Installation Guide

McAfee Management for Optimized Virtual Environments AntiVirus 4.5.0

For use with McAfee ePolicy Orchestrator
COPYRIGHT
© 2017 Intel Corporation

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 7

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

1 Planning your installation 9
System and hardware requirements ...................... 9
Supported McAfee management platform and software 11
Supported VMware management platform and software 11
Advantages of preconfiguring the product .............. 13
Are you upgrading an existing version? .................. 13
Are you ready to install? ............................. 14
Downloading software extensions and packages .......... 14

2 Multi-Platform installation and configuration 17
SVM assignment made easy .......................... 17
Multi-Platform deployment process using McAfee MOVE AntiVirus autoscaling ......... 18
Install the product files on the management server ....... 19
Register a VMware vCenter account with McAfee ePO ........ 20
Set up the SVM Manager ............................. 22
Deploy the McAfee MOVE AntiVirus SVM .............. 23
Check in the SVM package .......................... 23
Create a product deployment client task ................ 24
Assign a client task ............................... 24
Deploying the McAfee MOVE AntiVirus client ............ 25
Check in the client package .......................... 25
Create a product deployment client task ................ 26
Assign a client task ............................... 26
Assign the SVM using SVM Manager .................... 27
Add or edit an SVM Manager assignment rule using IP address ............... 28
Add or edit an SVM Manager assignment rule using McAfee ePO tag .............. 29
Install the McAfee MOVE AntiVirus client manually .......... 31
Exporting an SVM OVF template ........................ 32
Export the SVM OVF template using the export utility .......... 32
Export the SVM OVF template manually .................. 33
Export the OVF template manually ...................... 36
Specify the SVM template path in McAfee ePO ............. 37
Create an infrastructure group in McAfee ePO ............. 38
Enable and configure SVM autoscale settings ............... 39
Autoscale SVM details ................................ 41
Upgrade the standby SVMs .......................... 42
Deploy in a XenDesktop or VMware View environment ....... 42
Integrating TIE and Advanced Threat Defense ............. 43
How Threat Intelligence Exchange works ................. 43
Contents

Upgrade McAfee MOVE AntiVirus (Agentless) in an NSX environment ........ 100
Upgrade McAfee MOVE AntiVirus in vCNS environment ........................... 102
Uninstalling McAfee MOVE AntiVirus (Agentless) ................................. 102
Uninstalling McAfee MOVE AntiVirus (Agentless) 4.5.0 in an NSX environment 103
Uninstalling McAfee MOVE AntiVirus (Agentless) in a vCNS environment .... 104

Index .......................... 107
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.

- *Italic* — Title of a book, chapter, or topic; a new term; emphasis
- **Bold** — Text that is emphasized
- **Monospace** — Commands and other text that the user types; a code sample; a displayed message
- **Narrow Bold** — 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**: Extra information to emphasize a point, remind the reader of something, or provide an alternative method

**Tip**: Best practice information

**Caution**: Important 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 https://support.mcafee.com and click the Knowledge Center tab.
2. In the Knowledge Base pane under Content Source, click Product Documentation.
3. Select a product and version, then click Search to display a list of documents.
Planning your installation

Your Security Virtual Machine (SVM) and virtual systems must have specific hardware and software to run McAfee MOVE AntiVirus. Review these requirements and recommendations before installing the software to make sure that your installation is successful.

Contents

- System and hardware requirements
- Supported McAfee management platform and software
- Supported VMware management platform and software
- Advantages of preconfiguring the product
- Are you upgrading an existing version?
- Are you ready to install?
- Downloading software extensions and packages

System and hardware requirements

Make sure that each of your servers or workstations is running a supported version of Microsoft Windows and conforms to these requirements.

SVM requirements (Multi-Platform)

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

- **Operating system**
  - Windows Server 2008 R2 SP1
  - Windows Server 2008 SP2 (64-bit)
  - Windows Server 2012 R2
  - Windows Server 2016 (64-bit)

- **CPU**
  - CPU 4 vCPU, 2 GHz or higher

- **Memory**
  - 6 GB RAM or higher

- **Hard disk space for SVM deployment**
  - 2 GB or higher

- **IP requirements**
  - Static IP address (required for configuring policies with IP address)
SVM Manager details (Multi-Platform)

Operating system: Ubuntu 16.04
Software:
- VirusScan Enterprise for Linux
- McAfee Agent 5.0.3

Hypervisors:
- VMware ESXi 5.5 or later
- Citrix XenServer 6.0 or later
- Microsoft 2012 R2 Hyper-V or later

All hypervisors are supported. However, we tested the above mentioned hypervisors only.

To deploy on Hyper-V, convert the .vmdk file, part of SVM Manager appliance, into a .vhd file, then attach .vhd file as hard disk to a new VM in Hyper-V. To convert .vmdk to .vhd, you can use the Microsoft Virtual Machine Converter software.

CPU: 2 vCPU
Memory: 2 GB RAM or higher
Hard disk space for SVM Manager deployment: 16 GB or higher

By default, the SVM Manager has 16 GB hard disk bundled with it.

SVM requirements (Agentless)

- You must use the virtual machine we provide for Agentless SVM. 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 SVM 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 |
  | Memoory      | 2 GB RAM or higher       |
  | Hard disk space for SVM Deployment | 2 GB or higher |

These items come pre-installed:

- Operating system: Ubuntu 16.04
- Software:
  - VirusScan Enterprise for Linux
  - McAfee Agent
  - McAfee MOVE AntiVirus (Agentless)

Client system requirements

The McAfee MOVE AntiVirus client software requires one of these operating systems:

- Windows Vista (32-bit or 64-bit)
- Windows Server 2008 SP2 (32-bit or 64-bit)
- Windows 7 (32-bit or 64-bit)
- Windows Server 2008 R2 SP1 (64-bit)
Windows 8 (32-bit or 64-bit)
Windows Server 2012
Windows 8.1 (32-bit or 64-bit)
Windows Server 2012 R2 (64-bit)
Windows 10 (32-bit or 64-bit)
(Multi-Platform only) Windows Server 2016 (64-bit)

Supported McAfee management platform and software

You must be running a supported version of McAfee management platform and software.

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Agentless</td>
</tr>
<tr>
<td>McAfee ePO</td>
<td>5.1.3, 5.3.1, or 5.3.2</td>
</tr>
<tr>
<td>For details, see the McAfee ePolicy Orchestrator Installation Guide.</td>
<td></td>
</tr>
<tr>
<td>Cloud Workload Discovery</td>
<td>4.5.0 or later</td>
</tr>
<tr>
<td>McAfee Agent</td>
<td>5.0.3 (Part of SVM package)</td>
</tr>
<tr>
<td>VirusScan Enterprise</td>
<td>NA</td>
</tr>
<tr>
<td>VirusScan Enterprise for Linux</td>
<td>2.0.3</td>
</tr>
<tr>
<td>TIE</td>
<td>NA</td>
</tr>
<tr>
<td>Advanced Threat Defense</td>
<td>NA</td>
</tr>
<tr>
<td>Virtual Advanced Threat Defense</td>
<td>NA</td>
</tr>
<tr>
<td>DXL</td>
<td>NA</td>
</tr>
</tbody>
</table>

Supported VMware management platform and software

You must be running a supported version of VMware software.

Table 1-1  Agentless

<table>
<thead>
<tr>
<th>Appliance and software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vCenter</td>
<td>5.5 U2, 6.0, or 6.5</td>
</tr>
<tr>
<td></td>
<td><img src="https://example.com" alt="vCNS deployment is not supported with vSphere 6.5." /></td>
</tr>
<tr>
<td>VMware ESXi</td>
<td>5.5.x, 6.0.x, or 6.5.x</td>
</tr>
<tr>
<td>VMware NSX Manager</td>
<td>6.1.2, 6.1.4, 6.2.1, 6.2.2, or 6.2.4</td>
</tr>
<tr>
<td>VMware vCloud Networking and Security Manager</td>
<td>5.5.4</td>
</tr>
</tbody>
</table>

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 Configuration</td>
<td>Permissions required to add details such as new virtual switch, port group, virtual NIC.</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 and firewall</td>
<td>Permissions to reconfigure outgoing firewall connections to allow retrieval of Filter 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.

