection service must be installed on all ESXi servers. For details, see *Install the Guest Introspection Service in Additional information*.
- Virtual machines must have the latest VMware Tools installed, including the vShield Driver: VMware Tools 5.0 (Patch 1 ESX500-201109402-BG).
- Make sure that you have appropriate permission to perform the SVM deployment using McAfee ePO. You can enable this permission by navigating through Menu | Users | Permission Sets | MOVE AV [Agentless] SVM Deployment | Edit.

Using the VMware vSphere Web Client console, you can deploy the MOVE AntiVirus services on a set of clusters. Manage service deployments here by adding new services or deleting existing ones.

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

Make sure that you enabled the **VM-based scan configuration** option available under the MOVE AntiVirus (Agentless) SVM policy in McAfee ePO. For details, see *How VM-based scan configuration works*. 

---

Mcafee MOVE AntiVirus (Agentless) 3.6.1 Product Guide
Task

1. Log on to the VMware vSphere Web Client as a root user.

2. Click Home | Networking & Security | Installation | Service Deployments, then click the green + icon to display the Deploy Network & Security Services window.

3. From Select services & schedule, select the McAfee MOVE AV service and click Next.

   You can deploy immediately, or you can schedule for a later deployment.
4 From Select clusters, select the cluster that includes the ESXi servers on which to deploy the MOVE AntiVirus service, then click Next.
5 From **Select storage and Management Network**, for each cluster, select a datastore on which to store the MOVE SVM, the network (the distributed port group used by the vDS on the datacenter), and the IP assignment for the MOVE AntiVirus service to use.

![Select storage and Management Network](image)

The selected datastore must be available on all hosts in the selected cluster. Or, you can select **Specified on host**. If you are assigning static IP pools in the IP Assignment column to the MOVE AntiVirus service or Guest Introspection service, make sure that your default gateway and DNS is reachable/resolvable and the prefix length is correct. If not, the MOVE AntiVirus and Introspection service VMs are not activated and they cannot communicate to the NSX manager or McAfee ePO because their IPs are not on the same network as McAfee ePO or the NSX Manager.

If you selected **Specified on host**, the datastore for the ESXi host must be specified in the **AgentVM Settings** of the host before it is added to the cluster. For details, see vSphere API/SDK documentation. For details about configuring this network and IP address range with NSX Manager and vSphere Web Client, see *NSX Administration Guide* available at [http://pubs.vmware.com/NSX-6/index.jsp](http://pubs.vmware.com/NSX-6/index.jsp).

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

![Warning](image)

Make sure that you migrate all host networks and VMs to the DVport group.
7 Review the settings and click Finish to complete the deployment of MOVE AntiVirus service.

When deployment is complete, the MOVE AntiVirus service appears in the list of Network & Security Service Deployments. This action initiates the SVM deployment to all hypervisors in the selected cluster. The SVM deployment might take a few minutes to complete. You can then view the managed SVM in the System Tree of McAfee ePO.

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

8 After deploying the SVM, view these Service status details on the VMware vSphere Web Client console.

<table>
<thead>
<tr>
<th>Service Status</th>
<th>ID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNKNOWN</td>
<td>3</td>
<td>Specifies that the MOVE AntiVirus service status is unknown.</td>
</tr>
<tr>
<td>UP</td>
<td>N/A</td>
<td>Not applicable.</td>
</tr>
<tr>
<td>DOWN</td>
<td>1</td>
<td>Specifies that the MOVE AntiVirus service is stopped.</td>
</tr>
</tbody>
</table>

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

### Configuring the security group and security policy

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

The security policies for MOVE AntiVirus (Agentless) are automatically exported from the McAfee ePO server after you register the MOVE AntiVirus service on McAfee ePO. This configuration is a one-time initial activity for a vCenter. However, you must repeat this configuration when a new datacenter is added.

#### Create an NSX security policy

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

**Before you begin**

- The MOVE AntiVirus (Agentless) extension is installed on the McAfee ePO server.
- The MOVE AntiVirus service is already registered with McAfee ePO.
Task

1. In your vSphere Web Client, go to Home | Networking & Security | Service Composer and click the Security Policies tab, then click the New Security Policy icon.

2. Specify a unique user-friendly name and any details to identify the security policy, then click Next to open the Guest Introspection Service page.

3. Click the green plus sign to add a Guest Introspection Service. Provide a name for the Guest Introspection Service and define the following settings:

<table>
<thead>
<tr>
<th>For this...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type the name of the MOVE AntiVirus service.</td>
</tr>
<tr>
<td>Description</td>
<td>Type some details about the MOVE AntiVirus service, which help you to identify the SVM.</td>
</tr>
</tbody>
</table>
| Action      | • Apply — Select this to apply the SVM.  
              • Block — Select this to block the SVM. |
| Service Type| From the drop-down list, select Anti Virus. |
| Service Name| From the drop-down list, select McAfee MOVE AV. |
| Service Profile| McAfee MOVE AV_My Default-XX (Anti Virus) |

These are the profile configurations exported from McAfee ePO. If you create a policy or change an existing MOVE AntiVirus (Agentless) policy using McAfee ePO, it is immediately exported and available here to include for creating the security policy. However, any change to the name and description is not updated to NSX. You must manually update them, if necessary.
### For this... Do this...

<table>
<thead>
<tr>
<th>State</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Enabled — Select this to enable the service.</td>
<td></td>
</tr>
<tr>
<td>• Disabled — Select this to disable the service.</td>
<td></td>
</tr>
</tbody>
</table>

| Enforce | Yes |

---

4  Click OK in the **Add Network Inspection Service** dialog box, and click Finish to complete and close the **New Security Policy** page.

You have created your NSX security policy for deploying MOVE AntiVirus (Agentless).

### Create a global Security Group

You can select the necessary datacenters or their clusters from the available vCenter and configure them as a security group, so that you can assign the security policy to this group and protect its VMs.

#### Before you begin
- The MOVE AntiVirus (Agentless) extension is installed on the McAfee ePO server.
- VMware vSphere 5.5 is installed and added to the cluster.
- The MOVE AntiVirus service is registered with VMware NSX Manager using McAfee ePO.

#### Task
1  Log on to the VMware vCenter Web Client as a root user.

2  In your **vSphere Web Client**, go to Home | Networking & Security | Service Composer and click on the Security Groups tab, then click the **New Security Group** icon.

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

4  Keep the default configuration for the dynamic membership criteria that objects must meet to be part of this security group, then click Next to open the **Select objects to include** page.
5 From the **Object Type** drop-down list, select the required datacenter or cluster and select your objects to be protected, then click **Next** to open the **Select objects to exclude** page.

![Select objects to include](image)

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

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

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

Your Security Group is added and it contains the virtual machines to be protected from the selected cluster.

![Security Group](image)

**Apply the NSX security policy to the NSX security group**

Apply the security policy to the security group containing the VMs you want to protect.

**Before you begin**

- The MOVE AntiVirus (Agentless) extension is installed on the McAfee ePO server.
- The MOVE AntiVirus service is already registered with McAfee ePO.

Map a security policy (say **SP1**) to a security group (say **SG1**). The MOVE AntiVirus service and policy settings from McAfee ePO configured for **SP1** are applied to all virtual machines that are members of **SG1**.

**Task**

1 Log on to the VMware vSphere Web Client as a root user.

2 Go to **Home** | **Networking & Security** | **Service Composer**.
3. From the **Security Policies** tab, select the new security policy you have created, then click the **Apply Security Policy** icon.

4. In the **Apply Policy to Security Groups** window, select the security group that contains the VMs you want to protect and click **OK**.

The selected NSX security policy is now applied to all VMs in the selected NSX security group. The VMs from the selected security group are now protected according to the MOVE AntiVirus (Agentless) policy that is exported from McAfee ePO.

---

### Add hosts to your NSX cluster

Add an ESXi server to an NSX cluster that is protected by MOVE AntiVirus (Agentless). Make sure to complete the steps in the order described here.

**Task**

1. Add the host to the datacenter, but not directly to the cluster.
2. Connect the host to the Distributed Switch.
3. Move the host into the cluster.

When the host is moved into the cluster, the MOVE AntiVirus service is deployed automatically.

---

### Working with security tags

Begin by creating a security group to define the assets that you want to protect. Security groups might be static (including specific virtual machines) or dynamic where membership might be defined in one or more of the following ways.

- Regular expressions such as virtual machines with the name *VM1*
- vCenter containers such as cluster, datacenter, or port group
- Security tags, IPset, MACset, or other security groups

For example, you might include a criterion to add to the security group all members tagged with the specified security tag (such as `ANTI_VIRUS.VirusFound.threat=high`).

If you select a security group defined by virtual machines that have a certain security tag applied to them, you can create a dynamic or conditional workflow. The moment the tag is applied to a virtual machine, the virtual machine is automatically added to that security group.

Security group membership changes constantly. For example, a virtual machine tagged with the `ANTI_VIRUS.VirusFound.threat=high` or `MCAFEE.MOVE.unprotected=yes` tag can be moved into a dynamic security group that you configure (say `Quarantined`).

**MOVE AntiVirus (Agentless) tag**

After installing the MOVE AntiVirus (Agentless) extension and registering the MOVE AntiVirus service in McAfee ePO, the tag applied in your environment appears with details about the virtual machines where the tag has been applied. `MCAFEE.MOVE.unprotected=yes` is the MOVE AntiVirus (Agentless) tag.

Write down the exact tag name for adding a security group to include virtual machines with these tags.
You can view security tags applied on a virtual machine or create a user-defined security tag. For more information about adding, editing, assigning, and deleting security tags in your virtual environment, see *NSX Administration Guide*.

**Enable NSX tagging through McAfee ePO**

Using McAfee ePO, you can create a Scan policy that has the configurations required for high security.

**Before you begin**
- Make sure that you have registered the MOVE AntiVirus service in McAfee ePO.
- Make sure that you have specified your vCenter details in the **General Settings** tab of the MOVE AntiVirus (Agentless) **SVA** policy in McAfee ePO. For details, see *Create an SVA policy*.

Registering the MOVE AntiVirus service exports all Scan policies of MOVE AntiVirus (Agentless) from McAfee ePO to NSX. When a new scan policy is added or an existing scan policy is changed, all updates are immediately exported to NSX. These policies are included in the NSX security policy and are mapped to the NSX security group.

Using the **NSX tagging** option, this policy can be automatically assigned to a VM that has been tagged as **MCAFEE.MOVE.unprotected=yes** or **ANTI_VIRUS.VirusFound.threat=high**.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. Log on to McAfee ePO as an administrator.
2. Select **Menu** | **Automation** | **MOVE AV Agentless**.
3. From the **Configuration** tab, click **General** and select these tagging options under **NSX tagging**.
   - **NSX Virus Found Tag** — Enable this option so that the VM is tagged with **ANTI_VIRUS.VirusFound.threat=high** on detecting a malware.
     
     Here is the sequence of untagging:
     1. The **ANTI_VIRUS.VirusFound.threat=high** tag is automatically removed from the VMs when the first on-demand scan starts after tagging.
     2. If malware is detected during the on-demand scan, an action is taken as defined in the policy.
     3. The VM is again tagged with **ANTI_VIRUS.VirusFound.threat=high**.
     4. The same VM is again untagged when the next on-demand scan starts. It remains untagged if no malware is found.

   - **NSX Unprotected Tag** — Enable this option to automatically retrieve the details of the unprotected VMs, tag them with **MCAFEE.MOVE.unprotected=yes**, and display them on the NSX Manager. This tag resource indicates that these VMs are not protected by MOVE AntiVirus. By default, this option is enabled.

     The **MCAFEE.MOVE.unprotected=yes** tag is automatically removed from the VMs when they are protected.

Virtual machines tagged with the **MCAFEE.MOVE.unprotected=yes** tag can be moved into a dynamic security group that you configure (say **Quarantined**) and protected with MOVE AntiVirus Scan policies.
Service Composer scenarios

Here are some hypothetical scenarios for Service Composer from vSphere Web Client. Assume that different roles and permissions for Security Administrator and VM Administrator have been defined.

**Service Composer scenarios**

With MOVE AntiVirus (Agentless), Service Composer can identify infected systems in virtual environments and quarantine them to prevent further outbreaks.

**Before you begin**

- Make sure that you registered the MOVE AntiVirus service in McAfee ePO.
- Make sure that you enabled the NSX tagging option in McAfee ePO.

---

MOVE AntiVirus (Agentless) tags unprotected virtual machines with **MCAFEE.MOVE.unprotected=yes**

This sample scenario shows how you can protect your virtual machines end to end.

---

**Figure 3-1  Service composer conditional workflow**
**Task**

1. Install, register, and deploy the McAfee MOVE AV (Agentless) extension and service.

2. Create an NSX security policy for your desktops.
   - b. In Name, type DesktopPolicy.
   - c. In Description, type Antivirus scan for all desktops.
   - d. Under Advanced options, change the weight to 51000. The policy precedence is set high to ensure that it is enforced above all other policies.
   - e. Click Next.
   - f. On the Guest Introspection Service page, click and fill in these values.

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Desktop AV</td>
</tr>
<tr>
<td>Description</td>
<td>Mandatory policy to be applied on all desktops</td>
</tr>
<tr>
<td>Action</td>
<td>Accept the default value.</td>
</tr>
<tr>
<td>Service Type</td>
<td>From the drop-down list, select Anti Virus.</td>
</tr>
<tr>
<td>Service Name</td>
<td>From the drop-down list, select McAfee MOVE AV.</td>
</tr>
<tr>
<td>Service Profile</td>
<td>McAfee MOVE AV_McAfee Default-XX (Anti Virus)</td>
</tr>
</tbody>
</table>

These are the profile configurations exported from McAfee ePO. If you create a policy or change an existing MOVE AntiVirus (Agentless) policy using McAfee ePO, it is immediately exported and available here to include for creating the NSX security policy.

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Accept the default value.</td>
</tr>
<tr>
<td>Enforce</td>
<td>Accept the default value.</td>
</tr>
</tbody>
</table>

- g. Click OK.
- h. Do not add any firewall or network introspection services.
- i. Click Finish to complete and close the New Security Policy page.

You have created NSX security policy for your desktops.

3. Create an NSX security policy for infected virtual machines.
   - b. In Name, type QuarantinePolicy.
   - c. In Description, type Policy to be applied to all infected systems.
   - d. Do not change the default weight.
   - e. Click Next.
Deploying MOVE AntiVirus (Agentless) in an NSX environment
Service Composer scenarios

On the Guest Introspection Service page, click ➕ and fill in these values.

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>QuarantinePolicy.</td>
</tr>
<tr>
<td>Description</td>
<td>Policy to be applied to all infected systems.</td>
</tr>
<tr>
<td>Action</td>
<td>Accept the default value.</td>
</tr>
<tr>
<td>Service Type</td>
<td>From the drop-down list, select Anti Virus.</td>
</tr>
<tr>
<td>Service Name</td>
<td>From the drop-down list, select McAfee MOVE AV.</td>
</tr>
</tbody>
</table>

Service Profile: McAfee MOVE AV_Scan All-xx (Quarantine)

Make sure that this MOVE AntiVirus (Agentless) policy is configured for high security with settings like:
- On-Demand Scanning — Enabled.
- File types to scan — All files.
- Quarantine configuration — Enabled.