<table>
<thead>
<tr>
<th>Configuration Location</th>
<th>Permission description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vApp &gt; Import</td>
<td>Permissions to deploy SVM from OVF file.</td>
</tr>
<tr>
<td>Datastore &gt; Allocate Space</td>
<td>Permissions required to allocate space for SVM on datastore.</td>
</tr>
<tr>
<td>Network &gt; Assign Network</td>
<td>Permissions to assign SVM to networks.</td>
</tr>
<tr>
<td>Virtual Machine &gt; Configuration &gt; Add new disk</td>
<td>Permissions to add disks to SVM.</td>
</tr>
<tr>
<td>Virtual Machine &gt; Interaction &gt; Power On</td>
<td>Permissions to turn on SVM.</td>
</tr>
<tr>
<td>Virtual Machine &gt; Interaction &gt; Power Off</td>
<td>Permissions to turn off SVM.</td>
</tr>
<tr>
<td>VirtualMachine &gt; Configuration &gt; Rename</td>
<td>Permissions to rename a virtual machine or change the associated notes of a virtual machine.</td>
</tr>
</tbody>
</table>

**Activating the Virtual Machine**

In this step, the SVM is activated.

<table>
<thead>
<tr>
<th>Configuration Location</th>
<th>Permission description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Machine &gt; Configuration &gt; Advanced</td>
<td>Permissions to reconfigure virtual machine for dvfilter</td>
</tr>
</tbody>
</table>

**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 changes 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.

Advantages of preconfiguring the product

You can customize settings for product features before deploying the product to managed systems. This customization enables you to meet specific requirements, for example, in environments with security compliance standards. Preconfigured policy settings take effect as soon as the product is installed on the endpoint.

McAfee preconfigures features with default settings to protect systems in medium-risk environments. The user can use the systems without any interruption and can access important applications until there is time to revise the settings.

To preconfigure product features, first create a policy and configure it with the settings for your environment. Then assign this policy to managed systems when you deploy the client software. See the product guide for your management platform for instructions about configuring and assigning policies.

Are you upgrading an existing version?

If a supported version of McAfee MOVE AntiVirus (Agentless) or (Multi-Platform) is installed in your environment, you can upgrade to McAfee MOVE AntiVirus 4.5.0.

Upgrading from McAfee MOVE AntiVirus 4.0.0 to 4.5.0

Install the McAfee MOVE AntiVirus product extension to access the installation wizard. When the McAfee MOVE AntiVirus 4.5.0 is installed, the older product version is removed.

Upgrading from McAfee MOVE AntiVirus 3.5.x and 3.6.x to 4.5.0

Install the McAfee MOVE AntiVirus product and migration extensions to access the installation wizard to migrate the policy settings from the previous versions McAfee MOVE AntiVirus. You can continue to use both product versions until you are ready to remove the older ones.

Migrating legacy product settings from 3.5.x and 3.6.x to 4.5.0

When you upgrade these products, you can migrate (or preserve) your custom product settings:

- McAfee MOVE AntiVirus (Multi-Platform)
- McAfee MOVE AntiVirus (Agentless)

Before migrating, review your previous settings to ensure that they are up to date, then consolidate, remove duplicates, and remove unused settings, policies, and client tasks.
Use the McAfee MOVE AntiVirus Migration Assistant to create new policies based on your previous product settings. You can migrate all your settings automatically, or select which policies to migrate, then configure new settings manually. The Migration Assistant also migrates client tasks and other settings like McAfee MOVE AntiVirus deployment data.

**Best practice:** Enable debug logging before starting the uninstallation or upgrade process of McAfee MOVE AntiVirus, so that it eases the process to troubleshoot any issues.

---

**Are you ready to install?**

When your environment meets the specified requirements, you are ready to begin installation.

<table>
<thead>
<tr>
<th>These components...</th>
<th>Meet these requirements</th>
</tr>
</thead>
</table>
| All systems where you want to install the product | • Hardware components meet or exceed minimum requirements.  
• Supported Windows operating system is installed. |
| Managed systems only | • Required agent or software is installed and communicating with the McAfee ePO server.  
• (Upgrade) Supported version of software is installed. |
| Management server | • Supported management platform is installed.  
• (Optional) You have preconfigured policy settings for product features.  
• (Upgrade) Supported version of extension is installed. |

---

**Downloading software extensions and packages**

You must download these software extensions and product packages before the components can be installed on McAfee ePO or deployed to virtual systems.

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

<table>
<thead>
<tr>
<th>Package name</th>
<th>Description</th>
</tr>
</thead>
</table>
| MOVE-AV_Ext_4.5.0_Licensed.Zip | This main extension includes these extensions:  
• McAfee MOVE AntiVirus Common — Extension for product installation and deployment.  
• McAfee MOVE AntiVirus — Extension for configuring and managing policies.  
• McAfee MOVE AntiVirus License — License extension; upgrades evaluation extension to a fully licensed extension. |
<p>| MOVE-AV-MP_SVM_4.5.0.Zip | Multi-Platform SVM package |
| MOVE-AV-MP_Client_4.5.0_WIN.Zip | Multi-Platform client deployment package |
| MOVE-AV-MP_SVM_Manager_OVF_4.5.0.Zip | Multi-Platform SVM Manager OVF package |
| MOVE-AV-MP_SVM_OVF_Export_Utility_4.5.0.Zip | Multi-Platform SVM OVF export utility |
| MOVE-AV-AL_SVM_OVF_4.5.0.Zip | Agentless SVM OVF package |</p>
<table>
<thead>
<tr>
<th>Package name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOVE-AV-AL_RestoreTool_4.5.0.Zip</td>
<td>Agentless restore tool</td>
</tr>
<tr>
<td>MOVE-AV_Migration_Ext_4.5.0.Zip</td>
<td>Migration Assistant utility</td>
</tr>
<tr>
<td>MOVE-AV_HELP_EXT_4.5.0.Zip</td>
<td>Product Help extension</td>
</tr>
<tr>
<td>MOVE-AV_Migration_Help_Ext_4.5.0.zip</td>
<td>Migration Assistant utility Help extension</td>
</tr>
<tr>
<td>MOVE-AV_DOCS_4.5.0.Zip</td>
<td>Product documentation package</td>
</tr>
<tr>
<td>Cloud_Workload_Discovery_Private_4.5.0.zip</td>
<td>Cloud Workload Discovery extension. Install this extension to discover the VM information and import it to the System Tree.</td>
</tr>
<tr>
<td>Common UI Core.zip</td>
<td>Common UI Core extension. This extension must be installed on McAfee ePO to install Cloud Workload Discovery.</td>
</tr>
</tbody>
</table>
Planning your installation
Downloading software extensions and packages
Multi-Platform installation and configuration

To set up your environment for Multi-Platform deployment, download and install the McAfee MOVE AntiVirus (Multi-Platform) components and deploy the McAfee MOVE AntiVirus client and SVM to target systems.

Contents
- SVM assignment made easy
- Install the product files on the management server
- Register a VMware vCenter account with McAfee ePO
- Set up the SVM Manager
- Deploy the McAfee MOVE AntiVirus SVM
- Deploying the McAfee MOVE AntiVirus client
- Assign the SVM using SVM Manager
- Add or edit an SVM Manager assignment rule using IP address
- Add or edit an SVM Manager assignment rule using McAfee ePO tag
- Install the McAfee MOVE AntiVirus client manually
- Exporting an SVM OVF template
- Specify the SVM template path in McAfee ePO
- Create an infrastructure group in McAfee ePO
- Enable and configure SVM autoscale settings
- Upgrade the standby SVMs
- Deploy in a XenDesktop or VMware View environment
- Integrating TIE and Advanced Threat Defense
- Preparing to upgrade McAfee MOVE AntiVirus (Multi-Platform)
- Uninstalling McAfee MOVE AntiVirus (Multi-Platform)

SVM assignment made easy

An SVM can generally be assigned to 200–400 endpoints, depending on the load of the endpoints. Assigning policies to the SVM manually is a time-consuming task. The SVM Manager creates assignments based on IP address and tags where a range of endpoints are automatically assigned to a group of SVMs.

SVM autoscaling

The virtual environments are dynamic with the number of instances depending on time of the day and day of the week.

Provisioning your SVMs to accommodate this variation manually is not a scalable solution. You might end up running more SVMs than you require to accommodate peak load. Or, you might end up running fewer SVMs, resulting in endpoints not being protected.
The security administrator can define the number of backup SVMs that are ready to protect your client systems. Calculate the number of ready SVMs required for the maximum number of clients that need protection at any time of the day. The standby SVMs are automatically deployed based on the backup SVM value. For example, if you specify the backup SVM as 4, two standby SVMs are deployed automatically. Therefore, the SVMs automatically scale up and down depending on the number of endpoints connected.

The SVM deployment automatically transitions between three modes:

- **Standby** — Standby SVMs are created and are ready to transition to the backup SVM mode. The standby SVMs are automatically deployed based on the backup SVM value. These SVMs are powered off.

- **Ready** — Backup SVMs that will be ready for protecting your client systems. You need to calculate the number of ready SVMs required for the maximum number of clients that would need protection at any time of the day. These SVMs are powered on, but not protecting the client systems.

- **Running** — These SVMs are currently protecting the client systems.

**Multi-Platform deployment process using McAfee MOVE AntiVirus autoscaling**

Using McAfee MOVE AntiVirus SVM autoscaling, the overall McAfee MOVE AntiVirus SVM deployment of the Multi-Platform option consists of the following tasks.

1. Install these extensions on McAfee ePO in this order:
   - Cloud Workload Discovery
   - McAfee MOVE AntiVirus

2. Register a VMware vCenter account with McAfee ePO.

3. Set up your SVM Manager and configure its details.
4 Configure assignment rules in SVM Manager Settings policy.

5 Configure the SVM Manager details in the Options policy under MOVE AntiVirus 4.5.0 product.

6 Deploy McAfee MOVE AntiVirus SVM.

7 Deploy the McAfee MOVE AntiVirus client.

8 Export the SVM template and specify the McAfee MOVE AntiVirus SVM path in McAfee ePO.

   This is required only when you are using autoscaling method.

9 Create or edit the infrastructure group on McAfee ePO.

10 Configure the SVM Autoscale Settings in SVM Manager Settings policy and assign it to SVM Manager.

The SVM ready pool is now created based on the number of backup SVMs specified. The backup SVMs that you specified in McAfee ePO are deployed automatically.

A McAfee MOVE AntiVirus SVM can generally be assigned to 200–400 endpoints, depending on the load of the endpoints. The security administrator can define number of backup SVMs that will be ready for protecting your client systems. Calculate the number of ready SVMs required for the maximum number of clients that would need protection at any time of the day.

The standby SVMs are automatically deployed based on the backup SVM value. For example, if you specify the back up SVM as 4, two standby SVMs are deployed automatically. Therefore, the SVMs automatically scale up and down depending on the number of endpoints connected.

When a McAfee MOVE AntiVirus client system starts communicating with the SVM Manager, one SVM from the ready pool moves to the running pool and protects the client system. The transition from the ready pool to running pool occurs when no running SVMs exist or all the running SVMs have reached their client limit. The ready pool is again replaced with one McAfee MOVE AntiVirus SVM from the standby pool.

One McAfee MOVE AntiVirus SVM is automatically deployed to the standby pool to retain the number of standby SVMs, which is specified in McAfee ePO.

Install the product files on the management server

The product extensions for Cloud Workload Discovery, McAfee MOVE AntiVirus, and VirusScan Enterprise for Linux must be installed on the McAfee ePO server before you can manage McAfee MOVE AntiVirus on your virtual machines.

Before you begin

The extension files are in an accessible location on the network.

Install the VirusScan Enterprise for Linux extension to manage the VirusScan Enterprise for Linux policy on the SVM Manager. VirusScan Enterprise for Linux is only licensed for the SVM Manager, not for other Linux systems in your 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.
You must install the product extensions in this order.

<table>
<thead>
<tr>
<th>Extension</th>
<th>Package name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Workload Discovery</td>
<td>Cloud_Workload_Discovery_Private_4.5.0.zip</td>
</tr>
<tr>
<td></td>
<td>Make sure that you installed Common UI Core extension before installing Cloud Workload Discovery.</td>
</tr>
<tr>
<td>McAfee MOVE AntiVirus extension</td>
<td>MOVE-AV_Ext_4.5.0_Licensed.Zip</td>
</tr>
<tr>
<td>VirusScan Enterprise for Linux extension</td>
<td>McAfeeVSEForLinux-2.0.3.-release-epo.zip</td>
</tr>
<tr>
<td>Product Help extension</td>
<td>MOVE-AV_HELP_EXT_4.5.0.Zip</td>
</tr>
<tr>
<td></td>
<td>If you are upgrading from 4.0.0 version, remove the 4.0.0 Help extension manually.</td>
</tr>
</tbody>
</table>

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

4 Review the extension details and click OK.

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

Before you begin
- Note that registering VMware vCenter account is not mandatory if you are not using autoscale SVM feature.
- You configured your VMware vCenter server that manages the ESXi servers, which host the guest VMs.
- You installed the Cloud Workload Discovery extension on the 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 | Configuration | Registered Cloud Accounts, then click Add Cloud Account to open the Add Cloud Account dialog box.

3 From the Choose Cloud Provider drop-down list on the Add Cloud Account dialog box, 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 Username** — (Required) User name of the available VMware vCenter account.
- **vCenter Password** — (Required) Password of the available VMware vCenter account.
- **Sync Interval (In Minutes)** — Specify the interval for running the next vCenter discovery (default value is 5 minutes).
- **Port** — 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 same organization as the VMware vCenter.

8 To verify that the VMs were imported, select **Menu** | **Systems** | **System Tree**.

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 the System Tree.
Set up the SVM Manager

You must set up and configure the SVM Manager before registering the SVM and assigning it to a group of clients.

**Before you begin**
- You must have administrator rights to perform this task.
- The SVM Manager OVF package is in an accessible location on the network.

**Task**

1. Open the VMware vSphere client, then click **File | Deploy OVF Template**.

2. Browse to and select the SVM Manager OVF package (MOVE-AV-MP_SVM_Manager_OVF_4.5.0) on your computer, then click **Next** to start the installation wizard.

3. Complete the steps in the wizard, accepting the default values or entering different values as needed.

4. When finished, select **Power On** to turn on the virtual machine and open a **Console** window to configure the SVM Manager appliance.

5. At the prompt, log on with these credentials:
   - User name: svaadmin
   - Password: svaadmin

6. Configure the VM appliance with these details:
   - Time zone
   - Network — DHCP or Static
     (Recommended: select a Static IP address for SVM Manager)
   - DNS servers
   - IP address and host name of the McAfee ePO server
   - McAfee ePO credentials
     Check for the correct format of the user name, for example: domain\user name.

7. Verify that these communication ports are open and reachable on the SVM Manager:
   - **8080** — For communication between SVM Manager and the client
   - **8081** — For communication between McAfee Agent and McAfee ePO
   - **8443** — For communication between SVM Manager and the SVM

   **Best practice:** By default, these ports are already opened through the firewall installed on the appliance. However, verify that the firewall settings in your environment are configured to allow communication on these ports.