State: Accept the default value.
Enforce: Accept the default value.

Click OK.

Add the Firewall Rules, as needed. Do not add any firewall or network introspection services.

On Ready to complete page, click Finish to complete and close the New Security Policy page.

4 Move QuarantinePolicy to the top of the security policy table to ensure that it is enforced before all other policies.
   a Click the Manage Priority icon.
   b Select QuarantinePolicy and click the Move Up icon.

5 Create a security group for all desktops in your environment.
   a Log on to the vSphere Web Client.
   b Click Networking & Security, then click Service Composer.
   c Click the Security Groups tab and click the Add Security Group icon.
   d In Name, type DesktopSecurityGroup.
   e In Description, type All desktops.
   f Keep the default configurations and click Next on the next four pages.
   g Review your selections on the Ready to Complete page and click Finish.

6 Create a Quarantine security group to place the infected virtual machines.
   a Click the Security Groups tab and click the Add Security Group icon.
   b In Name, type QuarantineSecurityGroup.
c In Description, type Dynamic group membership based on infected VMs identified by the antivirus scan.

d On the Define membership Criteria page, click + and add the following criteria, then click Next.

![Membership criteria 1](image)

You can also apply the MOVE AntiVirus tag MCAFEE.MOVE.unprotected=yes.

e Keep the default configurations, then click Next on the next two pages.

f Review your selections on the Ready to Complete page, then click Finish.

7 Map DesktopPolicy policy to DesktopSecurityGroup.

a On the Security Policies tab, ensure that DesktopPolicy is selected.

b Click the Apply Security Policy icon and select DesktopSecurityGroup.

c Click OK.

This mapping ensures that all desktops (part of the DesktopSecurityGroup) are scanned when an anti-virus scan is triggered.

8 Navigate to the canvas view to confirm that QuarantineSecurityGroup does not yet include any virtual machines.

9 Map QuarantinePolicy to QuarantineSecurityGroup.

This ensures that the high security policy defined in McAfee ePO is applied to the infected systems.

The scan discovers infected virtual machines and tags them with the security tag ANTI_VIRUS.VirusFound.threat=high or MCAFEE.MOVE.unprotected=yes. The tagged virtual machines are instantly added to QuarantineSecurityGroup. The QuarantinePolicy configured with high security policy defined in McAfee ePO is applied to these VMs, so that these VMs are protected.

You can also verify that the Scan policy of MOVE AntiVirus (Agentless) in McAfee ePO is assigned to these infected VMs.
Deploying MOVE AntiVirus (Agentless) in an NSX environment
Service Composer scenarios
Deploying MOVE AntiVirus in vCNS environment

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

Contents

- Deploying the MOVE AntiVirus service (vCNS)
- Requirements
- Install the Data Center Connector for vSphere extension
- Install the MOVE AntiVirus (Agentless) extension
- Register a VMware vCenter account with McAfee ePO
- Set up a common configuration for SVM deployment
- Check in the SVM package to McAfee ePO
- Configure the IP Pool details
- Edit vShield Manager configuration
- Deploy SVM using McAfee ePO
- View the SVM deployment details

Deploying the MOVE AntiVirus service (vCNS)

The Data Center Connector for vSphere and MOVE AntiVirus (Agentless) extensions are installed into the McAfee ePO server for registering the VMware vCenter account and setting up the vCNS requirements. This is necessary before deploying the MOVE AntiVirus service and configuring the policies.

Overview of the deployment process

Using McAfee ePO, you can register, configure the MOVE SVM with vCNS, and deploy it to one or more clusters. This deployment automatically provides virus protection for virtual machines on a new hypervisor from the moment the hypervisor is added to the cluster.

The overall MOVE AntiVirus service deployment in a vCNS environment can be simplified into the following steps. The entire deployment process is only for vCNS environment and not for NSX environment.

1. Install the Data Center Connector for vSphere and MOVE AntiVirus (Agentless) extensions into McAfee ePO.

   If you install the MOVE AntiVirus (Agentless) extension before installing the Data Center Connector for vSphere extension and registering the vCenter account, the hypervisors do not appear under the McAfee MOVE AV (Agentless) page.
2 Register a VMware vCenter account with McAfee ePO.
3 Set up a common configuration for McAfee ePO and SVM on the McAfee ePO server.
4 Check in the SVM package to McAfee ePO.
5 Configure the IP Pool details.
6 Edit vShield Manager configuration.
7 Deploy SVM using McAfee ePO.

**Requirements**

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

**MOVE SVM requirements**

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

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

The McAfee Security Virtual Appliance (SVM) 3.6.1 package must be checked in to McAfee ePO. The MOVE SVM is built to meet these minimum hardware requirements:
**CPU**
2 vCPU, 1.6 GHz or higher

**Memory**
2 GB RAM or higher

**Disk space**
8 GB or higher

These items come preinstalled:

**Operating system**
Ubuntu 12.04.5

**Software**
VirusScan Enterprise for Linux 2.0.2.29099
McAfee Agent 4.8
MOVE AntiVirus Agentless

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

**VMware requirements**

You must be running this VMware software:

- VMware vSphere
  - VMware vCenter 5.5U2 or 6.0
  - VMware ESXi 5.5U2 or 6.0
  - VMware vCloud Networking and Security Manager 5.5

**Permissions required for SVM deployment**

The VMware vCenter account credentials specified in the Registered Cloud Account page of McAfee ePO for discovering the virtual instances must have these permissions.

**Preparing the ESX host**

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

<table>
<thead>
<tr>
<th>Configuration Location</th>
<th>Permission description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host &gt; Configuration &gt; Change Settings</td>
<td>Permissions Required to Query Modules on ESX.</td>
</tr>
<tr>
<td>Host &gt; Configuration &gt; Network</td>
<td>Permissions required to add new virtual switch, port group, virtual NIC etc.</td>
</tr>
<tr>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>Host &gt; Configuration &gt; Advanced Settings</td>
<td>Permissions required to setup networking for dvfilter communication on ESX.</td>
</tr>
<tr>
<td>Host &gt; Configuration &gt; Query Patch</td>
<td>Permissions required to install Filter Driver.</td>
</tr>
<tr>
<td>Host &gt; Configuration &gt; Security profile</td>
<td>Permissions to reconfigure outgoing firewall connections to allow retrieval of Filter</td>
</tr>
<tr>
<td>and firewall</td>
<td>Driver package from DSM.</td>
</tr>
<tr>
<td>Global &gt; Licenses</td>
<td>To check what licenses are installed, so that you can add or remove licenses.</td>
</tr>
<tr>
<td>Sessions &gt; Validate session</td>
<td>To verify the session validity.</td>
</tr>
</tbody>
</table>

**Deploying the Virtual Appliance**

This is the second step in SVM deployment, during which the virtual appliance itself is deployed from an OVF file.
Configuration Location | Permission description
--- | ---
vApp > Import | Permissions to deploy SVM from OVF file.
Datastore > Allocate Space | Permissions required to allocate space for SVM on datastore.
Network > Assign Network | Permissions to assign SVM to networks.
Virtual Machine > Configuration > Add new disk | Permissions to add disks to SVM.
Virtual Machine > Interaction > Power On | Permissions to turn on SVM.
Virtual Machine > Interaction > Power Off | Permissions to turn off SVM.
VirtualMachine > Configuration > Rename | Permissions to rename a virtual machine or modify the associated notes of a virtual machine.

### Activating the Virtual Machine

In this step the SVM is activated.

<table>
<thead>
<tr>
<th>Configuration Location</th>
<th>Permission description</th>
</tr>
</thead>
</table>
| Virtual Machine > Configuration > Advanced | Permissions to reconfigure virtual machine for dvfilter

### Enabling vShield Driver

This step involves enabling vShield driver on endpoints.

<table>
<thead>
<tr>
<th>Configuration Location</th>
<th>Permission description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VirtualMachine &gt; Interaction &gt; Vmware Tools Install</td>
<td>To mount and unmount the VMware Tools CD installer as a CD-ROM for the guest operating system.</td>
</tr>
<tr>
<td>VirtualMachine &gt; Guest Operations &gt; Guest Operation Program Execution</td>
<td>For execution of virtual machine operation programs.</td>
</tr>
<tr>
<td>VirtualMachine &gt; Guest Operations &gt; Guest Operation Modifications</td>
<td>For modifications of virtual machine operation.</td>
</tr>
</tbody>
</table>

### Remove Operations

In this step the SVM is removed.

<table>
<thead>
<tr>
<th>Configuration Location</th>
<th>Permission description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VirtualMachine &gt; Inventory &gt; Remove</td>
<td>To delete a virtual machine and to remove its underlying files from disk.</td>
</tr>
</tbody>
</table>

To have permission to perform this operation, you must have this privilege assigned to both the object and its parent object.

### McAfee ePO requirements

- ePolicy Orchestrator 4.6.8, 5.1.0, 5.1.1, or 5.3.0

For details about system requirements and instructions for setting up the ePolicy Orchestrator environment, see the [McAfee ePolicy Orchestrator Installation Guide](#).

### Guest VM operating system minimum requirement

We recommend that you install the latest version of the VMware Tools, so that the latest drivers are installed.
For information about the Guest VM operating systems that are supported for VMware vShield Endpoint, see VMware’s documentation: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1036847

Firewall settings

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

Additional requirements

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

- You have installed the latest extension for Data Center Connector for vSphere. For more information, see the product documentation for Data Center Connectors.
  
  If you install the MOVE AntiVirus (Agentless) extension before installing the Data Center Connector for vSphere extension and registering the vCenter account, the hypervisors do not appear under the MOVE AntiVirus (Agentless) page.

- You have registered a VMware vCenter account. For more information, see the product documentation for Data Center Connectors.

- You have installed the MOVE AntiVirus (Agentless) extension.

- You have installed and configured vShield Manager.

  The vShield Manager account must have vShield Administrator permissions.

- The McAfee ePO server and client systems are in domain. They should be able to communicate using their Fully Qualified Domain Name (FQDN).

- You have configured and registered all LDAP servers, which are managing the client systems to be protected, on the McAfee ePO server. For successful installation of vsepflt, the domain user used to register the LDAP server must have the admin rights.

Install the Data Center Connector for vSphere extension

Download and install the Data Center Connector for vSphere extension on the McAfee ePO server to be able to discover the VM information and import it to the System Tree.

Before you begin

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

From the McAfee download site (http://www.mcafee.com/us/downloads/), you can download the extension for vSphere connector.

<table>
<thead>
<tr>
<th>Connector</th>
<th>Suite</th>
<th>Package</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Center Connector for vSphere</td>
<td>McAfee Server Security Advanced</td>
<td>vSphere_Ext_3.6.1.zip</td>
</tr>
<tr>
<td></td>
<td>McAfee Server Security Essential</td>
<td>vSphere_Ext_3.6.1.zip</td>
</tr>
</tbody>
</table>
Task
For details about product features, usage, and best practices, click ? or Help.

1 Log on to McAfee ePO as an administrator.

2 Select Menu | Software | Extensions | Install Extension.

3 Browse to and select the extension file for vSphere connector, then click OK.

4 Review the extension details and click OK.

Install the MOVE AntiVirus (Agentless) extension
A product’s extension must be installed before McAfee ePO can manage the product.

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

Task
For option definitions, click ? in the interface.

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

<table>
<thead>
<tr>
<th>Extension</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main product extension</td>
<td>MOVE-AV-AL_EXT_3.6.1.Zip</td>
</tr>
<tr>
<td>License extension</td>
<td>MOVE-AV-AL_license_EXT_3.6.1.Zip</td>
</tr>
</tbody>
</table>

2 Log on to McAfee ePO as an administrator.

3 Select Menu | Software | Extensions | Install Extension.

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

5 Verify that the product name appears in the Extensions list.

Register a VMware vCenter account with McAfee ePO
To enable and manage the security of the virtual machines in your datacenter with MOVE AntiVirus (Agentless), you must first add the vCenter to the McAfee ePO server.

Before you begin
- Make sure that you have configured your VMware vCenter server that manages the ESXi servers, which host the guest VMs.

Task
For details about product features, usage, and best practices, click ? or Help.

1 Log on to McAfee ePO as an administrator.

2 Select Menu | Configuration | Registered Cloud Accounts, then click Add Cloud Account to open the Add Cloud Account page.
3 From the Choose Connector drop-down list on the Description page, select VMware vSphere, then click OK.

![vCenter Account Details](image)

4 On the vCenter Account Details page, type these details:
   - **Account Name** — A name for the VMware vCenter account in McAfee ePO. Account names can include characters a–z, A–Z, 0–9, and [_.-], without space.
   - **Server Address** — (Required) IP address or the host name of the available VMware vCenter.
   - **vCenter Username** — (Required) User name of the available VMware vCenter account.
   - **vCenter Password** — (Required) Password of the available VMware vCenter account.
   - **Connection protocol** — The protocol required to establish the connection with the VMware vCenter.
   - **Sync Interval (In Minutes)** — Specify the interval for running the next vCenter discovery.
     - The default value is 5 minutes.
   - **Port No** — The port number required to establish the connection with the available VMware vCenter.
   - **Tag** — The administrator specifies this to identify the VMs. Tag name can include characters a–z, A–Z, 0–9, and [_.-], with space.

5 Click Test Connection to validate VMware vCenter account details and verify the connection to the VMware vCenter, then click Next to open the Validate Certificate page.

6 Click Accept to validate the certificate, then click Finish.
7 When prompted to confirm, click OK to register the vCenter account.

This action registers the VMware vCenter and imports all discovered virtual machines, which are unmanaged, into the System Tree. The instances are imported with the similar structure and hierarchy present in VMware vCenter.

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

8 View the imported VMs: select Menu | Systems | System Tree in McAfee ePO.

After the discovery, you can find your vCenter account under the group vSphere. The clusters and hosts from vCenter are logically grouped under each datacenter group in McAfee ePO.

---

**Set up a common configuration for SVM deployment**

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

**Task**

For details about product features, usage, and best practices, click ? or Help.

1 Log on to McAfee ePO as an administrator.

2 Select Menu | Automation | MOVE AV Agentless.

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

**Table 4-1 McAfee ePO credentials**

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Type the password of the McAfee ePO console that the administrator has currently logged on.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Retype the password of the McAfee ePO console that the administrator has currently logged on.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Hostname Prefix</td>
<td>Type a unique prefix that is added to the host name of the SVM. The prefix can include characters a–z, A–Z, 0–9, and [-], without space.</td>
</tr>
<tr>
<td>Password</td>
<td>Type a password to be used as SVM password during deployment. • The password must be at least 6 characters long. • The password must contain at least one uppercase letter (A–Z) and one numeral (0–9).</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Retype the password of the available SVM.</td>
</tr>
</tbody>
</table>

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

### Check in the SVM package to McAfee ePO

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

**Before you begin**
Verify that you installed the MOVE AntiVirus (Agentless) 3.6.1 extension.

Make sure that you do not change the file name of the SVM package for a successful check-in.