8. Use this command to manually run the configuration script: `sudo /home/svaadmin/.sva-config`.

Now, the SVM Manager service can communicate with McAfee ePO through the McAfee Agent. You must now set the required policies in McAfee ePO.
Deploy the McAfee MOVE AntiVirus SVM

After you add the McAfee MOVE AntiVirus SVM package to McAfee ePO, you can deploy the SVM to your virtual machines.

Tasks

- **Check in the SVM package on page 23**
  Check in the McAfee MOVE AntiVirus (Multi-Platform) SVM and client packages to the Master Repository so that McAfee ePO can deploy them.

- **Create a product deployment client task on page 24**
  Deploying McAfee MOVE AntiVirus SVM from McAfee ePO requires two tasks. You must first create a deployment client task, then assign that task to virtual machines.

- **Assign a client task on page 24**
  After creating the product deployment client task, you must assign that task to virtual machines.

Check in the SVM package

Check in the McAfee MOVE AntiVirus (Multi-Platform) SVM and client packages to the Master Repository so that McAfee ePO can deploy them.

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 | Master Repository, then click Actions | Check In Package.
3. Select the package type, then browse to and select the package file MOVE-AV-MP_SVM_4.5.0.zip.
4. Click Next to open the Package Options page.
5. Confirm or configure these options:
   - **Package info** — Confirm this is the correct package.
   - **Branch** — Select the required branch.
     
     If your environment requires testing new packages before deploying them throughout the production environment, use the Evaluation branch to check in packages. Once you finish testing the packages, move them to the Current branch by clicking Menu | Software | Master Repository.
   - **Options** — Select one:
     - **Move the existing package to the Previous branch** — When selected, moves packages in the Master Repository from the Current branch to the Previous branch when a newer package of the same type is checked in. Available only when you select Current in Branch.
     - **Package signing** — Specifies if the package is signed by McAfee or is a third-party package.

6. Click Save to begin checking in the package, then wait while the package is checked in.

The SVM package appears in the Packages list on the Master Repository tab.
Create a product deployment client task
Deploying McAfee MOVE AntiVirus SVM from McAfee ePO requires two tasks. You must first create a deployment client task, then assign that task to virtual machines.

**Before you begin**
- You checked in the McAfee MOVE AntiVirus SVM package.
- The McAfee Agent and VirusScan Enterprise 8.8 are installed on the target virtual system.

**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. Select Product Deployment in the Client Task Types menu, then click Actions | New Task.
4. Select Product Deployment from the list, then click OK to open the Client Task Builder wizard.
5. Type a name for the task you are creating, and add any descriptive information in the Description field.
6. Make sure that Windows is the only target platform selected.
7. For Products and components:
   a. For SVM, select MOVE AV [Multi-Platform] SVM 4.5.0 from the drop-down list.
   b. Set the action to Install, set the language to Language Neutral, and set the branch to Current.
   c. Leave the Command line setting blank.
8. Review the task settings, then click Save.

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

Assign a client task
After creating the product deployment client task, you must assign that task to virtual machines.

**Before you begin**
- The McAfee Agent must already be deployed to target virtual systems.
- Check in the McAfee MOVE AntiVirus (Multi-Platform) 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 | Policy | Client Task Assignments, then click the Assigned Client Tasks tab.
3. Click Actions | New Client Task Assignment.
Configure these settings, then click Next.
- **Product** — McAfee Agent
- **Task Type** — Product Deployment
- **Task Name** — The name of the task you used when you created the client task

On the **Schedule** tab, specify the schedule for running the client task and then click Next.

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

The McAfee MOVE AntiVirus SVM is deployed to systems in the selected group in the System Tree.

---

**Deploying the McAfee MOVE AntiVirus client**

After the McAfee MOVE AntiVirus client package has been added to McAfee ePO, you can deploy the client to virtual machines, so that McAfee ePO can manage the McAfee MOVE AntiVirus configuration on the client systems.

**Check in the client package**

Check in the McAfee MOVE AntiVirus (Multi-Platform) client package to the Master Repository so that McAfee ePO can deploy it to your client virtual machines.

**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** | **Master Repository**, then click **Actions** | **Check In Package**.
3. Select the package type, then browse to and select the package file **MOVE-AV-MP_Client_4.5.0_WIN.zip**.
4. Click Next to open the **Package Options** page.
5. Confirm or configure these options:
   - **Package info** — Confirm this is the correct package.
   - **Branch** — Select the required branch.
     - If your environment requires testing new packages before deploying them throughout the production environment, use the **Evaluation** branch to check in packages. Once you finish testing the packages, move them to the **Current** branch by clicking **Menu** | **Software** | **Master Repository**.
   - **Options** — Select one:
     - **Move the existing package to the Previous branch** — Moves packages in the Master Repository from the Current branch to the Previous branch when a newer package of the same type is checked in. Available only when you select Current in Branch.
     - **Package signing** — Specifies if the package is signed by McAfee or is a third-party package.
6. Click Save to begin checking in the package, then wait while the package is checked in.

The client package appears in the **Packages** list on the **Master Repository** tab.
Create a product deployment client task
Deploying the McAfee MOVE AntiVirus client from McAfee ePO requires two tasks. You must first create a deployment client task, then assign that task to virtual machines.

Before you begin
Check in the McAfee MOVE AntiVirus (Multi-Platform) client 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 | Policy | Client Task Catalog.
3 Select Product Deployment in the Client Task Types menu, then click Actions | New Task.
4 Select Product Deployment from the list, then click OK to open the Client Task Builder wizard.
5 Type a name for the task you are creating, and add any descriptive information in the Description field.
6 Make sure that Windows is the only target platform selected.
7 For Products and components:
   a For client, select MOVE AV [Multi-Platform] Client 4.5.0 from the drop-down list.
   b Set the action to Install, set the language to Language Neutral, and set the branch to Current.
   c Leave the Command line setting blank.
8 Review the task settings, then click Save.
The task is added to the list of client tasks for the selected client task type.

Assign a client task
After creating the product deployment client task, you must assign that task to virtual machines.

Before you begin
• The McAfee Agent must already be deployed to target virtual systems.
• Check in the McAfee MOVE AntiVirus (Multi-Platform) client 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 | Policy | Client Task Assignments, then click the Assigned Client Tasks tab.
3 Click Actions | New Client Task Assignment.
4 Configure these settings, then click Next.
   • Product — McAfee Agent
   • Task Type — Product Deployment
   • Task Name — The name of the task you used when you created the client task
5 On the Schedule tab, specify the schedule for running the client task and then click Next.
6 Examine the settings on the Summary tab, then click Save to assign the task.
   The McAfee MOVE AntiVirus client is deployed to every system in the selected group in the System Tree.
7 Confirm that the McAfee MOVE AntiVirus client is successfully installed:
   a Log on to the McAfee MOVE AntiVirus client system as an administrator.
   b Open the McAfee MOVE AntiVirus client command prompt and enter this command: mvadm status
   The command line returns protection status details if the client is successfully installed.

Assign the SVM using SVM Manager
Create and assign a policy, so that the SVM Manager specifies which SVM a group of virtual machines uses. You can also manually specify the SVM which a group of virtual machines should use.

Before you begin
• You installed the McAfee MOVE AntiVirus extension on the McAfee ePO server.
• You checked in the McAfee MOVE AntiVirus (Multi-Platform) software packages (MOVE-AV-MP_Client_Pkg_4.5.0.zip and MOVE-AV-MP_SVM_Pkg_4.5.0.zip) to the McAfee ePO server.
• You deployed the McAfee MOVE AntiVirus SVM package to the SVM host.
• You deployed the McAfee MOVE AntiVirus client package to the client systems.
• You already set up the SVM Manager.
• You configured your McAfee ePO details in the General page under Automation | MOVE AntiVirus Deployment | Configuration.

Task
For details about product features, usage, and best practices, click ? or Help.
1 Log on to McAfee ePO as an administrator.
2 Click Menu | Policy | Policy Catalog, select MOVE AntiVirus 4.5.0 from the Product drop-down list, then select Options from the Category drop-down list.
3 Click New Policy or click the name of an existing policy to edit it.
4 Type a name for the new policy (for example, SVM Assignment Policy), then click OK.
Under SVM Assignment on the policy settings page, configure options as needed, then click Save to commit your changes.

1. Select Assign SVM using SVM Manager to make sure that the given SVM is assigned to a set of virtual machines.
   - Enter the SVM Manager IP address, host name, or FQDN (domain name), and the SVM Manager Port. Default is 8080.

2. Select Assign SVM manually and configure the SVM details:
   - Enter IP Address, host name, or FQDN of SVM-1, and the SVM Port. Default is 9053.
   - McAfee MOVE AntiVirus Multi-Platform supports Fully Qualified DNS names, which allow for DNS Round-Robin Load Balancing. This type of load balancing distributes client requests across multiple servers.
   - Enter IP Address, host name, or FQDN of SVM-2, and the SVM Port. Default is 9053.
   - Best practice: Use two different addresses when setting up the primary and secondary servers. Using the same address for both servers results in delayed coverage, which occurs when recovering from loss of connection to the primary server.

Now, the clients request the SVM Manager when they require an SVM. SVM Manager serves them an SVM based on the filtering rules created in the SVM Manager Settings policy.

Add or edit an SVM Manager assignment rule using IP address

Using their IP address range, assign a set of endpoints to a selected SVM or a number of SVMs, so that those clients are protected by the SVM Manager assignment rule.

Before you begin

- You installed the McAfee MOVE AntiVirus extension on the McAfee ePO server.
- You checked in the McAfee MOVE AntiVirus (Multi-Platform) software packages (MOVE-AV-MP_Client_Pkg_4.5.0.zip and MOVE-AV-MP_SVM_Pkg_4.5.0.zip) to the McAfee ePO server.
- You deployed the McAfee MOVE AntiVirus SVM package to the SVM host.
- You deployed the McAfee MOVE AntiVirus client package to the client systems.
- You set up the SVM Manager.

Things to remember:

- You can define different rules to overwrite the autoscale settings. After defining the generic SVM autoscale requirements in SVM Autoscale Settings, you can also define rule-based autoscale settings.
- Rule-based autoscale settings can overwrite the regular SVM Autoscale Settings.
- You can separate IP addresses or ranges with a comma (,) or a new line.

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 | Policy Catalog, select MOVE AntiVirus 4.5.0 from the Product drop-down list, then select SVM Manager Settings from the Category drop-down list.
3 Click New Policy or click the name of an existing policy to edit it.

4 Type a name for the new policy (for example, MOVE AV SVM Manager Policy), then click OK.

5 On the Assignment Rules tab on the Policy Settings page, click Add to open the Add/Edit SVM IP Assignment Rule dialog box and configure these settings as needed.

<table>
<thead>
<tr>
<th>For this option...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule name</td>
<td>Type a unique user-friendly name that can help you identify the rule.</td>
</tr>
<tr>
<td>Client IP Addresses</td>
<td>Type the IP address or a range of IP addresses of the endpoints, which must be assigned to the SVM.</td>
</tr>
<tr>
<td>SVM IP Addresses</td>
<td>Type the IP address of the SVM, which must be assigned to the client.</td>
</tr>
<tr>
<td>Select and add to infrastructure groups</td>
<td>Select the Default Group or an infrastructure group you have created using the Menu</td>
</tr>
<tr>
<td>Customize SVM Settings</td>
<td>This is the SVM assignment rule specific to autoscale settings. Here, each rule can be assigned for individual SVM deployment settings. You can define different rules which overwrite the common autoscale settings defined under SVM Autoscale Settings.</td>
</tr>
<tr>
<td></td>
<td>• Number of backup SVMs — Type the number of ready SVMs required to protect your client systems.</td>
</tr>
<tr>
<td></td>
<td>Calculate the number of ready SVMs required for the maximum number of clients that need protection at any time of the day. The standby SVMs are automatically deployed based on the backup SVM value. For example, if you specify the backup SVM as 4, two standby SVMs are deployed automatically. Therefore, the McAfee MOVE AntiVirus SVMs automatically scale up and down depending on the number of endpoints connected.</td>
</tr>
<tr>
<td>Alarms</td>
<td>Threshold for number of connected endpoints (per SVM) — Specify the SVM capacity threshold level. A warning appears when the number of connected endpoints is more than this level.</td>
</tr>
</tbody>
</table>

The Assign SVM if no rule is defined for the above client option is used to assign the SVM to endpoints, which are not defined in any of the rules. By default, this option is enabled.

6 Click OK to save your changes.

**Add or edit an SVM Manager assignment rule using McAfee ePO tag**

Assign a set of endpoints to a selected SVM using their tag group, so that they are protected by the SVM Manager assignment rule.

**Before you begin**
- You installed the McAfee MOVE AntiVirus extension on the McAfee ePO server.
- You checked in the McAfee MOVE AntiVirus (Multi-Platform) software packages (MOVE-AV-MP_Client_Pkg_4.5.0.zip and MOVE-AV-MP_SVM_Pkg_4.5.0.zip) to the McAfee ePO server.
- You deployed the McAfee MOVE AntiVirus SVM package to the SVM host.
- You deployed the McAfee MOVE AntiVirus client package to the client systems.
You set up the SVM Manager.

You create a tag Default Rule in the tag catalog of McAfee ePO. This tag is automatically applied to McAfee MOVE AntiVirus SVMs when you don't configure any tag rule.

Things to remember:

- You can define different rules to overwrite the autoscale settings. After defining the generic SVM autoscale requirements in SVM Autoscale Settings, you can also define rule-based autoscale settings.
- Rule-based autoscale settings overwrite the regular SVM Autoscale Settings.
- Separate tag names with a comma (,).
- Tag-based assignment rules takes priority over IP address-based assignment rules.

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 | Policy Catalog, select MOVE AntiVirus 4.5.0 from the Product drop-down list, then select SVM Manager Settings from the Category drop-down list.

3 Click New Policy or click the name of an existing policy to edit it.

4 Type a name for the new policy (for example, MOVE AV SVM Manager Policy), then click OK.

5 In the Tag Assignment Rules tab on the Policy Settings page, click Add to open the Add/Edit SVM Tag Assignment Rule dialog box and configure these settings as needed.

<table>
<thead>
<tr>
<th>For this option...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule name</td>
<td>Type a unique user-friendly name that can help you identify the rule.</td>
</tr>
<tr>
<td>Select and add to client tags</td>
<td>Select the tag names of the endpoints, which must be assigned to the SVM.</td>
</tr>
<tr>
<td>Select and add to SVM Tags</td>
<td>Select the tag name of the SVM, which must be assigned to the client.</td>
</tr>
<tr>
<td>Select and add to infrastructure groups</td>
<td>Select the Default Group or an infrastructure group you have created using the Menu</td>
</tr>
</tbody>
</table>
Install the McAfee MOVE AntiVirus client manually

You can install the client manually without deploying it from McAfee ePO.

**Before you begin**
- Download the McAfee MOVE AntiVirus installer and store it in a location accessible from the system where it is installed.
- The McAfee Agent is installed on the target system.

This procedure is used only when you don't want to use McAfee ePO to deploy the client to the target system.

**Task**
1. From the McAfee MOVE AntiVirus client package, extract the appropriate client installer based on your Windows operating system.
   - **64-bit** — setup-win-amd64.exe
   - **32-bit** — setup-win-x86.exe
2. Run the installer, then click Next on the Welcome screen.
3. On the License Agreement screen, accept the EULA, then click Next.
4. On the Customer information screen, enter a user name and organization, then click Next.
5. On the Destination folder screen, choose the default location or specify a different location, then click Next.
6. On the Ready to install the program screen, click Install.
7. Click Finish to complete the installation.
To configure the SVM assignment manually, open the McAfee MOVE AntiVirus client command prompt: click Start | Programs | McAfee | MOVE AV client Command Prompt, and run these commands.