**Task**
For details about product features, usage, and best practices, click ? or Help.

1. Log on to McAfee ePO as an administrator.
2. Select **Menu | Automation | MOVE AV Agentless**.
3. From the **Configuration** tab, click **SVM Repository** to open the MOVE SVM repository configuration page with these SVM details and actions:

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVM Name</td>
<td>Name of the SVM package checked in to McAfee ePO.</td>
</tr>
<tr>
<td>SVM Version</td>
<td>Version of the SVM package checked in to McAfee ePO.</td>
</tr>
<tr>
<td>SVM Use Count</td>
<td>Specifies the number of hypervisors that are using this MOVE SVM.</td>
</tr>
<tr>
<td>Action</td>
<td>• Delete — To remove an existing SVM when it is not deployed to any hypervisor.</td>
</tr>
</tbody>
</table>

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

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

### Configure the IP Pool details

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

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

An IP pool's range cannot intersect one another, thus one IP address can belong to only one IP pool. When using DHCP for the SVM, the IP Pool option is not applicable.

**Task**
For details about product features, usage, and best practices, click ? or Help.

1. Log on to McAfee ePO as an administrator.

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

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

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

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Pool Name</td>
<td>Type a name for the IP Pool.</td>
</tr>
<tr>
<td>Start IP</td>
<td>Type the starting IP address for the pool.</td>
</tr>
<tr>
<td>End IP</td>
<td>Type the ending IP address for the pool.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Type the default gateway address.</td>
</tr>
<tr>
<td>Prefix Length</td>
<td>Type the Prefix length.</td>
</tr>
<tr>
<td>DNS Suffix</td>
<td>(Optional) Type the domain name of the DNS server.</td>
</tr>
<tr>
<td>Primary DNS</td>
<td>(Optional) Type the IP address of the Primary DNS server for hostname-to-IP address resolution.</td>
</tr>
<tr>
<td>Secondary DNS</td>
<td>(Optional) Type the IP address of the Secondary DNS server for hostname-to-IP address resolution.</td>
</tr>
<tr>
<td>Used/Total</td>
<td>Specifies the total number of IP addresses and the number of used IP addresses of the IP Pool. Example: 2/3 means that 2 IP addresses are used out of the available 3 IP addresses in the IP Pool.</td>
</tr>
</tbody>
</table>

   | Action        | Delete — Use this option to delete the IP Pool when its IP addresses are not in use. |

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

---

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

**Before you begin**
- You have configured and registered the vShield Manager account.
- Make sure that the vShield Manager account has **vShield Administrator** permissions.
Using this configuration available on the ePolicy Orchestrator server, you are able to view the registration status of the vShield Manager and take the required action, as appropriate.

**Task**
For details about product features, usage, and best practices, click ? or Help.

1. Log on to McAfee ePO as an administrator.
2. Select Menu | Automation | MOVE AV Agentless.
3. From the Configuration tab, click vShield Manager. The vShield Manager: Configuration page appears with these details.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Account</td>
<td>Displays the name of the registered vCenter account.</td>
</tr>
<tr>
<td>vShield Manager</td>
<td>Displays the name of the registered vShield Manager.</td>
</tr>
<tr>
<td>Registration Status</td>
<td>Displays these registration statuses:</td>
</tr>
<tr>
<td></td>
<td>• Registered — Indicates that the vShield Manager is registered and ready for deployment.</td>
</tr>
<tr>
<td></td>
<td>• Not Registered — Indicates that the vShield Manager is not registered. Therefore click Edit and configure it before deployment.</td>
</tr>
<tr>
<td></td>
<td>• Credentials unknown — Indicates that the vShield Manager is registered with VMware vCenter, however, the credentials are unknown. Therefore, click Edit and configure it before deployment.</td>
</tr>
<tr>
<td>Action</td>
<td>Edit — Click to edit and validate the existing vShield Manager configuration.</td>
</tr>
</tbody>
</table>

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

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Name</td>
<td>Specifies the name of the registered vCenter account.</td>
</tr>
<tr>
<td>vShield Manager Name</td>
<td>Specifies the name of the registered vShield Manager.</td>
</tr>
<tr>
<td>vShield Manager Address</td>
<td>Type the IP address or the host name of the available vShield Manager.</td>
</tr>
<tr>
<td>vShield Manager Username</td>
<td>Type the user name of the available vShield Manager.</td>
</tr>
<tr>
<td>vShield Manager Password</td>
<td>Type the password of the available vShield Manager.</td>
</tr>
</tbody>
</table>

   Make sure that the credentials have vShield Administrator permissions.

5. Click Validate to verify the credentials of the vShield Manager and check that the connection to the vShield Manager works, then click OK to register the vShield Manager account.
Deploy SVM using McAfee ePO

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

Before you begin

- Verify that you installed the MOVE AntiVirus (Agentless) 3.6.1 extension.
- Verify that you checked in the SVM package to McAfee ePO.
- Make sure that you have appropriate permissions for the VMware vCenter account.
- Make sure that you configured and registered a vShield Manager account with vCenter. You can edit the existing vShield Manager configuration using the Edit option under Menu | Automation | MOVE AV Agentless | Configuration | vShield Manager.
- Make sure that the client systems have the required VMTools installed.
- You have configured and registered all LDAP servers, which are managing the client systems to be protected, on the McAfee ePO server. For successful installation of vsepflt, the domain user used to register the LDAP server must have the admin rights.
- Make sure that your McAfee ePO and client systems are in the domain. They must be able to communicate using their FQDN.
- Before deploying or removing the SVM using McAfee ePO, make sure that you manually synchronize the vCenter account using McAfee ePO. This action is important because the SVM deployment using McAfee ePO depends on the latest synchronization status provided by Data Center Connector for vSphere. For details, see the product documentation for Data Center Connector for vSphere.
- Make sure that you have appropriate permission to perform the SVM deployment task using McAfee ePO. You can enable this permission by navigating through Menu | Users | Permission Sets | MOVE AV [Agentless] SVM Deployment | Edit.

The SVM deployment process using McAfee ePO involves these three simple tasks:

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

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

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

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

Task

For details about product features, usage, and best practices, click ? or Help.

1 Log on to McAfee ePO as an administrator.

2 Select Menu | Automation | MOVE AV Agentless.
3 From the **Service** tab, click **Actions | Deploy** to open the **Selection** page with these details:

- **Hypervisors** — Lists the hypervisors present under the registered VMware vCenter account.
- **vCenter Account** — Specifies the name of the VMware vCenter account that is registered with McAfee ePO.
- **SVM Version** — Specifies the version of the SVM.
- **SVM Deployment Status** — Highlights any of these statuses during the deployment. This status is applicable to both the first time and upgrade deployment.

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

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

- **Hypervisors** — Lists the hypervisors present under the registered VMware vCenter account.
- **SVM Version** — Specifies the version of the SVM.
- **SVM Host Name** — Displays the name of the SVM host.
- **Datastore (Free Space)** — Specifies the free space present in the datastore, where the SVM service virtual machines storage is added.
- **Provision Type** — Specifies the provision type.
- **Management Network** — Specifies the details of the Management Network.
• **IP Configuration** — Specifies the DHCP IP or Static IP Pool to be used.

• **Action** — Click **Edit** to change these configurations for a single hypervisor.

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

<table>
<thead>
<tr>
<th>Edit Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypervisor</td>
</tr>
<tr>
<td>SVM Hostname</td>
</tr>
<tr>
<td>SVM VM Name</td>
</tr>
<tr>
<td>SVM Version</td>
</tr>
<tr>
<td>Datastore (Free Space)</td>
</tr>
<tr>
<td>Provision Type</td>
</tr>
<tr>
<td>Management Network</td>
</tr>
<tr>
<td>IP Configuration</td>
</tr>
</tbody>
</table>

1. You can select multiple hypervisors and click **Actions | Group edit** to change these hypervisor settings, so that the selected settings are applicable to all selected hypervisors.

- **SVM Version**
- **SVM Hostname Prefix**
Click **Save** and review the configurations of the hypervisor and SVM, then click **Next** to view the validation of these components and their status.

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

You can view these Validation Statuses:

- **Passed** — Indicates that all prerequisites are available and configured correctly.
- **Failed** — Indicates any of the prerequisites is not available or not configured correctly.
- **Warning** — Check for specific warnings like:
  - VM Tools are not running.
  - Compatibility checking failed.
  - VMs are not part of the domain as McAfee ePO.

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

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

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

**Before you begin**
- Verify that you installed the MOVE AntiVirus (Agentless) extension.
- Make sure that you have initiated the SVM deployment using McAfee ePO.

**Task**
For details about product features, usage, and best practices, click ? or Help.

1. Log on to McAfee ePO as an administrator.
2. Select **Menu | Automation | MOVE AV Agentless**.
3. From the **Status** tab, you can view the SVM deployment or upgrade details.
4. Click any of the SVM deployment jobs to view these **Job Status Details** and its **Task Status Details**.

### Table 4-3  Job status

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
<td>Indicates the date and time when the SVM deployment started.</td>
</tr>
<tr>
<td>End Time</td>
<td>Indicates the date and time when the SVM deployment ended.</td>
</tr>
<tr>
<td>Deployment Type</td>
<td>Displays whether the SVM deployment type is <strong>Deploy</strong>, <strong>Upgrade</strong>, <strong>Remove</strong>.</td>
</tr>
<tr>
<td>Status</td>
<td>Specifies the deployment status such as <strong>Started</strong>, <strong>Completed</strong>, <strong>Failed</strong>, <strong>Completed with error</strong>, and <strong>Fatal error</strong>.</td>
</tr>
<tr>
<td>vCenter Name</td>
<td>Specifies the name of VMware vCenter account that is registered with McAfee ePO.</td>
</tr>
<tr>
<td>Hypervisors</td>
<td>Specifies the name of the hypervisor.</td>
</tr>
</tbody>
</table>

### Table 4-4  Task status

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node Type</td>
<td>Specifies whether the node is an SVM or a hypervisor, or a VM.</td>
</tr>
<tr>
<td>Task Type</td>
<td>Specifies the set of internal tasks that happen within a deployment or an upgrade job. The task list for a single job is displayed in sequence with <strong>Start Time</strong>, <strong>End Time</strong>, and <strong>Failure Reasons</strong>, if applicable. For the list of tasks and details, see <strong>Task status details</strong>.</td>
</tr>
<tr>
<td>Node Name</td>
<td>Displays the SVM VM name, or Hypervisor name, or the guest VM name.</td>
</tr>
<tr>
<td>Status</td>
<td>Specifies the task status such as <strong>Started</strong>, <strong>Completed</strong>, <strong>Skipped</strong>, <strong>Failed</strong>, and <strong>In Progress</strong>.</td>
</tr>
<tr>
<td>Failure Reason</td>
<td>Specifies the reason for the failure of the task.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Indicates the date and time when the task started.</td>
</tr>
<tr>
<td>End Time</td>
<td>Indicates the date and time when the task ended.</td>
</tr>
</tbody>
</table>

The rollback functionality is available while deploying and upgrading the SVM. For example, if the SVM deployment fails, the system automatically performs the rollback of the deployment at individual task level and reverts the system to its original state.
Task type and status details
These are the task types that specify the set of internal tasks that happen within a deployment or an upgrade job. The task list for a single job is displayed in sequence with Start Time, End Time, and Failure Reasons, if applicable.

Table 4-5  During SVM deployment

<table>
<thead>
<tr>
<th>Task type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing vShield Endpoint</td>
<td>Indicates that the vShield Endpoint installation is in progress.</td>
</tr>
<tr>
<td>Deploying SVM</td>
<td>Indicates that the SVM deployment is in progress.</td>
</tr>
<tr>
<td>Powering on SVM</td>
<td>Specifies that the SVM is turned on.</td>
</tr>
<tr>
<td>Registering SVM with McAfee ePO</td>
<td>Registers the SVM with McAfee ePO.</td>
</tr>
<tr>
<td>Validating MOVE Service Status</td>
<td>Validates the status of the MOVE Service whether it is active.</td>
</tr>
<tr>
<td>Registering vendor with VSM</td>
<td>Registers the vendor with vShield Manager.</td>
</tr>
<tr>
<td>Registering solution with VSM</td>
<td>Registers the solution with vShield Manager.</td>
</tr>
<tr>
<td>Setting SVM IP and Port to VSM</td>
<td>Sets the SVM IP and Port to vShield Manager.</td>
</tr>
<tr>
<td>Activating SVM (Enabling security)</td>
<td>Specifies that the SVM is activated and the malware protection is enabled.</td>
</tr>
<tr>
<td>Enabling vShield Driver</td>
<td>Enables vShield Driver on the client systems.</td>
</tr>
<tr>
<td>Testing EICAR</td>
<td>Tests EICAR on one of the client system on which vShield Driver installation is successful.</td>
</tr>
</tbody>
</table>

Table 4-6  During SVM removal

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

Table 4-7  During SVM upgrade

<table>
<thead>
<tr>
<th>Task type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploying SVM</td>
<td>Indicates that the SVM deployment is in progress.</td>
</tr>
<tr>
<td>Uninstalling vShield Endpoint</td>
<td>Indicates that the vShield Endpoint removal is in progress.</td>
</tr>
<tr>
<td>Installing vShield Endpoint</td>
<td>Indicates that the vShield Endpoint installation is in progress.</td>
</tr>
<tr>
<td>Deactivating SVM (Disabling Security)</td>
<td>Specifies that the SVM is deactivated and the malware protection is disabled.</td>
</tr>
<tr>
<td>Clearing SVM IP and Port from VSM</td>
<td>Removes the IP and Port details of the SVM from the vShield Manager.</td>
</tr>
</tbody>
</table>
### Table 4-7  During SVM upgrade (continued)

<table>
<thead>
<tr>
<th>Task type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unregistering solution from VSM</td>
<td>Removes the registration of the SVM from the vShield Manager.</td>
</tr>
<tr>
<td>Unregistering vendor from VSM</td>
<td>Removes the registration of the vendor from the vShield Manager.</td>
</tr>
<tr>
<td>Powering off SVM</td>
<td>Specifies that the SVM is turned off.</td>
</tr>
<tr>
<td>Renaming SVM</td>
<td>Renaming the old turned off SVM.</td>
</tr>
<tr>
<td>Renaming SVM</td>
<td>Renaming the new deployed off SVM.</td>
</tr>
<tr>
<td>Powering on SVM</td>
<td>Specifies that the SVM is turned on.</td>
</tr>
<tr>
<td>Registering SVM with McAfee ePO</td>
<td>Registers the SVM with McAfee ePO.</td>
</tr>
<tr>
<td>Validating MOVE Service Status</td>
<td>Validates the status of the MOVE service whether it is active.</td>
</tr>
<tr>
<td>Registering vendor with VSM</td>
<td>Registers the vendor with vShield Manager.</td>
</tr>
<tr>
<td>Registering solution with VSM</td>
<td>Registers the solution with vShield Manager.</td>
</tr>
<tr>
<td>Setting SVM IP and Port to VSM</td>
<td>Sets the SVM IP and Port to vShield Manager.</td>
</tr>
<tr>
<td>Activating SVM (Enabling security)</td>
<td>Specifies that the SVM is activated and the malware protection is enabled.</td>
</tr>
<tr>
<td>Removing SVM</td>
<td>Removing the turned off old SVM from hypervisor</td>
</tr>
<tr>
<td>Enabling vShield Driver</td>
<td>Enables vShield Driver on the client systems.</td>
</tr>
<tr>
<td>Testing EICAR</td>
<td>Tests EICAR on one of the client system on which vShield Driver installation is successful.</td>
</tr>
</tbody>
</table>

### Table 4-8  During rollback

<table>
<thead>
<tr>
<th>Task type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rollback : Uninstalling vShield Endpoint</td>
<td>Rolls back the Installing vShield Endpoint task.</td>
</tr>
<tr>
<td>Rollback : Powering off SVM</td>
<td>Rolls back the turning on SVM task.</td>
</tr>
<tr>
<td>Rollback : Remove SVM</td>
<td>Rolls back the Deploying SVM task.</td>
</tr>
<tr>
<td>Rollback : Testing EICAR</td>
<td>Rolls back the testing EICAR SVM upgrade.</td>
</tr>
<tr>
<td>Rollback : Returning Static IP to IPPool</td>
<td>Rolls back the static IP to IPPool which was assigned to the deployed SVM.</td>
</tr>
</tbody>
</table>
Manual deployment of the SVM

You can manually deploy the SVM to each hypervisor from the vSphere Client. The vSphere Client must be connected to a vCenter server, and not directly to a hypervisor.

The manual deployment of the SVM is a legacy method. So, we recommend that you use the McAfee ePO wizard-based deployments.

Contents
- Install VMware Endpoint
- Manually deploy the OVF

Install VMware Endpoint

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

For instructions, see the VMware vShield Endpoint Quick Start Guide at http://www.vmware.com/pdf/vshield_5.5_quickstart.pdf.

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

Task
1. Install ESXi.
2. Install and configure vCloud Networking and Security Manager.
3. Install vShield Endpoint on the hypervisors.

Manually deploy the OVF

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

Before you begin
- VMware vShield Endpoint must be installed on the hypervisor.
- To ensure that vMotion does not move the MOVE SVM from the selected hypervisor, deploy the MOVE SVM on local datastore.
- The vSphere Client must be connected to a vCenter server to successfully deploy the OVF.
- From the McAfee download site, download and extract the contents of MOVE-AV-AL_OVF_3_6.1.Zip.
**Task**

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

2. Apply these settings to deploy the OVF:

<table>
<thead>
<tr>
<th>For this option...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
<td>Browse to and select <code>move-svm.ovf</code> file.</td>
</tr>
<tr>
<td>OVF Template Details</td>
<td>Review details about the OVF.</td>
</tr>
<tr>
<td>End User License Agreement (EULA)</td>
<td>Accept this to continue.</td>
</tr>
<tr>
<td>Name and Location</td>
<td>Specify the name of the MOVE SVM and the inventory location.</td>
</tr>
<tr>
<td>Storage</td>
<td>Select the datastore for the MOVE SVM.</td>
</tr>
<tr>
<td></td>
<td>This page is displayed only if the hypervisor has multiple datastores.</td>
</tr>
<tr>
<td>Disk Format</td>
<td>Select the required disk provisioning.</td>
</tr>
<tr>
<td>Network Mapping</td>
<td>Map the OVF networks to the existing networks on the selected hypervisor.</td>
</tr>
<tr>
<td>Properties</td>
<td>If you specify the configuration information about the Properties page, then the MOVE SVM is automatically configured during the initial start. See <strong>OVF properties</strong>. To manually configure the MOVE SVM, do not specify the settings on the Properties page. See <strong>Manually configure the SVM</strong>.</td>
</tr>
<tr>
<td></td>
<td>We recommend manually configuring the MOVE SVM.</td>
</tr>
<tr>
<td></td>
<td>If you deploy the MOVE SVM from VMware vCenter, do not specify any NSX Manager details.</td>
</tr>
<tr>
<td>Nails</td>
<td>Set the required VSEL password. You can also leave this option blank.</td>
</tr>
<tr>
<td>Keys</td>
<td>Leave this option blank.</td>
</tr>
<tr>
<td>Ready to Complete</td>
<td>Review the options you selected.</td>
</tr>
</tbody>
</table>

3. Click **Finish**.
Upgrading MOVE AntiVirus (Agentless)

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

Review this list before you unregister the existing SVM and deploy the new SVM in your environment.

- The 3.6.1 McAfee ePO extension upgrades the 3.5.x and 3.6.0 extensions.
- Quarantine settings and policy assignments are not migrated. Redefine and assign the quarantine settings and policies after migration.

Contents
- Manual upgrade of the SVM
- Upgrade MOVE AntiVirus (Agentless) in an NSX environment
- Upgrade MOVE AntiVirus in vCNS environment

Manual upgrade of the SVM

You can manually upgrade MOVE AntiVirus (Agentless) by unregistering the existing SVM from vCloud Networking and Security Manager, and deploying a new SVM to the hypervisor.

Upgrade the extension

Version 3.6.1 of the MOVE AntiVirus (Agentless) extension upgrades the 3.5.x and 3.6.0 extensions.

Before you begin

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

All policies created in versions 3.5.x and 3.6.0 exist after you upgrade to version 3.6.1.

Task

For details about product features, usage, and best practices, click ? or Help.

1. Log on to McAfee ePO as an administrator.
2. Select Menu | Software | Extensions.
3. When the Extensions page opens, click Install Extension.
4. Browse to and select the MOVE-AV-AL_EXT_3.6.1.Zip file, then click OK.
5. After a confirmation message, click OK.
6. Browse to and select the MOVE-AV-AL-License_EXT_3.6.1.Zip file, then click OK.
7. After a confirmation message, click OK.
Deploy a new MOVE SVM manually
Unregister the 3.5.x or 3.6.0 MOVE SVM before deploying the new 3.6.1 SVM.

Task
1. From the McAfee download site, download MOVE-AV-AL_OVF_3.6.1.Zip.
2. Log on to the existing MOVE SVM.
3. Run `sudo /opt/McAfee/move/bin/sva-config`.
4. Enter `Yes` to register or unregister this MOVE SVM with vCloud Networking and Security Manager.
5. Enter `u` to unregister.
6. Turn off the MOVE SVM.
7. Deploy a new SVM to the hypervisor.

- Do not delete this MOVE SVM until the 3.6.1 version is successfully deployed. This MOVE SVM can be used to troubleshoot deployment issues.

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

Task
For option definitions, click ? in the interface.
1. Log on to McAfee ePO as an administrator.
   
   Each assigned policy per category appears in the details pane.
3. Locate the policy category that you want, then click Edit Assignment.
4. If the policy is inherited, select Break inheritance and assign the policy and settings below next to Inherited from.
5. Select a policy from the Assigned policy drop-down list.

- From this location, you can also edit the selected policy's settings, or create a policy.
6. Choose whether to lock policy inheritance.
   
   Locking policy inheritance prevents any systems that inherit this policy from having another one assigned in its place.
7. Click Save.
Upgrade MOVE AntiVirus (Agentless) in an NSX environment

Use McAfee ePO and VMware vSphere Web Client to upgrade MOVE AntiVirus (Agentless) 3.5.x and 3.6.0 to 3.6.1.

**Before you begin**
- Make sure that your NSX Manager is registered with your vCenter account.
- Make sure that you remove the existing dummy policy template that is included in the security policy.

MOVE AntiVirus (Agentless) 3.6.1 supports upgrading or migrating these components of 3.5.x and 3.6.0:
- MOVE AntiVirus (Agentless) extension
- NSX Manager details
- McAfee MOVE AV service
- MOVE SVM

**Task**
For details about product features, usage, and best practices, click ? or Help.

2. Select the security policy, which has the MOVE global policy and click Actions | Edit | Guest Introspection Services, then delete MOVE global policy.
3. On McAfee ePO, upgrade the Data Center Connector for vSphere and MOVE AntiVirus (Agentless) extensions to 3.6.1.

   Version 3.6.1 extension of Data Center Connector for vSphere is a minimum requirement for upgrading to MOVE AntiVirus (Agentless) 3.6.1 in an NSX environment. The vCenter account registration automatically detects and sends the details of your existing NSX Manager to McAfee ePO. Make sure that the vCenter account synchronization is completed successfully after upgrading the Data Center Connector for vSphere extension. You should then upgrade your MOVE AntiVirus (Agentless) extension.

4. Check in the MOVE SVM 3.6.1 package to McAfee ePO.
5. From McAfee ePO, select Menu | Automation | MOVE AV Agentless | Configuration | General and complete the common configuration.
6. From the Service tab on McAfee ePO, click NSX Manager to open the MOVE Service Registration page.
7. Under Actions, click Upgrade to open the MOVE Service registration dialog box.
8. Select the latest MOVE SVM and click OK. The latest MOVE AV service is now registered with the vCenter account that is registered with NSX Manager.

The Upgrade option for MOVE AV service is available under Installation | Service Deployments in vSphere Web Client.
9 Verify that the MOVE AntiVirus (Agentless) 3.6.1 Scan policies are exported from McAfee ePO to NSX in real time and are available in Profile Configurations under Networking & Security | Service Definitions | McAfee MOVE AV | Actions | Edit settings | Manage | Profile Configurations with a ID and description.

10 On vSphere Web Client, configure the security policy using the latest MOVE AntiVirus (Agentless) Scan policies exported from McAfee ePO. For details, see Create an NSX security policy.

11 Apply the NSX security policy to the NSX security group. For details, see Apply the NSX security policy to the NSX security group.

12 Deploy the latest MOVE AntiVirus service using the Upgrade button available under Installation | Service Deployments in vSphere Web Client.

---

**Upgrade MOVE AntiVirus in vCNS environment**

Use McAfee ePO to upgrade MOVE AntiVirus (Agentless) 3.6.0 to 3.6.1. MOVE AntiVirus (Agentless) 3.6.1 supports upgrading these components of 3.6.0:

- MOVE AntiVirus service
- MOVE SVM
- MOVE AntiVirus (Agentless) extension

**Task**

For details about product features, usage, and best practices, click ? or Help.

1 Upgrade the Data Center Connector for vSphere and MOVE AntiVirus (Agentless) extensions to 3.6.1.

   Version 3.6.1 extension of Data Center Connector for vSphere is a minimum requirement for upgrading to MOVE AntiVirus (Agentless) 3.6.1 in vCNS environment. The vCenter account registration automatically detects and sends the details of your existing vCNS details to the McAfee ePO server. Make sure that the vCenter account synchronization is completed successfully after upgrading the Data Center Connector for vSphere extension.

2 Check in the MOVE SVM 3.6.1 package to McAfee ePO.

3 From McAfee ePO, select Menu | Automation | MOVE AV Agentless | Configuration | General and verify the common configuration.

4 From the Service tab, click Actions | Upgrade to open the Selection page.

5 From the Selection page, select the required hypervisor to deploy the SVM, then click Next to open the Configuration page.

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

7 From the Verification page, click Deploy to start the SVM deployment.

You can now navigate to the vCNS Job Status tab and view the deployment tasks and their details.
Uninstalling MOVE AntiVirus (Agentless)

The process of removing MOVE AntiVirus (Agentless) consists of removing the MOVE AV service from the clusters and removing the configurations and extensions from McAfee ePO.

Contents
- Uninstalling MOVE AntiVirus (Agentless) 3.5.x or 3.6.0 in an NSX environment
- Uninstalling MOVE AntiVirus (Agentless) 3.6.1 in an NSX environment
- Uninstalling MOVE AntiVirus (Agentless) in a vCNS environment

Uninstalling MOVE AntiVirus (Agentless) 3.5.x or 3.6.0 in an NSX environment

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

Remove MOVE AV service from the cluster

Using the vSphere Web Client console, you can remove the MOVE AV service, which is deployed to one or more clusters.

Task
1. Log on to vSphere Web Client as an administrator.
3. Select McAfee MOVE AV and click the Delete service deployment icon. The Confirm Delete message appears.
4. Click Delete now to confirm, then click OK. You can also schedule to delete it later.

Remove the MOVE Guest Introspection Service from the security policy

Remove the MOVE Guest Introspection Service from the security policy using the VMware vCenter Web Client console.

Task
1. Log on to the VMware vCenter Web Client as an administrator.
2. Click Networking & Security | Service Composer | Security Policies, then select an existing Security Policy and click the Edit Security Policy icon to open the Name and description page.
3. Change the name and description, if necessary, then click Next to open the Guest Introspection Services page.

4. Select the required MOVE Guest Introspection Service, then click the Delete icon.

5. Click Finish. This action removes the MOVE Guest Introspection Service.

**Unregister the VMware NSX Manager from McAfee ePO**

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

**Task**

1. Log on to McAfee ePO as an administrator.

2. Select Menu | Configuration | MOVE Service Registration. This action lists all NSX Managers registered in McAfee ePO.

3. From the Actions column on the MOVE Service configuration page, click Unregister for the registered NSX Manager. A confirmation dialog box appears.

4. Click OK to confirm.

**Remove NSX Manager details from McAfee ePO**

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

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. Log on to McAfee ePO as an administrator.

2. Select Menu | Configuration | Registered Servers to open the Registered Servers page.

3. Select the existing NSX Manager that you want to remove, then click Actions | Delete. A confirmation dialog box appears.

4. Click Yes to confirm.

**Uninstall the extension**

Uninstall the MOVE AntiVirus (Agentless) extension from McAfee ePO.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. Log on to McAfee ePO as an administrator.

2. Select Menu | Software | Extensions.

3. Next to the extension that you want to remove, click Remove.

<table>
<thead>
<tr>
<th>Extension</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main product extension</td>
<td>MOVE-AV-AL_EXT_x.x.x.zip</td>
</tr>
<tr>
<td>License extension</td>
<td>MOVE-AV-AL_License_EXT_x.x.x.zip</td>
</tr>
</tbody>
</table>

This action removes the MOVE AntiVirus (Agentless) extension and the MOVE SVM package, which is already checked in to the McAfee ePO server.
Uninstalling MOVE AntiVirus (Agentless) 3.6.1 in an NSX environment

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

Remove MOVE AV service from the cluster
Using the vSphere Web Client console, you can remove the MOVE AV service, which is deployed to one or more clusters.

Task
1. Log on to vSphere Web Client as an administrator.
3. Select McAfee MOVE AV and click the Delete service deployment icon. The Confirm Delete message appears.
4. Click Delete now to confirm, then click OK. You can also schedule to delete it later.

   Make sure that you wait until the MOVE AV service is removed from all clusters.

Remove the MOVE Guest Introspection Service from the security policy
Remove the MOVE Guest Introspection Service from the security policy using the VMware vCenter Web Client console.

Task
1. Log on to the VMware vCenter Web Client as an administrator.
2. Click Networking & Security | Service Composer | Security Policies, then select an existing Security Policy and click the Edit Security Policy icon to open the Name and description page.
3. Change the name and description, if necessary, then click Next to open the Guest Introspection Services page.
4. Select the required MOVE Guest Introspection Service, then click the Delete icon.
5. Click Finish. This action removes the MOVE Guest Introspection Service.

Unregister the McAfee MOVE AV service using McAfee ePO
Select the registered version of the MOVE AV service and unregister it from the NSX Manager.

Task
For details about product features, usage, and best practices, click ? or Help.
1. Log on to McAfee ePO as an administrator.
2. Select Menu | Automation | MOVE AV Agentless.
3. From the Service tab, click NSX Manager to open the MOVE Service Registration page.
4. Click Unregister under Actions to unregister the selected MOVE AV service. The MOVE AV service details are now removed from NSX Manager.
Uninstall the extension

Uninstall the MOVE AntiVirus (Agentless) extension from McAfee ePO.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. Log on to McAfee ePO as an administrator.
2. Select **Menu** | **Software** | **Extensions**.
3. Next to the extension that you want to remove, click **Remove**.