- mvadm status
- mvadm config set serveraddress1=<Address of svm 1>
- mvadm config set serveraddress2=<Address of svm 2>

The SVM address can be entered in FQDN or IPv4 format.

- mvadm enable

The McAfee MOVE AntiVirus client is now installed and running on the target system.

---

**Exporting an SVM OVF template**

An SVM OVF template is a master image of a virtual machine that can be used to create and deploy many SVMs.

When you export the SVM, you create a copy of the entire virtual machine, including its settings, installed software, and other configuration details. Exporting the SVM saves time when you are deploying many SVMs. You can create and configure a single SVM, then deploy it multiple times, rather than creating and configuring each SVM individually.

When deploy an SVM from OVF template, the resulting SVM is independent of the original SVM or template. Changes to the original SVM or template are not reflected in the deployed SVM, and changes to the deployed SVM are not reflected in the original SVM or template.

Exporting an SVM OVF template is required only when you are using autoscaling method.

**Export the SVM OVF template using the export utility**

Using the export utility, you can create a template to make a master image of an SVM, from which you can deploy many SVMs.

**Before you begin**

- Windows PowerShell 2.0 is installed to run the script.
- The SVM is managed by McAfee ePO.
- VMware Tools are installed on the SVM: C:\Program Files\VMware\VMware Tools \vmtoolsd.exe.
- The SVM virtual machine should not have any snapshot.
- Make sure that the SVM is not part of any domain, so that the exported SVM template is a generic one and can be deployed on any domain.
- Make sure that you do not configure the SVM Manager IP details under SVM Manager Assignment in McAfee ePO until you create and export the SVM template.

**Task**

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

1. Create an SVM. For details, see Deploy the McAfee MOVE AntiVirus SVM.

Make sure that you use the static IP for the SVM from which you create the OVF template.
2 Duplicate the McAfee Default General policy from McAfee Agent and disable the Enable self protection option and apply this policy to the SVM virtual machine from which you take the template.

3 Copy and extract the MOVE-AV-MP_SVM_OVF_Export_Utility_4.5.0.Zip file to any Windows system.
   These two files are present in the extracted MOVE-AV-MP_SVM_OVF_Export_Utility_4.5.0.Zip folder:
   - config.ini
   - svm-export.exe

   ! Do not modify the script files present in the Autoconfig_scripts folder.

4 Using any word editor, open the config.ini file and configure these settings:
   • vCenter IP
   • vCenter password
   • SVM VM name
   • User name and password of SVM, which is created in step 1. This user account must have the local administrator privileges.
   • The directory location where the exported SVM OVF template is saved.

5 Double-click to run the svm-export.exe file.
   A command-line window appears with the status of the configuration and closes when the export is complete. The SVM OVF template files (**.ovf and **.vmdk) are created in the specified location.

6 Copy the OVF template files to the system where your McAfee ePO server is installed and use it for SVM autoscaling, as required.

**Export the SVM OVF template manually**
Export an SVM OVF template from master image of an SVM, from which you can deploy many SVMs.

**Before you begin**
- Windows PowerShell 2.0 is installed to run the script.
- The SVM is managed by McAfee ePO.
- VMware Tools are installed on the SVM: C:\Program Files\VMware\VMware Tools\vmtoolsd.exe.
- The SVM virtual machine should not have any snapshot.
- Make sure that the SVM is not part of any domain, so that the exported SVM template is a generic one and can be deployed on any domain.
- Make sure that you do not configure the SVM Manager IP details under SVM Manager Assignment in McAfee ePO until you create and export the SVM template.
**Task**

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

1. Create an SVM. For details, see Deploy the McAfee MOVE AntiVirus SVM.
   - Make sure that you use the static IP for the SVM from which you create the OVF template.

2. Create a folder under C drive C:\Autoconfig_scripts.

3. Extract the MOVE-AV-MP_SVM_OVF_Export_Utility_4.5.0.Zip and copy these files from the extracted Autoconfig_script folder to C:\Autoconfig_scripts.
   - CreateSVMAutoConfigScheduledTask.ps1
   - svm_auto_config.ps1
   - svm_auto_configure.xml

   a. Select Start | All Programs | Accessories, select and right-click Windows PowerShell, then select Run As Administrator.

5. Set the execution policy of PowerShell to remote signed.
   - Set-ExecutionPolicy RemoteSigned

6. Change directory to C:\Autoconfig_scripts and execute the script CreateSVMAutoConfigScheduledTask.ps1.

7. Specify the full path of the script file svm_auto_config.ps1, when prompted. This script creates a scheduled task, which is used to configure the auto-deployed SVM during the first turn on.
   - Make sure that you do not run the script svm_auto_config.ps1 manually. Otherwise, the script does not run while deploying the SVM template.

8. Open Task Scheduler and verify that the task svm_auto_configure is present.

9. Double-click Task and select Trigger, then click Edit.

10. From Begin the task drop-down list, select At startup, so that the task starts during the system start-up.

11. Ensure that the Activate option is not selected and the Enabled option is selected.

12. Duplicate the McAfee Default General policy from McAfee Agent and disable the Enable self protection option and apply this policy to the SVM virtual machine from which you take the template.
13 Remove the McAfee Agent GUID.
   a Click Start | Run and type regedit, then click OK.
   b Remove the GUID:
      32-bit — [HKEY_LOCAL_MACHINE\SOFTWARE\Network Associates\ePolicy Orchestrator \Agent\AgentGUID]
      64-bit — [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Network Associates\ePolicy Orchestrator\Agent\AgentGUID]

14 Turn off the VM.

   If you are enabling TIE and Advanced Threat Defense integration, make sure that you have installed the DXL client before turning off the VM. For details, see the product documentation for TIE and Advanced Threat Defense.

Tasks

- **Enable vApp functionality for the SVM on page 35**
  Enable the vApp functionality to set and configure it for OVF parameters.

- **Edit OVF settings on page 35**
  Customize and configure your OVF requirement by editing OVF settings.

- **Edit Advanced vApp options on page 36**
  To add support for multiple IP Allocation schemes and IP protocols, edit advanced options like custom properties and IP allocation.

**Enable vApp functionality for the SVM**

Enable the vApp functionality to set and configure it for OVF parameters. Enabling these options allows the SVM to receive OVF Environment properties at boot time. The OVF environment can contain values for custom properties including network configuration and IP addresses.

**Task**

1 Right-click the turned off SVM and select Edit Settings.
2 From the Virtual Machine Properties dialog box, click the Options tab.
3 Select vApp Options.
4 Select Enable to activate vApps functionality and to show the vApps options.
5 Click OK.

**Edit OVF settings**

Customize and configure your OVF requirement by editing OVF settings.

**Task**

1 From the Virtual Machine Properties dialog box, click the Options tab.
2 From OVF Settings, select VMware Tools under OVF Environment Transport.
3 Click OK.
Edit Advanced vApp options
To add support for multiple IP Allocation schemes and IP protocols, edit advanced options like custom properties and IP allocation.

Before you begin
vApp options must be enabled.

Task
1. From the Virtual Machine Properties dialog box, click the Options tab.
2. Select Advanced.
3. Click Properties to add or edit the custom vApp properties.
   a. Click New and add each of these properties:
      - Click OK.
4. Click IP Allocation to edit the supported IP allocation schemes of this vApp.
5. Select DHCP and OVF Environment, so that the vApp can obtain its network configuration through the OVF environment or a DHCP server.
6. Click OK when complete.

Export the OVF template manually
The OVF package captures the state of a virtual machine or vApp into a self-contained package. The disk files are stored in a compressed, sparse file format.

Before you begin
- You have the required vApp.Export privileges.

Task
1. Rename the SVM to a preferred name.
2. Right-click the virtual machine (SVM) and click Edit Settings.
3 Unmount the CD/DVD drive from the SVM.