<table>
<thead>
<tr>
<th>Extension</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main product extension</td>
<td>MOVE-AV-AL_EXT_x.x.x.zip</td>
</tr>
<tr>
<td>License extension</td>
<td>MOVE-AV-AL_License_EXT_x.x.x.zip</td>
</tr>
</tbody>
</table>

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

Uninstalling MOVE AntiVirus (Agentless) in a vCNS environment

A full uninstall involves removing these components: MOVE AntiVirus service, MOVE SVM, vShield Manager details, and the MOVE AntiVirus (Agentless) extension.

**Remove SVM using McAfee ePO**

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

**Before you begin**

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

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. Log on to McAfee ePO as an administrator.
2. Select **Menu** | **Automation** | **MOVE AV Agentless**.
3. From the **Service** tab, click **Actions** | **Undeploy** to open the **Selection** page with these details.
   - **Hypervisors** — Lists the hypervisors, present under the registered VMware vCenter account, where the SVM is already deployed.
   - **vCenter Account** — Displays the name of the VMware vCenter account that is registered with McAfee ePO.
   - **SVM Version** — Displays the SVM version.
4. From the **Selection** page, select the required hypervisors from where you want to remove the SVM and click **Next** to open the **Verification** page with these details:
   - **Hypervisors** — Lists the hypervisors present under the registered VMware vCenter account.
   - **vCenter Account** — Specifies the name of the VMware vCenter account that is registered with McAfee ePO.
- SVM Version — Specifies the version of the SVM.
- SVM VM Name — Displays the name of the SVM host.
- Validation Status — Displays the validation status that specifies whether the SVM can be removed.

5 Click Remove to remove the SVM from the selected hypervisors.

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

**Table 7-1  Job status**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time</td>
<td>Indicates the date and time when the SVM deployment started.</td>
</tr>
<tr>
<td>End Time</td>
<td>Indicates the date and time when the SVM deployment ended.</td>
</tr>
<tr>
<td>Deployment Type</td>
<td>Displays the SVM deployment type as Remove.</td>
</tr>
<tr>
<td>Status</td>
<td>Specifies the deployment status such as Started, Completed, Failed, Completed with error, and Fatal error.</td>
</tr>
<tr>
<td>vCenter Name</td>
<td>Specifies the name of VMware vCenter account that is registered with McAfee ePO.</td>
</tr>
<tr>
<td>Hypervisors</td>
<td>Specifies the name of the hypervisor.</td>
</tr>
</tbody>
</table>

**Table 7-2  Task status**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node Type</td>
<td>Specifies whether the node is an SVM or a hypervisor.</td>
</tr>
<tr>
<td>Task Type</td>
<td>Specifies the set of internal tasks that happen within a deployment or an upgrade job. The task list for a single job is displayed in sequence with Start Time, End Time, and Failure Reasons, if applicable. For the list of tasks and details, see Task status details.</td>
</tr>
<tr>
<td>Node Name</td>
<td>Displays the name or IP address of the SVM.</td>
</tr>
<tr>
<td>Status</td>
<td>Specifies the task status such as Started, Completed, Failed, and Skipped.</td>
</tr>
</tbody>
</table>
| Failure Reason | Specifies the reason for the failure of the task. Example:  
  • SVMs are still registered  
  • Returning DHCP IP is not applicable                                                               |
| Start Time   | Indicates the date and time when the task started.                                                   |
| End Time     | Indicates the date and time when the task ended.                                                     |

**Uninstall the extension**

Uninstall the MOVE AntiVirus (Agentless) extension from McAfee ePO.
Task
For details about product features, usage, and best practices, click ? or Help.

1. Log on to McAfee ePO as an administrator.
2. Select Menu | Software | Extensions.
3. Next to the extension that you want to remove, click Remove.

<table>
<thead>
<tr>
<th>Extension</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main product extension</td>
<td>MOVE-AV-AL_EXT_x.x.x.zip</td>
</tr>
<tr>
<td>License extension</td>
<td>MOVE-AV-AL_license_EXT_x.x.x.zip</td>
</tr>
</tbody>
</table>

This action removes the MOVE AntiVirus (Agentless) extension and the MOVE SVM package, which is already checked in to the McAfee ePO server.
Monitoring and managing your environment

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

Contents
- Integration with ePolicy Orchestrator
- Policy management
- Configuring role-based access control for policies and SVM deployment
- How quarantine works
- Enabling the scan policy quarantine configuration
- Using the SVA policy quarantine settings
- Configure the quarantine folder
- How VM-based scan configuration works
- Scan diagnosis
- Monitoring the SVM

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 SVM on a regular interval through the McAfee Agent. The McAfee Agent enforces policies on the SVM, 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 SVM at the next agent-server communication. To enforce policies immediately, send an agent wake-up call to the targeted SVM 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 policy to change behavior on managed systems.

Task
For option definitions, click ? in the interface.

1 Log on to McAfee ePO as an administrator.
2 Select Menu | Policy | Policy Catalog.
3 From the Product drop-down list, select MOVE AV Agentless 3.6.1.
4 From the Category drop-down list, select SVA.
5 Click New Policy.
6 On the New Policy page, configure the policy settings, then click OK.
7 In the General Settings tab of the Policy Settings page for the newly created policy, configure these settings to control basic behavior.
   • Protocol — Select https or http, depending on the protocol the server uses to receive client requests.
   • Hypervisor/vCenter Server — Enter the valid IP address of either the hypervisor that the SVM resides on or the vCenter server.
   • User — Enter the user name credentials to connect with the server.
Password — Enter the password associated with the user.

After you save and reopen an SVA policy, the vCenter password appears blank. Even though it appears blank, it is saved in the policy settings. You must retype the password to test connection settings. The user account requires at least read access to the vCenter server or the ESXi host. Domain-based credentials are supported only when the vCenter server or the ESXi host has been configured to support domain-based authentication.

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

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 SVM 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.

In the Quarantine settings tab, configure the network share, so that all detected malware is quarantined to the specified network share. However, the malware that is detected on any virtual machine is quarantined only when you have enabled the Quarantine configuration option under Scan policy.

Create a scan policy

Create a Scan policy to change behavior on managed systems.

Task

For option definitions, click ? in the interface.

1. Log on to McAfee ePO as an administrator.
2. Select Menu | Policy | Policy Catalog.
3. From the Product drop-down list, select MOVE AV Agentless 3.6.1.
4. From the Category drop-down list, select Scan.
5. Click New Policy.
6. On the New Policy page, configure the policy settings, then click OK.
7. In the General tab of the Policy Settings page for the newly created policy, configure the settings to control basic behavior.
8. In the Scan Items tab, configure these settings to control which files are scanned.
Table 8-1 Scan items

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-Access Scan files</td>
<td>When an attempt is made to open, close, or rename a file, the scanner intercepts the operation and takes these actions. 1. The scanner determines if the file should be scanned based on this criteria: • The file’s extension matches the configuration. • The file has not been cached, excluded, or previously scanned. 2. If the file meets the scanning criteria, the scanner compares the information in the file to the known malware signatures in the currently loaded DAT files. • If the file is clean, the result is cached and read, write, or rename operation is granted. • If the file contains a threat, the operation is denied and the configured action is taken.</td>
</tr>
<tr>
<td>File types to scan</td>
<td>• All files — Select to scan all files. • Following only — Select to specify a list of file extensions to scan. You can add, edit, and remove file extensions that are included for scanning. • Default + Additional files — Select to scan the default file types or any additional file types. You can add, edit, and remove any additional file types, which are included for scanning. From version 3.6, this option is selected by default. However, when upgrading from previous versions to 3.6, the last selected option is retained.</td>
</tr>
<tr>
<td>Compressed files</td>
<td>• Scan inside archives (e.g., .ZIP) — Examines archive (compressed) files (such as .zip, .CAP, .LZH, and .UUE files) and their contents. • Decode MIME encoded files — Detects, decodes, and scans Multipurpose Internet Mail Extensions (MIME) encoded files.</td>
</tr>
<tr>
<td>Heuristics</td>
<td>Uses heuristics to find unknown unwanted programs, trojans, and macro threats.</td>
</tr>
<tr>
<td>McAfee Global Threat Intelligence file reputation</td>
<td>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.</td>
</tr>
<tr>
<td>Unwanted program detection</td>
<td>Detect unwanted programs — The on-access and on-demand scanners detect unwanted programs based on the Unwanted Programs Policy that you configured. When a detection occurs, the scanner that detected the potentially unwanted program applies the action that you configured on the Actions tab for that scanner.</td>
</tr>
</tbody>
</table>

In the Exclusions tab, configure the Path Exclusions by adding, editing, or removing a specific file path. The MOVE AntiVirus (Agentless) allows you to fine-tune the list of file types scanned. For example, you can exclude from scanning individual files, folders, and disks. These exclusions might be needed because the scanners could scan and lock a file when that file is being used by a database or server. This scenario could cause the database or server to fail or generate errors.

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

For more information about how to use wildcards when creating exclusions in MOVE AntiVirus (Agentless) 3.x, see McAfee KnowledgeBase article KB82110.
10 In the Actions tab, configure When a threat is found behavior. Make sure that you 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.

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

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

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

if you are deploying the MOVE SVM using NSX Manager, make sure that you assign the policy from NSX Manager.

Task
For option definitions, click ? in the interface.

1 Log on to McAfee ePO as an administrator.

2 Select Menu | Systems | System Tree.

3 Select the group containing the SVM.

4 Click Assigned Policies.

5 In the Product drop-down list, select MOVE AV Agentless 3.6.1.

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

7 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.

8 Click Save.

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

Before you begin
   • Make sure that the policy is configured and has been delivered to the client before testing.
   • The on-access scanner must be enabled.
**Task**

For option definitions, click ? in the interface.

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

   The file should be prevented from downloading.

2. Log on to McAfee ePO as an administrator.

3. Select **Menu** | **Systems** | **System Tree**.

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

   Client events are sent to MOVE SVM.

5. View the **Threat Event Log**: select **Menu** | **Reporting** | **Threat Event Log**.

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

---

**Configuring role-based access control for policies and SVM deployment**

McAfee ePO administrator rights management determines what administrators can do while managing the MOVE AntiVirus (Agentless) software.

The administrator can set up MOVE AntiVirus Agentless-specific permission sets for different users in McAfee ePO. The permission sets can be created for various roles including but not restricted to Executive Reviewer, Global Reviewer, Group Admin, and Group Reviewer. The MOVE AntiVirus (Agentless) extension enables McAfee ePO administrators to control SVM deployment and policies that are managed through McAfee ePO.

The McAfee ePO administrator for MOVE AntiVirus (Agentless) can:

- View and change the MOVE AntiVirus (Agentless) policy and task settings.
- View and edit SVM deployment configurations.

Administrative roles can be configured and implemented using the **User Management** | **Permission Sets** option in McAfee ePO. It is possible to configure several admin roles using this option.

For more information about configuring roles, see the documentation for the relevant version of McAfee ePO.

You can create different permission roles and assign them with different **MOVE AV [Agentless] Permission Sets** to different users.

The MOVE AntiVirus (Agentless) Permissions are:

- **MOVE AV [Agentless] Policy Permission**
- **MOVE AV [Agentless] SVM Deployment**

You can enable this permission by navigating through **Menu** | **Users** | **Permission Sets** | **MOVE AV [Agentless] SVM Deployment** | **Edit**.
To verify the configured permission sets, log off from McAfee ePO, then log on with a user account that belongs to any one of the new roles.

Use the correct format of the user name when logging on to McAfee ePO.

How quarantine works

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

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

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

A file is quarantined when:

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

Quarantined files are automatically deleted after 28 days.

The restore tool at-a-glance

This diagram provides an overview of how the quarantine restore tool works.
The restore tool requires Java Runtime Environment (JRE) 1.6 or 1.7.

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

1. Connect to a quarantine share.
2. View the list of quarantined files.
3. View the VMs corresponding to the selected file.
4. Save a file to your local system.
5. Restore a specific file to one or more selected VMs.

**Restore a file**

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

**Before you begin**

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

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

- Download MOVE-AV-AL_RestoreTool.3.6.1.Zip from the McAfee download site and extract the contents.

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

**Task**

1. From the folder where you extracted MOVE-AV-AL_RestoreTool.3.6.1.Zip, run `quarantine_restore.cmd` to start the quarantine restore tool.

   The Connect dialog box is automatically displayed.

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

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

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

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

4. Choose one of these two options:
To...                             Do this...
Save the file to your local system 1 Select Save File.
                                           2 Browse to the location, enter a file name, and click OK.
                                           The file is saved to the specified location. The quarantined file remains on the share.

Restore the file to selected VMs 1 Select the VMs where you want to restore the file, then click Restore.
                                           2 Enter valid credentials to restore the file to all selected VMs.
                                           The same file can be restored to multiple VMs by multi-selecting the VM hosts before you click Restore. The same credentials must be valid for all selected VMs for this method to work.
                                           The file is restored to each selected VM. The quarantined file is removed from the share after it is successfully restored. When the restore is completed, the list of quarantined files and VMs are updated to reflect the current state.

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

### Enabling the scan policy quarantine configuration

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

**Table 8-2** Quarantine settings

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarantine configuration</td>
<td>Enable or disable quarantine functionality.</td>
</tr>
</tbody>
</table>

### Using the SVA policy quarantine settings

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

**Table 8-3** Quarantine settings

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarantine network share</td>
<td>Quarantined files are stored on the specified network share. The share is mounted as CIFS, so the remote share must support this protocol. Read and write permissions are required. For details, see Configure the quarantine folder. Make sure that you enter the server name in a manner that can be resolved by the SVM. How this is entered depends on the environment and how the SVM is configured.</td>
</tr>
<tr>
<td>Network domain name</td>
<td>The domain used to access the specified share.</td>
</tr>
</tbody>
</table>
Table 8-3 Quarantine settings (continued)

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network user name</td>
<td>The user name used to access the specified share.</td>
</tr>
<tr>
<td>Network password</td>
<td>The password used to access the specified share. After you save and reopen a scan policy, the network password appears blank. Even though it appears blank, it is saved in the policy settings. Click Set password to set/reset the password for the quarantine share.</td>
</tr>
</tbody>
</table>

Configure the quarantine folder

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

Tasks

- Set permissions for shared folders on page 90
  Setting permission for the quarantine folder allows you to specify who has access to the share.

Set permissions for shared folders

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

Before you begin

Create the following:

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

Task

1. Right-click the quarantine folder, then select Properties.
2. Select the Sharing tab and click Advanced Sharing.
3. In the Advanced Sharing dialog box, select Share this folder, then change Share name to quarantine$. The $ symbol hides the share.
4. Click Permissions, select the default user name Everyone, click Remove, then click Apply.
5. Click Add to select an object type.
   
   You can give permission only to administrators who require access to the quarantine folder.

   a. In Select Users or Groups, enter your Domain User account in the object names dialog box, then click OK.
   b. Select the user name you created earlier, select Full Control, then click OK.
6. Click Add to select an object type.
   
   a. In Select Users or Groups, enter your Domain Local Security Group in the object names dialog box, then click OK.
   b. With this group selected, select Full Control, then click OK.
How VM-based scan configuration works

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

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

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

Enable the VM-based scan configuration setting

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

Before you begin

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

Task

For details about product features, usage, and best practices, click ? or Help.