4 Select the SVM VM and select File | Export | Export OVF Template to specify the details required to store the OVF file.

5 In the Export OVF Template dialog box, type the name of the template.

6 Type the directory location where the exported SVM template is saved, or click "..." to browse to the location. The C:\ drive is the default location where the template is stored.

7 Copy this OVF on the McAfee ePO server and use this as a template for automatic staging and deployment of the SVM, as required.

Specify the SVM template path in McAfee ePO

You must specify the path of the McAfee MOVE AntiVirus SVM template in McAfee ePO, so that you can deploy it to the hypervisor.

Before you begin
- You installed the McAfee MOVE AntiVirus 4.5.0 extension on the McAfee ePO server.
- The exported SVM OVF is copied to the system where your McAfee ePO server is installed.

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 AntiVirus Deployment.

3 On the Configuration tab, click SVM Repository to open the SVM Repository 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 McAfee MOVE AntiVirus SVM package checked in to McAfee ePO.</td>
</tr>
<tr>
<td>SVM Version</td>
<td>Version of the McAfee MOVE AntiVirus SVM package checked in to McAfee ePO.</td>
</tr>
<tr>
<td>SVM Use Count</td>
<td>Specifies the number of SVMs, which are present in the infrastructure.</td>
</tr>
<tr>
<td>Action</td>
<td>Delete — To remove an existing McAfee MOVE AntiVirus SVM when it is not deployed to any hypervisor. It is possible to delete the SVM only when the SVM Use Count is zero.</td>
</tr>
</tbody>
</table>

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

5 Select Configure OVF location and specify the SVM Location and Version details, then click OK.

You can specify any user-friendly name and description for the McAfee MOVE AntiVirus SVM details.
Create an infrastructure group in McAfee ePO

After registering your vCenter account, your default group is added to the MOVE AntiVirus Deployment wizard when you access the Infrastructure Details option under Autoscale. You can edit the details of the default infrastructure group, as needed.

Before you begin
You registered your VMware vCenter account with McAfee ePO.

You can deploy the SVM to any infrastructure group by configuring the SVM Manager and autoscale settings in McAfee ePO. By default, an infrastructure group is added to the MOVE AntiVirus Deployment wizard when you access the Infrastructure Details option under Autoscale.

Using the Infrastructure Details option, you can create a hypervisor-based or cluster-based infrastructure group. You can then customize and select the infrastructure group for SVM deployment.

You can customize the SVM Manager Settings policy for creating and assigning IP-based or tag-based assignment rules for SVM deployment. Here, you can select and include individual infrastructure groups for 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 AntiVirus Deployment.

3 On the Configuration tab, click Infrastructure Details to open the Infrastructure Details page with the default infrastructure group details.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group name</td>
<td>Specifies the name of the infrastructure group.</td>
</tr>
<tr>
<td>Cloud Account Name</td>
<td>Specifies the account name of the registered vCenter account.</td>
</tr>
<tr>
<td>ESXi/Cluster</td>
<td>Specifies the IP address or name of the hypervisor or the cluster selected as part of the infrastructure group.</td>
</tr>
<tr>
<td>IP Pool Name</td>
<td>Specifies the name of the IP Pool used in the infrastructure group.</td>
</tr>
<tr>
<td>Provisioning</td>
<td>Specifies the provisioning type as Thin or Thick.</td>
</tr>
<tr>
<td>Network Name</td>
<td>Specifies the name of the management network used by the group.</td>
</tr>
<tr>
<td>Datastore Name</td>
<td>Specifies the name of the datastore used by the infrastructure group.</td>
</tr>
</tbody>
</table>
| Action          | • Edit — Click to edit the infrastructure group properties.  
|                 | • Delete — Click to delete any of the unused infrastructure group. |
4 Click Actions | Create and configure these properties for the custom infrastructure group details. It is not mandatory to configure the custom group details when the default group is available.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Type a name for the infrastructure group.</td>
</tr>
<tr>
<td>Infrastructure Type</td>
<td>Select whether you want to create a group based your hypervisor or cluster.</td>
</tr>
<tr>
<td>Select Host (Cluster)</td>
<td>Select the IP address of your host.</td>
</tr>
<tr>
<td>Hostname Prefix</td>
<td>Type a unique prefix that is added to the host name of the hypervisor or cluster. The prefix can include characters a–z, A–Z, 0–9, and [-], without space.</td>
</tr>
<tr>
<td>IP Pool</td>
<td>Configure the IP Pool as Static or DHCP.</td>
</tr>
<tr>
<td>AD Server</td>
<td>Select the registered Active Directory server, so that the deployed SVM is automatically added to the selected domain.</td>
</tr>
<tr>
<td>Provisioning Type</td>
<td>Select the provisioning type as Thin or Thick.</td>
</tr>
<tr>
<td>Network Name</td>
<td>Select the required management network.</td>
</tr>
<tr>
<td>Datastore Name</td>
<td>Select the configured datastore for the infrastructure.</td>
</tr>
</tbody>
</table>

5 Click Save to store the infrastructure details.

Enable and configure SVM autoscale settings

Create and assign a policy that specifies which SVM an infrastructure group uses. You can define the McAfee MOVE AntiVirus SVM autoscale settings, so that the McAfee MOVE AntiVirus SVM deployment
starts automatically depending on the number of clients connecting to the McAfee MOVE AntiVirus SVM for protection.

**Before you begin**
- You installed the McAfee MOVE AntiVirus extension on the McAfee ePO server.
- You checked in the McAfee MOVE AntiVirus (Multi-Platform) software packages (MOVE-AV-MP_Client_Pkg_4.5.0.zip and MOVE-AV-MP_SVM_Pkg_4.5.0.zip) to the McAfee ePO server.
- You deployed the McAfee MOVE AntiVirus client package to the client systems.
- You set up the SVM Manager.
- You configured your McAfee ePO details on the General page under Automation | MOVE AntiVirus Deployment | Configuration.

You can track the status of the SVM deployment on the Job Status Details page on the 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 | Policy | Policy Catalog, select MOVE AntiVirus 4.5.0 from the Product drop-down list, then select SVM Manager Settings from the Category drop-down list.

3 Click New Policy or click the name of an existing policy to edit it.

4 Type a name for the new policy (for example, MOVE AV Server Policy), then click OK.

5 Under SVM Manager Configuration, configure these settings as needed, then click Save to commit your changes.

<table>
<thead>
<tr>
<th>For this option...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVM Port</td>
<td>Specify the port for the SVM to communicate to SVM Manager. Default is 8443.</td>
</tr>
<tr>
<td>Client Port</td>
<td>Specify the port for the client system to communicate to SVM Manager. Default is 8080.</td>
</tr>
</tbody>
</table>

6 From SVM Autoscale Settings, select Enable auto scaling of SVMs and configure these options:

- **Number of backup SVMs** — Type the number of ready SVMs required to protect your client systems. Calculate the number of ready SVMs required for the maximum number of clients that need protection at any time of the day. The standby SVMs are automatically deployed based on the backup SVM value. For example, if you specify the backup SVM as 4, two standby SVMs are deployed automatically.

The ready SVMs are not protecting your clients, but running SVMs are protecting your clients. The backup SVMs are the ready SVMs, which enable faster protection for new client systems that might be added during peak hours or a cloud burst situation.
- **Threshold for number of connected endpoints (per SVM)** — Specify the SVM capacity threshold level. A warning appears when the number of connected endpoints is more than this level.

> When the SVM reaches minimum threshold for the number of connected endpoints, the running SVMs move to the standby SVM pool.

7. Click **Show Advanced** and configure the **Assignment Rules** options as needed, then click **Save** to commit your changes.

### Autoscale SVM details

When you define the McAfee MOVE AntiVirus SVM autoscale settings, the SVM deployment starts automatically depending on the number of clients connecting to the McAfee MOVE AntiVirus SVM for protection.