1. Create an SVA policy or edit an existing SVA policy and assign it to the target SVMs. For details, see Create an SVA policy.

2. In the Scan Settings tab of the Policy Settings page of the newly-created or edited policy, select VM-based scan configuration and click Save. The VM-based scan configuration setting is now active. These policies are enforced to SVM within the default policy collection interval, which is 60 minutes. Follow these steps to run the policy collection immediately:
   a. Select Menu | Configuration | Server Settings, then click MOVE AV [Agentless] under Setting Categories.
   b. Click Run. The Policy collection completed successfully message appears on successful collection of the policies.
   c. Send an agent wake-up call to the target SVMs.
Scan diagnosis

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

Create and run a scan diagnostic client task using McAfee ePO

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

Before you begin
Make sure that you have installed the MOVE AntiVirus (Agentless) 3.6.1 extension.

Task
For details about product features, usage, and best practices, click ? or Help.

1. Log on to McAfee ePO as an administrator.
2. Select Menu | Policy | Client Task Catalog.
3. From Client Task Types, select MOVE AV [Agentless] 3.6.1 | Scan Diagnostics.
4. Click the name of an existing client task or click New Task and confirm the task type.
5. Configure these settings on each tab and click Save.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task Name</td>
<td>Specifies a unique user-friendly name for the task.</td>
</tr>
<tr>
<td>Description</td>
<td>Specifies some user-friendly description about the task.</td>
</tr>
</tbody>
</table>
| Diagnosis Time    | Specifies the time period, in minutes, set for calculating the frequently scanned files. For example, 1–10 minutes.

6. Click Assign, specify the SVM where you want to assign the task, then click OK.
7. Click 2 Schedule to schedule the task. At the end of specified minutes, the McAfee ePO completes the analysis and displays the results. The default allowed time limit is 10 minutes.
8. Select Menu | Reporting | Queries & Reports and select MOVE AV [Agentless] under McAfee Groups to view and run these scan diagnostic queries:
   - MOVE AV [Agentless]: Top 10 Scanned File Extensions for each SVM — Lists the top 10 file extensions scanned by the SVM.
   - MOVE AV [Agentless]: Top 10 Scanned Files for each SVM — Lists the top 10 files scanned by the SVM.
   - MOVE AV [Agentless]: Top 10 Scanned Virtual Machines for each SVM — Lists the top 10 virtual machines that are sending maximum scan and checksum requests.

Run the scan diagnostic tool using command line

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

Before you begin
Make sure that the user is a root user, or has sudo permissions.
Access the command line interface (CLI) of the SVM to create and display this report.

**Task**

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

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

These parameters are available:

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

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

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

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

This diagnostic tool captures these details:
Monitoring the SVM

Monitor the status of the SVM 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. Log on to McAfee ePO as an administrator.
2. Select Menu | Reporting | Threat Event Log
3. Click any of the column titles to sort the events. You can also click Actions | Choose Columns.
4. From the Available Columns drop-down list, select table columns as needed, then click Save.
5. 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 SVM 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.
Use McAfee ePO 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 McAfee ePO database.

For information about how to run a query or report, see the product documentation for your version of McAfee ePO.

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

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

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

McAfee Agent isn’t installed on each VM. Only the SVM appears in the McAfee ePO console, which means you don’t see each VM. vShield Manager provides a report that validates the protection status of each VM.

### Contents

- Predefined MOVE AntiVirus (Agentless) queries
- View default queries
- Predefined datacenter queries
- Data Center and Public Cloud dashboards

### Predefined MOVE AntiVirus (Agentless) queries

You can use predefined queries as is, edit them, or create queries from events and properties stored in the McAfee ePO database.

You can’t edit predefined queries in McAfee ePO 5.1.1 and later.

To create custom queries, your assigned permission set must include the ability to create and edit private queries.
MOVE AntiVirus (Agentless) provides these predefined queries:

<table>
<thead>
<tr>
<th>Query</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOVE AV [Agentless]: DAT Version</td>
<td>Specifies the DAT version available on the VMs. This query is available only when the Data Center Connector for vSphere extension is installed.</td>
</tr>
<tr>
<td>MOVE AV [Agentless]: Detection Response Summary</td>
<td>Displays the number of threats on which an action such as Modify, Access denied, and Deleted is taken versus the number of threats on which no action was taken, in the last three months.</td>
</tr>
<tr>
<td>MOVE AV [Agentless]: Licensing Information</td>
<td>Displays the number of VMs within the licensed SVM.</td>
</tr>
<tr>
<td>MOVE AV [Agentless]: On-Demand Scan Events Summary</td>
<td>Displays a summary of the on-demand scan events for the last three months.</td>
</tr>
<tr>
<td>MOVE AV [Agentless]: Service Events Summary</td>
<td>Displays a summary of the service events for the last three months.</td>
</tr>
<tr>
<td>MOVE AV [Agentless]: Summary of Threats Detected in the Last 24 Hours</td>
<td>Displays a summary of the threats detected in the last 24 hours.</td>
</tr>
<tr>
<td>MOVE AV [Agentless]: Summary of Threats Detected in the Last 7 Days</td>
<td>Displays a summary of the threats detected in the last seven days.</td>
</tr>
<tr>
<td>MOVE AV [Agentless]: Threat Count by Severity</td>
<td>Specifies the slice count, which is the number of MOVE AntiVirus (Agentless) events. Slice indicates different event severities for the last months.</td>
</tr>
<tr>
<td>MOVE AV [Agentless]: Threat Names Detected per Week</td>
<td>Displays the name and number of different threats detected every week for the last three months.</td>
</tr>
<tr>
<td>MOVE AV [Agentless]: Threats Detected in the Last 24 Hours</td>
<td>Specifies the number of threats detected in the last 24 hours.</td>
</tr>
<tr>
<td>MOVE AV [Agentless]: Threats detected in the Last 7 Days</td>
<td>Specifies the number of threats detected in the last seven days.</td>
</tr>
<tr>
<td>MOVE AV [Agentless]: Threats Detected Over the Previous 2 Quarters</td>
<td>Specifies the number of threats detected for the last three quarters.</td>
</tr>
<tr>
<td>MOVE AV [Agentless]: Threats Detected per Week</td>
<td>Displays the number of threats detected every week for the last three months.</td>
</tr>
<tr>
<td>MOVE AV [Agentless]: Top 10 Detected Threats</td>
<td>Displays the top 10 threats detected in the last three months.</td>
</tr>
<tr>
<td>MOVE AV [Agentless]: Top 10 Scanned File Extensions for each SVM</td>
<td>Lists the top 10 file extensions scanned by the SVM.</td>
</tr>
<tr>
<td>MOVE AV [Agentless]: Top 10 Scanned Files for each SVM</td>
<td>Lists the top 10 files scanned by the SVM.</td>
</tr>
<tr>
<td>MOVE AV [Agentless]: Top 10 Scanned Virtual Machines for each SVM</td>
<td>Lists the top 10 virtual machines that are sending maximum scan and checksum requests.</td>
</tr>
<tr>
<td>MOVE AV [Agentless]: Top 10 Threats per Threat Category</td>
<td>Displays the top 10 threats within a threat category for the last three months. The threats are grouped by threat category and threat name.</td>
</tr>
<tr>
<td>MOVE AV [Agentless]: Top 10 Virtual Machines with the Most Detections</td>
<td>Displays the top 10 virtual machines with the most threat detections in the last three months.</td>
</tr>
<tr>
<td>MOVE AV [Agentless]: Unwanted Programs Detected in the Last 24 Hours</td>
<td>Displays the number of potentially unwanted program events for the last 24 hours.</td>
</tr>
<tr>
<td>MOVE AV [Agentless]: Unwanted Programs Detected in the Last 7 Days</td>
<td>Displays the number of potentially unwanted program events for the last seven days.</td>
</tr>
<tr>
<td>MOVE AV [Agentless]: Virtual Machines with Threats Detected per Week</td>
<td>Displays the number of virtual machines detected with threats per week for the last three months.</td>
</tr>
</tbody>
</table>
**View default queries**

Run the predefined queries to generate reports based on McAfee MOVE AV components.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. Log on to the McAfee ePO server as an administrator.
2. Select Menu | Reporting | Queries & Reports.
3. From the Groups pane, select MOVE AV [Agentless] to display the queries for the selected group.
   - **McAfee ePO 4.6.8 and later** — Reports are grouped under Shared Groups.
   - **McAfee ePO 5.1.1 and later** — Reports are grouped under McAfee Groups.
4. From the Queries list, select a query, then click Run.
5. In the query results page, click any item in the results to drill down further.
6. Click Close when finished.

**Predefined datacenter queries**

You can use predefined queries as is, edit them, or create queries from events and properties stored in the McAfee ePO database.

You can’t edit predefined queries in McAfee ePO 5.1.1 and later.

To create custom queries, your assigned permission set must include the ability to create and edit private queries.

Datacenter provides these predefined queries:

<table>
<thead>
<tr>
<th>Query</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Anti-malware Status</strong></td>
<td>Specifies whether the system is in one of these states:</td>
</tr>
<tr>
<td></td>
<td>• Application Control Enabled — These VMs have McAfee® Application Control installed and enabled.</td>
</tr>
<tr>
<td></td>
<td>• Only Anti-Virus Enabled — These VMs have a McAfee anti-malware product installed and enabled.</td>
</tr>
<tr>
<td></td>
<td>• Unprotected — These VMs don’t have any McAfee anti-malware product enabled.</td>
</tr>
<tr>
<td><strong>Application Reputation</strong></td>
<td>Categorizes the applications based on McAfee® Global Threat Intelligence™ (McAfee GTI) file reputation:</td>
</tr>
<tr>
<td></td>
<td>• Good</td>
</tr>
<tr>
<td></td>
<td>• Bad</td>
</tr>
<tr>
<td></td>
<td>• Unclassified</td>
</tr>
<tr>
<td></td>
<td>For details about file reputation, see the product documentation for McAfee Application Control.</td>
</tr>
<tr>
<td><strong>AV Protection by Product</strong></td>
<td>Displays the anti-virus protection status of McAfee products.</td>
</tr>
<tr>
<td>Query</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Security Incidents (last 14 days)</td>
<td>Displays the events reported for these components on the VMs in the last 14 days.</td>
</tr>
<tr>
<td></td>
<td>• Application Control</td>
</tr>
<tr>
<td></td>
<td>• Antivirus</td>
</tr>
<tr>
<td></td>
<td>• Firewall</td>
</tr>
<tr>
<td></td>
<td>• Memory Protection</td>
</tr>
<tr>
<td>Data Centers</td>
<td>Displays all registered datacenters.</td>
</tr>
<tr>
<td>File Integrity Monitoring Status</td>
<td>Displays the number of VMs with File Integrity Monitoring (FIM) installed and enabled.</td>
</tr>
<tr>
<td></td>
<td>For details about FIM, see the product documentation for McAfee® Change Control.</td>
</tr>
<tr>
<td>Host Firewall Status</td>
<td>Specifies whether the system is in one of these two states:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Firewall Enabled</strong> — These VMs have McAfee® Host Intrusion Prevention (McAfee Agent-based) installed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Not in use</strong> — These VMs don’t have McAfee Host Intrusion Prevention (McAfee Agent-based) installed.</td>
</tr>
<tr>
<td>OS Distribution</td>
<td>The <strong>OS Type</strong> shows the template value selected while creating the VMs. However, it might not be the actual operating system installed on the VM.</td>
</tr>
<tr>
<td>Boot Attestation Status of Hypervisors</td>
<td>Displays the boot attestation status of VMs. For details, see the product documentation for McAfee® Boot Attestation Service.</td>
</tr>
<tr>
<td>Usage Metering Report</td>
<td>Displays the usage of cloud accounts in number of hours per month. This data is displayed for six months.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Usage Start Time</strong> — Specifies starting month and year for the usage calculation.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Account Name</strong> — Specifies the name of the cloud account.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Sum of Total vCPU Usage Hours</strong> — Specifies the sum of CPU usage hours.</td>
</tr>
<tr>
<td>Endpoint Scan Report</td>
<td>Displays the details of the last scan of the endpoints.</td>
</tr>
<tr>
<td></td>
<td>To get accurate data in the Endpoint Scan Report, before running this report, select **Menu</td>
</tr>
<tr>
<td></td>
<td>• <strong>Endpoint</strong> — Displays the name of the endpoint.</td>
</tr>
<tr>
<td></td>
<td>• <strong>IP Address</strong> — Displays the IP address of the endpoint.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Category</strong> — Displays the group/resource pool/host of the endpoint.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Operating System</strong> — Displays the operating system details.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Last Scan</strong> — Displays the last on-demand scan time for an endpoint with anti-virus software.</td>
</tr>
</tbody>
</table>
Endpoints Security Report displays the protection status of the endpoints.

To get accurate data in the Endpoint Scan Report, before running this report, select Menu | Automation | Server Tasks and run the server task Data Center: Compute Endpoint Reports.

- **Endpoint** — Displays the name of the endpoint.
- **IP Address** — Displays the IP address of the endpoint.
- **Virtual** — Specifies whether the endpoint is a virtual system.
- **VM Classification** — Specifies if the VM is a part of public (Cloud Machine) or private (Virtual Machine) cloud.
- **Vendor** — Displays the name of the cloud service provider of the endpoint.
- **Power Status** — Specifies the power status of the endpoint.
- **Category** — Displays the group/resource pool/host of the endpoint.
- **Operating System** — Displays the operating system details.
- **AntiVirus/Antimalware** — Displays the name of the McAfee anti-virus and anti-malware software installed on the endpoint.
- **Firewall** — Displays the name of the McAfee software with the firewall protection active on the endpoint.
- **Whitelisting** — Specifies whether the whitelisting feature is enabled.
- **Access Protection** — Displays the name of the McAfee software that provides access protection.
- **Memory Protection** — Displays the name of the McAfee software that provides memory protection.
- **Last Communication** — Displays the time details of the last server-client communication.

<table>
<thead>
<tr>
<th>Query</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Security Report</td>
<td>Displays the protection status of the endpoints.</td>
</tr>
<tr>
<td>To get accurate data in the Endpoint Scan Report, before running this report, select Menu</td>
<td>Automation</td>
</tr>
<tr>
<td>Endpoint</td>
<td>Displays the name of the endpoint.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Displays the IP address of the endpoint.</td>
</tr>
<tr>
<td>Virtual</td>
<td>Specifies whether the endpoint is a virtual system.</td>
</tr>
<tr>
<td>VM Classification</td>
<td>Specifies if the VM is a part of public (Cloud Machine) or private (Virtual Machine) cloud.</td>
</tr>
<tr>
<td>Vendor</td>
<td>Displays the name of the cloud service provider of the endpoint.</td>
</tr>
<tr>
<td>Power Status</td>
<td>Specifies the power status of the endpoint.</td>
</tr>
<tr>
<td>Category</td>
<td>Displays the group/resource pool/host of the endpoint.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Displays the operating system details.</td>
</tr>
<tr>
<td>AntiVirus/Antimalware</td>
<td>Displays the name of the McAfee anti-virus and anti-malware software installed on the endpoint.</td>
</tr>
<tr>
<td>Firewall</td>
<td>Displays the name of the McAfee software with the firewall protection active on the endpoint.</td>
</tr>
<tr>
<td>Whitelisting</td>
<td>Specifies whether the whitelisting feature is enabled.</td>
</tr>
<tr>
<td>Access Protection</td>
<td>Displays the name of the McAfee software that provides access protection.</td>
</tr>
<tr>
<td>Memory Protection</td>
<td>Displays the name of the McAfee software that provides memory protection.</td>
</tr>
<tr>
<td>Last Communication</td>
<td>Displays the time details of the last server-client communication.</td>
</tr>
</tbody>
</table>
### Query Definition

<table>
<thead>
<tr>
<th>Query</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Asset Management Report</td>
<td>Displays the security status of vCenter endpoints.</td>
</tr>
<tr>
<td></td>
<td>This report is visible only after you install the Data Center Connector for vSphere extension.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Endpoint</strong> — Displays the name of the endpoint.</td>
</tr>
<tr>
<td></td>
<td>- <strong>IP Address</strong> — Displays the IP address of the endpoint.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Operating System</strong> — Displays the operating system details.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Power Status</strong> — Specifies the power status of the endpoint.</td>
</tr>
<tr>
<td></td>
<td>- <strong>VM Classification</strong> — Specifies if the VM is a part of public (<strong>Cloud Machine</strong>) or private (<strong>Virtual Machine</strong>) cloud.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Category</strong> — Displays the group/resource pool/host of the endpoint.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Host</strong> — Displays the host IP address.</td>
</tr>
<tr>
<td></td>
<td>- <strong>vCenter</strong> — Displays the vCenter IP address.</td>
</tr>
<tr>
<td></td>
<td>- <strong>AntiVirus/Antimalware</strong> — Displays the name of the McAfee anti-virus and anti-malware software installed on the endpoint.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Firewall</strong> — Displays the name of the McAfee software with the firewall protection active on the endpoint.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Whitelisting</strong> — Specifies whether the whitelisting feature is enabled.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Access Protection</strong> — Displays the name of the McAfee software that provides access protection.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Memory Protection</strong> — Displays the name of the McAfee software that provides memory protection.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Last Communication</strong> — Displays the time details of the last server-client communication.</td>
</tr>
<tr>
<td>Data Protection per Cloud Volume</td>
<td>Displays the number of volumes that are encrypted and not encrypted.</td>
</tr>
<tr>
<td>Data Protection per Cloud VM</td>
<td>Displays the number of VMs that are encrypted and not encrypted.</td>
</tr>
</tbody>
</table>

### Data Center and Public Cloud dashboards

The Data Center and the Public Cloud dashboards are added to your McAfee ePO server when you install the datacenter software.

- The Data Center dashboard displays a collection of monitors based on the results of the default datacenter software queries.

- The Public Cloud dashboard displays the collection of monitors for default public cloud account queries.

  The data in these monitors on the dashboard is refreshed every 15 minutes.
The default monitors that appear under these dashboards are:

- **Data Centers** — Displays all registered datacenters.

![Data Centers Pie Chart](image1)

- **OS Distribution** — Displays the operating system type. It shows the template value selected while creating the VMs. However, it might not be the actual operating system installed on the VM.

![OS Distribution Pie Chart](image2)

- **Security Incidents (last 14 days)** — Specifies events reported for these components on the VMs in the last 14 days.
  - Application Control
  - Antivirus
- Firewall
- Memory Protection
- **Anti-malware Status** — Displays the state of the VM.
  - **Application Control Enabled** — These VMs have McAfee Application Control installed and enabled.
  - **Only Anti-Virus Enabled** — These VMs have a McAfee anti-virus product installed and enabled.
  - **Unprotected** — These VMs don't have any McAfee anti-malware product enabled.

- **Host Firewall Status** — Displays the state of the system.
  - **Firewall Enabled** — These VMs have McAfee Host Intrusion Prevention installed.
  - **Not in use** — These VMs don't have McAfee Host Intrusion Prevention installed.
• **File Integrity Monitoring Status** — Displays the number of VMs with File Integrity Monitoring (FIM) installed and enabled.
  
  • **Enabled** — File Integrity Monitoring is enabled on these VMs.
  
  • **Not enabled** — File Integrity Monitoring is disabled on these VMs.
  
  • **Not installed** — File Integrity Monitoring isn’t installed on these VMs.

For more details about FIM, see the product documentation for McAfee Change Control.

• **Data Protection per Cloud Volume** — Displays the number of volumes that are encrypted and the number of volumes that are not encrypted.
• **Data protection per Cloud VM** — Displays the number of VMs that are encrypted versus number of VMs that are not encrypted.

  - **Encrypted** — These VMs are encrypted.
  - **Not Encrypted** — These VMs are not encrypted.

<table>
<thead>
<tr>
<th>Encryption Status</th>
<th>Number of VMs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypted</td>
<td>8</td>
</tr>
<tr>
<td>Not Encrypted</td>
<td>31</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>39</strong></td>
</tr>
</tbody>
</table>

• **Usage Metering Report** — Displays the usage of cloud accounts by the instances, in number of hours per month.

  - **Usage Start Time** — Specifies starting month and year for the usage calculation.
  - **Account Name** — Specifies the name of the cloud account.
  - **Sum of Total vCPU Usage Hours** — Specifies the sum of CPU usage hours.
• **Application Reputation** — Categorizes the applications based on McAfee GTI file reputation.
  
  - Good
  
  - Bad
  
  - Unclassified

  This dashboard retrieves data from the McAfee Application Control extension.

  ![Application Reputation Dashboard](image)

  For details about file reputation, see the product documentation for McAfee Application Control.

• **Boot Attestation Status for Hypervisors** — Displays the Boot Attestation status of vCenter hypervisors. For details, see the product documentation for Boot Attestation Service.

• **Endpoint Scan Report** — Displays the last scan details of the endpoints.

  This report is run every eight hours.

  - **Endpoint** — Displays the name of the endpoint.
  
  - **IP Address** — Displays the IP address of the endpoint.
  
  - **Category** — Displays the group/resource pool/host of the endpoint.
  
  - **Operating System** — Displays the operating system details.
  
  - **Last Scan** — Displays the last on-demand scan time for an endpoint with different anti-virus software.

  To get accurate data in the Endpoint Scan Report, before running this report, select **Menu | Automation | Server Tasks** and run the server task **Data Center: Compute Endpoint Reports**.

• **Endpoint Security Report** — Displays the protection status of the endpoints.

  This report is run every eight hours.

  - **Endpoint** — Displays the name of the endpoint.
  
  - **IP Address** — Displays the IP address of the endpoint.
• **Virtual** — Specifies whether the endpoint is a virtual system.

• **VM Classification** — Specifies if the VM is a part of public (Cloud Machine) or private (Virtual Machine) cloud.

• **Vendor** — Displays the name of the cloud service provider of the endpoint.

• **Power Status** — Specifies the power status of the endpoint.

• **Category** — Displays the group/resource pool/host of the endpoint.

• **Operating System** — Displays the operating system details.

• **AntiVirus/Antimalware** — Displays the name of the McAfee anti-virus and anti-malware software that is installed on the endpoint.

• **Firewall** — Displays the name of the McAfee software with the firewall protection active on the endpoint.

• **Whitelisting** — Specifies whether the whitelisting feature is enabled.

• **Access Protection** — Displays the name of the McAfee software that provides access protection.

• **Memory Protection** — Displays the name of the McAfee software that provides memory protection.

• **Last Communication** — Displays the time details of the last server-client communication.

---

To get accurate data in the Endpoint Scan Report, before running this report, select **Menu | Automation | Server Tasks** and run the server task **Data Center: Compute Endpoint Reports**.

---

• **vCenter Asset Management Report** — Displays the security status of vCenter endpoints.

  This report is visible only after you install the Data Center Connector for vSphere extension.

• **Endpoint** — Displays the name of the endpoint.

• **IP Address** — Displays the IP address of the endpoint.

• **Operating System** — Displays the operating system details.

• **Power Status** — Specifies the power status of the endpoint.

• **VM Classification** — Specifies if the VM is a part of public (Cloud Machine) or private (Virtual Machine) cloud.

• **Category** — Displays the group/resource pool/host of the endpoint.

• **Host** — Displays the host IP address.

• **vCenter** — Displays the vCenter IP address.

• **AntiVirus/Antimalware** — Displays the name of the McAfee anti-virus and anti-malware software that is installed on the endpoint.

• **Firewall** — Displays the name of the McAfee software with the firewall protection active on the endpoint.

• **Whitelisting** — Specifies whether the whitelisting feature is enabled.

• **Access Protection** — Displays the name of the McAfee software that provides access protection.

• **Memory Protection** — Displays the name of the McAfee software that provides memory protection.

• **Last Communication** — Displays the time details of the last server-client communication.
Additional information

Here is information on the SVM security requirements and setting up the required resources for deploying MOVE AntiVirus (Agentless) in an NSX environment.

Contents

- SVM security requirements
- Install a vSphere Distributed Switch
- Prepare ESXi servers
- Install the guest introspection service
- Frequently asked questions
SVM security requirements

The following security measures are implemented on the SVM.

<table>
<thead>
<tr>
<th>Security measure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>apparmor</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: /etc/apparmor.d/opt.McAfee.move.bin.msvc. There are two apparmor modes: complain and enforce. By default, msvc is in enforce mode. You can change the mode to complain with the aa-logprof command. To enable enforce mode, use the aa-enforce msvc command. While in complain mode, you can use the command aa-logprof to analyze any requests that the process has made outside of its profile. For more information, visit this website: <a href="https://help.ubuntu.com/12.04/serverguide/apparmor.html">https://help.ubuntu.com/12.04/serverguide/apparmor.html</a></td>
</tr>
<tr>
<td>iptables</td>
<td>The sva-firewalls script enables the built-in firewall. Usage is sva-firewalls: start</td>
</tr>
<tr>
<td>SVM .vmx</td>
<td>Add these options to harden the SVM from a VM perspective: isolation.tools.diskWiper.disable=TRUE isolation.tools.diskShrink.disable=TRUE isolation.device.connectable.disable=TRUE isolation.device.edit.disable=TRUE RemoteDisplay.maxConnections=1 vmci0.unrestricted=FALSE log.rotateSize=1000000 log.keepOld=10 For more information, visit this website: <a href="http://www.vmware.com/security/hardening-guides">http://www.vmware.com/security/hardening-guides</a></td>
</tr>
</tbody>
</table>

Install a vSphere Distributed Switch

To use MOVE AntiVirus (Agentless) in a VMware NSX virtual network environment, your vCenter Server must be using a vSphere Distributed Switch (vDS).

**Task**

1. Open your vSphere Web Client and navigate to your datacenter in your networking inventory.
2. Right-click on the datacenter and select New vSphere Distributed Switch to display the New Distributed Switch wizard.
3. Type a name for the distributed switch.
4 Select Distributed Switch Version: 5.5 or later.

5 Click Edit Settings and change these settings:
   a Select the number of uplink ports.
   b Set Network I/O Control to Enabled.
   c Choose to create a default port group.
   d Give the Port Group a name.

6 Confirm your settings and click Finish.

Your vSphere Distributed Switch is now installed.

---

Prepare ESXi servers

Before the MOVE AV service can be deployed to your datacenter, your ESXi servers must first be prepared by installing the drivers necessary for network traffic inspection. This operation is performed on the cluster.

**Task**

1 In your vSphere Web Client, go to Home | Networking & Security Installation and click the Host Preparation tab.

2 Locate the NSX cluster you are going to protect with MOVE AntiVirus (Agentless) in the Clusters & Hosts list and click Install in the Installation Status column.

   The installation completes and the driver version is displayed in the Installation Status column.

Host preparation is now complete. For more complete instructions on host preparation, see your VMware documentation.
Install the guest introspection service

To protect your VMs with MOVE AntiVirus (Agentless), you must install the guest Introspection service on the cluster that contains your ESXi servers.

**Task**

1. Log on to the VMware vSphere Web Client as a root user.

2. Click **Home | Networking & Security | Installation | Service Deployments**, then click the **+** icon to display the **Deploy Network & Security Services** window.

3. From **Select services & schedule**, select the **Guest Introspection** service and click **Next**.

   You can deploy immediately, or you can schedule for a later deployment.
From **Select clusters**, select the cluster that contains the ESXi servers and VMs that you want to protect, then click **Next**.
From **Select storage and Management Network**, for each cluster, select a datastore on which to store the MOVE SVM, the network (the distributed port group used by the vDS on the datacenter), and the IP assignment for the MOVE AntiVirus service to use.

The selected datastore must be available on all hosts in the selected cluster. Or, you can select **Specified on host**. If you are assigning static IP pools in the IP Assignment column to the MOVE AntiVirus service or Guest Introspection service, make sure that your default gateway and DNS is reachable/resolvable and the prefix length is correct. If not, the MOVE AntiVirus and Introspection service VMs are not activated and they cannot communicate to the NSX manager or McAfee ePO because their IPs are not on the same network as McAfee ePO or the NSX Manager.

If you selected **Specified on host**, the datastore for the ESXi host must be specified in the **AgentVM Settings** of the host before it is added to the cluster. For details, see vSphere API/SDK documentation. For details about configuring this network and IP address range with NSX Manager and vSphere Web Client, see *NSX Administration Guide* available at [http://pubs.vmware.com/NSX-6/index.jsp](http://pubs.vmware.com/NSX-6/index.jsp).

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

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

Review the settings and click **Finish** to complete the deployment of Guest Introspection service. When deployment is complete, the Guest Introspection service appears in the list of **Network & Security Service Deployments**.

The Guest Introspection service is now deployed to the cluster when the **Installation Status** is **Successful** and the **Service Status** is **UP**.
Frequently asked questions

Here are answers to some of the most frequently asked questions relating to the security implications of running MOVE AntiVirus and using its deployment modes.

MOVE AntiVirus Agentless and Multi-Platform

What is the difference between MOVE AntiVirus (Multi-Platform) and (Agentless) deployments?

- **Agentless** mode leverages VMware vSphere offloading APIs.
- **Multi-Platform** mode uses the McAfee unique network-based offloading that works on any hypervisor platform (including VMware vSphere).

How can I purchase MOVE AntiVirus?

You can purchase MOVE AntiVirus as a standalone product (for servers or virtual desktops) or as part of one of the following suites:

- McAfee Server Security Suite Essentials
- McAfee Server Security Suite Advanced
- McAfee Security Suite for Virtual Desktops

How do the Agentless and Multi-Platform deployment options compare?

This table outlines the features offered in each deployment option as of MOVE AntiVirus 3.6.1.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Agentless deployment</th>
<th>Multi-Platform deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-Access Scanning</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>On-Demand Scanning (ODS)</td>
<td>Weekly scheduling</td>
<td>Weekly and instant scheduling</td>
</tr>
<tr>
<td>Quarantine restore</td>
<td>Restore from utility</td>
<td>Restore from McAfee ePO</td>
</tr>
<tr>
<td>Automatic SVM deployment through NSX</td>
<td>Yes</td>
<td>NA</td>
</tr>
<tr>
<td>Automatic SVM deployment through vCloud Networking and Security Manager</td>
<td>Yes</td>
<td>NA</td>
</tr>
<tr>
<td>Flexible tuning policies</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Exclusions</td>
<td>Path-based only</td>
<td>Path-based and process name-based</td>
</tr>
<tr>
<td>GTI File Reputation</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Available with Server Security suites</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SVM Manager for scan server load balancing</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Locate unprotected endpoints through scan reports</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Visibility to enabled OS memory protection</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>McAfee Agentless Firewall</td>
<td>Yes</td>
<td>NA</td>
</tr>
</tbody>
</table>

What are the architectural differences between Agentless and Multi-Platform?

This table describes the architectural differences at a high level.
**Which is the better deployment option?**

It is not necessary to compare one deployment versus another. We offer options for the flexibility you need, and all deployment options are included in the license. Use the following requirements to guide your choice of a deployment option.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Deployment option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using multiple hypervisors: VMware/Citrix/Microsoft</td>
<td>Multi-Platform deployment</td>
</tr>
<tr>
<td>Using VMware vSphere</td>
<td>Either deployment option</td>
</tr>
<tr>
<td>Support for end-user notifications in guest (pop-ups)</td>
<td>Multi-Platform deployment</td>
</tr>
<tr>
<td>Instant protection without deploying software to the VM</td>
<td>Agentless deployment</td>
</tr>
<tr>
<td>Support for GTI Proxy</td>
<td>Multi-Platform deployment</td>
</tr>
<tr>
<td>Flexible Scan server concept and not on every physical HV</td>
<td>Multi-Platform deployment</td>
</tr>
<tr>
<td>Scanning of network drives</td>
<td>Multi-Platform deployment</td>
</tr>
<tr>
<td>Support for VMware vMotion</td>
<td>Either deployment option</td>
</tr>
<tr>
<td>Unique security policy per virtual machine</td>
<td>Either deployment option</td>
</tr>
</tbody>
</table>

**Which operating system and hypervisor environments does MOVE AntiVirus support?**

MOVE AntiVirus offers support for multiple operating systems and hypervisor environments. To view the supported operating systems and hypervisor environments, go to [http://kc.mcafee.com/corporate/index?page=content&id=KB74865](http://kc.mcafee.com/corporate/index?page=content&id=KB74865).

**How long will MOVE AntiVirus 2.6 and 3.0 be supported?**

With the release of MOVE AntiVirus 3.6, we announced the end-of-sale for MOVE AntiVirus 2.6 and MOVE AntiVirus 3.0. These versions are no longer available on the download site. End-of-support is set for January 4, 2016. We recommend that you upgrade to MOVE AntiVirus 3.6 as soon as you can.

**Where can I find the product documentation for MOVE AntiVirus?**

These links provide the product documentation details for both MOVE AntiVirus deployment options.
- **Agentless**
- **Multi-Platform**

**What is included with the MOVE AntiVirus for Virtual Servers?**

MOVE AntiVirus for Virtual Servers (SKU: MOVCKE) ships with the following:
- MOVE AntiVirus for Virtual Servers
  - Multi-Platform deployment option
    - Support for VMware vSphere, ESX/ESXi, Citrix XenServer, Microsoft Hyper-V
What is included with MOVE AntiVirus for Virtual Desktops?

MOVE AntiVirus for Virtual Desktops (SKU: MOVCDE) ships with the following.

- MOVE AntiVirus for Virtual Desktops
- Multi-Platform deployment option
  - Support for VMware Horizon View, Citrix XenDesktop, Citrix VDI-In-A-Box, and Microsoft Hyper-V
- Agentless deployment option
  - Support for VMware Horizon View, Citrix XenDesktop, Citrix VDI-In-A-Box (requires VMware vShield Endpoint)
- McAfee VirusScan Enterprise (for use on offload servers only)
- McAfee VirusScan Enterprise for Linux (for use on offload servers only)
- Data Center Connector for vSphere
- McAfee Host IPS for Desktops
- McAfee SiteAdvisor Enterprise Plus
- McAfee ePO

Is MOVE AntiVirus offered as part of any security suites?

Yes, MOVE AntiVirus is a featured product within three separate security suites from McAfee.

- McAfee Server Security Suite Essentials
- McAfee Server Security Suite Advanced
- McAfee Security Suite for VDI

The two McAfee Server Security Suites include several other products. They also provide the McAfee Data Center Connectors for the public cloud; these add McAfee ePO integration with Amazon Web Services accounts and OpenStack and Microsoft Azure. Further information about McAfee's security suites for the datacenter is available at: https://sales.mcafee.com/us/employee/sales/sales-plays/server-security.aspx.

Can I upgrade to the latest version of MOVE AntiVirus?

Yes, with a valid support contract.

If I purchased MOVE AntiVirus when it did not include any other product components, am I eligible for the new MOVE AntiVirus components?

Yes. The same MOVE AntiVirus SKU is used for the new release. When you enter the grant number on the download website, all product components associated with the SKU are available for download.

What should I do if I am purchasing MOVE AntiVirus, but already have a license for McAfee VirusScan Enterprise?
MOVE AntiVirus is not eligible for a discount, because McAfee VirusScan Enterprise is not included in MOVE AntiVirus. Only a limited-use license of McAfee VirusScan Enterprise is included for the offload server but not for the virtual desktops.

**Which hypervisors are supported for MOVE AntiVirus?**

For a complete list of supported hypervisors, see the supportability site at https://kc.mcafee.com/corporate/index?page=content&id=KB74865.

**Which virtual machine operating systems are supported?**

See Requirements in this document for your virtual environment.

**Does MOVE AntiVirus (Agentless) work with Citrix XenDesktop, or is my only option to use Multi-Platform?**

The Agentless deployment requires a VMware hypervisor. For Citrix XenDesktop, use MOVE AntiVirus (Multi-Platform).

**Why does MOVE AntiVirus (Agentless) support only path-based exclusions?**

Currently the vShield Endpoint driver is limited to path exclusions. We have requested VMware to expand the options with exclusions. However, MOVE AntiVirus Multi-Platform deployment option allows you to exclude processes and define exclusions based on path and file name.

**How do I size the resources for my SVMs when using (Agentless) deployment?**

One SVM is required for each ESX hypervisor. Because of the architecture of vShield Endpoint, each ESX host must have access to the disk subsystem.

**What resources do I need to set up my SVM?**

The SVM is preconfigured with 2 GB of RAM and 2 vCPUs, which is the correct virtual resources for most environments. We recommend that you monitor the ESXi average CPU usage and ESXi average Active Memory usage using the default OVF template. If the default configuration shows that more resources are needed, increase the number of vCPUs for the MOVE AntiVirus (Agentless) SVM.

**How do I clean up McAfee ePO from Dynamic Virtual Desktops that are no longer present?**

McAfee Agent 4.8 or later offers improved management of Dynamic Virtual Machines. Installing the agent in a new "VDI mode" deprovisions the virtual image every time it is shut down and enables the McAfee ePO server to save the deprovisioned agents in its database.

**Does the McAfee ePO console display virtual machines if McAfee Agent isn't deployed?**

When managing MOVE AntiVirus (Agentless), McAfee Agent is installed on the SVM and the SVM is shown in the McAfee ePO console. But, because there is no McAfee component on each virtual machine, each virtual machine does not currently appear in McAfee ePO. However, this is now possible with Data Center Connector for vSphere.

**If McAfee Agent is not installed on virtual machines running MOVE AntiVirus (Agentless), what details are included in the reports?**

We provide detailed reporting, and obtain the specific VM name from vCenter when an event occurs on the SVM.

**Can we have a view in the McAfee ePO System Tree of all virtual endpoint protected by an SVM?**

If you check in the Data Center Connector for vSphere extension and register the VMware vCenter account, you can view the VMware vCenter servers, hypervisors, and virtual machines.

**Why is there no event notification on the guest VM (client pop-up)?**

VMware currently can't notify the user without installing an agent on the guest VM. Trend Micro has built their own client agent and they deploy it to all virtual machines to provide a guest notification. We don't see the point to deploy an agent, when the solution is agentless just to get a notification. We have asked VMware to make a way for us to notify the guest using their vShield Endpoint thin agent in VMtools. It is on their roadmap. For today, if this is an important feature for you, we recommend that you use MOVE AntiVirus (Multi-Platform).

**How do I enable logging for Syslog?**
1. Log on to the SVM console.
2. Run this command to open and edit the file 25-discard.conf:
   
   ```
   sudo vi /etc/rsyslog.d/25-discard.conf.
   ```
   
   **Make sure that you run the command with Sudo permission.**
3. Add `#` in front of `*.debug` and `*.info`.
4. Save the file.
5. Run this command to restart service:
   
   ```
   service rsyslog restart.
   ```
6. Access the log at: `/var/log/syslog`.

**SVM and McAfee ePO time zones are not synchronized, so the events are rejected and the database is not updated. What do I do?**

See the KnowledgeBase article [KB82196](#).

You can also try these steps:

**Method 1**

1. Restart the MOVE AntiVirus services and send the events to McAfee ePO.
2. Perform a Data Center Connector sync.

**Method 2**

1. On the systems where you see the issue, run these commands one at a time.
   
   ```
   • fltmc unload vsepflt
   • fltmc load vsepflt
   ```
2. Send the events to McAfee ePO.
3. Perform a Data Center Connector sync.

When the events are uploaded to McAfee ePO and you verify that the sync requests are successful, the updated status is displayed.

Check the registration of the SVMs with their respective hypervisors. The SVMs are listed in the vShield tab.

**During the SVM configuration, I specified a McAfee ePO local account. Can this account continue to be active or enabled with the same password?**

Once the deployment is completed, the password field is not used. The only requirement is that if you logged on as `admin` with the password as `xx`. Use the same password `xx` for SVM deployment.

**So, can I disable or delete the McAfee ePO account once the final SVM is registered?**

Yes.

**When running a report from queries and reports, it displays only the MOVE AntiVirus appliance that detected the malware, but not the virtual server where that malware was detected.**

The vCenter IP address and credentials are not properly configured in the SVA policy.

**How do I verify that the applied exclusions are working?**
See KnowledgeBase article KB73316.

All the commands documented in the article must be specified with elevated permission. Either run the command with `sudo` or use `sudo -s` to elevate the command prompt from $ to #, root level.

**Does MOVE AntiVirus occupy memory from high to low address on Windows 64-bit? In some extreme scans on large files, is memory use limited for MOVE AntiVirus?**

The memory allocation typically depends on the Microsoft architecture. MOVE AntiVirus does not interfere with this behavior. In scenarios where a complex or large file is scanned, make sure that you use the scan time-out setting to end the scanning, if the file is taking unexpectedly long.

McAfee AV engine scans the file in small chunks and scans only certain parts of the files. So, there should not be any noticeable memory increase when scanning large files.
Index

A
about this guide 7
access protection 97
account
  NSX Manager 32
  vShield Manager 60
accounts, registering 28, 56
  VMware vCenter 28, 56
Agentless deployment option 115
  install extension 16, 28, 56
  integration with ePolicy Orchestrator 81
  policy management 81
anti-malware status dashboard 100
application control 97, 100
application reputation dashboard, GTI 100

B
Boot Attestation Service 97, 100

C
change control
  file integrity monitoring status 97, 100
common configuration
  setting up 30, 58
components
  defined 11
  overview 11
configuration
  quarantine settings 87
  security tags 44
  security virtual appliance 19
  tagging 46
  VM-based scanning 91
connector, choosing 28, 56
conventions and icons used in this guide 7

D
dashboards, datacenter (continued)
  OS Distribution 100
  security incidents 100
Data Center Connector for vSphere
  install extension 16, 27, 55
default queries, displaying 97
deployment
  McAfee ePO 51
  MOVE AV service 23, 36
  options 18
  overview 23
  OVF 69
deployment option
  Agentless 115
  manual 69
  Multi-Platform 115
diagnostic tool
  running 92
  scan avoidance 12
distributed switch
  installing 110
documentation
  audience for this guide 7
  product-specific, finding 8
typographical conventions and icons 7

E
editing
  NSX Manager 32
  vShield Manager 60
ePolicy Orchestrator
  install extension 16, 27, 55
  integration with Agentless 81
exporting
  scan policy 35
extensions
  Agentless deployment option 16, 28, 56
  downloading 15, 26
  installing 16, 27, 28, 51, 55, 56, 71
  removing 76, 78, 79
  VirusScan for Linux 17
Index

F
features 12
file reputation 100
FIM (File Integrity Monitoring Status) 100
firewall status 100
frequently asked questions 115

G
GTI (Global Threat Intelligence), file reputation 100
Guest Introspection service
installing 112

H
Health and Alarms page
view 94
Host Intrusion Prevention
host firewall status 97, 100
hosts, adding 44
hypervisors 28, 56

I
installation
extensions 16, 28, 56
test 85
vCloud Networking and Security Manager 69
VirusScan for Linux extension 17
VMware Tools 69
VMware vShield Endpoint 69

L
LDAP server
configuring and registering 51

M
management
diagnostic tool 92
policies 81
quarantine 87
scan policies 89
McAfee ServicePortal, accessing 8
MOVE AV Agentless 75, 77
MOVE AV service
deploying 23, 36
removing 75, 77
upgrading 73, 74
MOVE service
register 34

N
NSX Manager
editing 32
removing 76

NSX tagging
enabling 45, 46

O
open virtualization format
deployment options 18
manual deployment 69
properties 20
overview
deployment process 23

P
permissions
VMware vCenter 51
policies
Agentless 81
applying 85
assigning 72
configuring for Agentless 82
creating a Scan policy 83
creating an SVA policy 82
management 81
Scan 82, 83
SVA 82
protection status, displaying 97, 100

Q
quarantine
folder, configuring 90
overview 87
restore a file 88
restore tool 87
scan policy settings 89
queries
reports 95
queries, datacenter
predefined 97
queries, MOVE AV Agentless
default, viewing 97
pie charts 97
predefined 95
viewing default queries 97

R
register
MOVE service 34
vCenter server 26
removing
MOVE service 77
reports 95
reports, datacenter 97
anti-malware status 100
application reputation 100
reports, datacenter 97 (continued)
  File Integrity Monitoring Status 100
  Firewall Status 100
  OS Distribution 100
  security incidents 100
requirements
  NSX Manager-based deployment 24
operating systems 24, 52
software 24, 52
SVM security 24, 52
vCNS-based deployment 52
rollback, SVM deployment 66

S
scan configuration
  enabling 91
scan diagnosis 92
scan policies
  creating 83
  exporting 35
quarantine configuration 89
scenario
  service composer 46
security group
  applying security policy 43
  creating 42
security group, configuring 40
security incidents dashboard 100
security policies
  configuring 43
security policy
  assigning to security group 43
  creating 40
security tags
  enabling 44
security virtual appliance
  create a policy 82
  deploying 72
  manually configure 19
security virtual machine
  monitoring 94
  view status 94
ServicePortal, finding product documentation 8
status
  firewall 100
status (continued)
  trust 100
SVM deployment
  viewing details 66
SVM package
  checking in 31
SVM security
  configuring 18
  monitoring 81
  requirements 24, 52
T
tags
  defining 28, 56
technical support, finding product information 8
threat event log 94
type
  SVM deployment 66
U
uninstalling 75, 77
upgrading
  manually 71
V
virtual machines
  boot status 28, 56
virtual properties, displaying 28, 56
VMware vCenter
  registering 51
VMware vCenter account
  defining 28, 56
  registering 28, 56
VMware vShield Endpoint
  deploy the SVM 69
  installation 69
vShield Manager
  configuring and registering 51
  editing 60