You can view the SVM deployment mode, its status, and the purging details on the **SVM Details: Autoscale SVM Details** page.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preset</td>
<td>You can select an option to filter and display the deployed SVM modes:</td>
</tr>
<tr>
<td></td>
<td>• All — Filters and displays all the SVMs deployed using the autoscale deployment.</td>
</tr>
<tr>
<td></td>
<td>• Standby — Filters and displays all the standby SVMs.</td>
</tr>
<tr>
<td></td>
<td>• Ready — Filters and displays all the ready SVMs.</td>
</tr>
<tr>
<td></td>
<td>• Running — Filters and displays all the running SVMs.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Host name of the deployed McAfee MOVE AntiVirus SVM.</td>
</tr>
<tr>
<td>Assignment Rule</td>
<td>Specifies the name of assignment rule, which assigns a set of endpoints to a selected SVM or a number of SVMs, so that those clients are protected by the SVM Manager assignment rule.</td>
</tr>
<tr>
<td>Infrastructure Group</td>
<td>Specifies whether it is a hypervisor-based or cluster-based infrastructure group.</td>
</tr>
<tr>
<td>Version</td>
<td>Specifies the version of the SVM.</td>
</tr>
<tr>
<td>SVM Mode</td>
<td>Specifies the mode of the deployed SVM:</td>
</tr>
<tr>
<td></td>
<td>• Standby — Standby SVMs are created and are ready to transition to the backup SVM mode. The standby SVMs are automatically deployed based on the backup SVM value. These SVMs are turned off.</td>
</tr>
<tr>
<td></td>
<td>• Ready — Backup SVMs that will be ready for protecting your client systems. You need to calculate the number of ready SVMs required for the maximum number of clients that would need protection at any time of the day. These SVMs are powered on, but not protecting the client systems.</td>
</tr>
<tr>
<td></td>
<td>• Running — These SVMs are currently protecting the client systems.</td>
</tr>
<tr>
<td>SVM Status</td>
<td>Specifies whether the SVMs are running.</td>
</tr>
<tr>
<td>Action</td>
<td>• Delete — Deletes the selected SVMs.</td>
</tr>
<tr>
<td></td>
<td>• Upgrade Standby SVMs — Removes the existing standby SVMs and deploys the new standby SVMs with the latest OVF template.</td>
</tr>
</tbody>
</table>
Upgrade the standby SVMs

When the latest OVF template package is configured in McAfee ePO, it is possible to deploy it from McAfee ePO to all running and ready SVMs. But, the same is not possible on standby SVMs as they are turned off and not managed by McAfee ePO. The ready and running SVMs are turned on.

**Before you begin**
You have created your latest OVF template using the steps in *Creating and Exporting the SVM template.*

When you define the McAfee MOVE AntiVirus SVM autoscale settings, the McAfee MOVE AntiVirus SVM deployment starts automatically depending on the number of clients connecting to the McAfee MOVE AntiVirus SVM for protection. You can view all SVM deployment mode, its status, and the purging details on the SVM Details: Autoscale SVM Details page.

**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 AntiVirus Deployment.
3. On the Configuration tab, click SVM Details to open the SVM Details: Autoscale SVM Details page with the autoscale SVM deployment details.
4. Select the standby SVMs and click Actions | Upgrade Standby SVMs.

This action removes the existing standby SVMs and deploys the new standby SVMs with the latest OVF template.

Deploy in a XenDesktop or VMware View environment

When operating in a XenDesktop or VMware View environment, follow these steps to avoid creating duplicate systems in McAfee ePO.

**Before you begin**
- The McAfee Agent is installed on the master image.
- The McAfee MOVE AntiVirus client is in the Master Repository.

**Task**
1. Deploy the McAfee MOVE AntiVirus client to the master image, then verify that it was applied successfully.
2. Configure and apply McAfee MOVE AntiVirus policies to the master image, then verify that they were applied successfully.

**Best practice:** Build up the cache by running the ODS on the master image to get the faster response from the scanning when you clone the virtual machines.
3 In the master image, delete the registry key AgentGUID from the location determined by your Windows operating system.
   - **32-bit** — HKEY_LOCAL_MACHINE\SOFTWARE\Network Associates\ePolicy Orchestrator\Agent (32-bit)
   - **64-bit** — HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Network Associates\ePolicy Orchestrator\Agent (64-bit)

4 Shut down the master image and clone all virtual machines from that master image. When cloned images are turned on, new agent GUID values are automatically generated.

---

### Integrating TIE and Advanced Threat Defense

McAfee® Threat Intelligence Exchange (TIE) provides context-aware adaptive security for your virtual environment. It quickly analyzes files and content from the SVM in your environment and makes informed security decisions. These decisions are based on a file's security reputation and your own criteria set in the **Shared Cloud Solutions** policy of McAfee MOVE AntiVirus.

The Multi-Platform deployment, with TIE and Advanced Threat Defense integration, becomes a multi-layered solution that involves various techniques to scan and detect the malware. It includes:

- Pattern matching
- Global reputation
- Program emulation
- Static analysis
- Dynamic analysis

All these layers are seamlessly integrated and provide a single point of control for easy configuration and management.

#### How Threat Intelligence Exchange works

Threat Intelligence Exchange uses the Data Exchange Layer framework to share file and threat information instantly across the entire network.

In the past, you sent an unknown file or certificate to McAfee for analysis, then updated the file information throughout your network later. Threat Intelligence Exchange enables file reputation to be controlled at a local level, your virtual environment. You decide which files can run and which are blocked, and the Data Exchange Layer shares the information immediately throughout your environment.

#### TIE and Advanced Threat Defense integration process

The overall TIE and Advanced Threat Defense integration process of the Multi-Platform consists of the following tasks.

1. Install the Threat Intelligence Exchange server appliance.
2. Deploy the Data Exchange Layer client to McAfee MOVE AntiVirus SVM.
3. Verify the Threat Intelligence Exchange server installation.
4. Create a new registered server in McAfee ePO.
5. Enable TIE and Advanced Threat Defense protection for McAfee MOVE AntiVirus.
6 Verify the TIE server integration.
7 Verify the Advanced Threat Defense integration.

**Threat Intelligence Exchange components**
Threat Intelligence Exchange includes these components.

- A server that stores information about file and certificate reputations, then passes that information to other systems.
- Data Exchange Layer brokers that allow bidirectional communication between managed systems on a network.

These components are installed as McAfee ePO extensions and add several new features and reports:

- McAfee TIE server extension
- McAfee DXL broker management
- McAfee DXL client for McAfee ePO
- McAfee DXL client management

**How Advanced Threat Defense works**
If Advanced Threat Defense is present, the following process occurs.

1. When a file reputation is looked up in TIE and TIE determines that it is an Advanced Threat Defense candidate, then the file is submitted to Advanced Threat Defense for further analysis through TIE from SVM based on the settings in Shared Cloud Solutions policy under McAfee MOVE AntiVirus.

2. Advanced Threat Defense analyses the file and sends file reputation results to the TIE server using the Data Exchange Layer. The TIE server also updates the database and sends the updated reputation information to the SVM.

The Advanced Threat Defense solution primarily consists of the Advanced Threat Defense Appliance and the pre-installed software. The Advanced Threat Defense Appliance is available in two models. The standard model is the ATD-3000. The high-end model is the ATD-6000.

For installing and setting-up Advanced Threat Defense, see the installation guide for your version of Advanced Threat Defense.

**Advanced Threat Defense components**
Advanced Threat Defense integrates its native capabilities with McAfee MOVE AntiVirus to provide you a multilayered defense mechanism against malware.

These are the features and components of Advanced Threat Defense that integrate with McAfee MOVE AntiVirus for better malware detection:

- Its preliminary detection mechanism consists of a local blacklist to quickly detect known malware.
- It integrates with McAfee GTI for cloud-lookups to detect malware that has already been identified by organizations throughout the globe.
- It has the McAfee Gateway Anti-Malware Engine embedded within it for emulation capability.
- It has the McAfee Anti-Malware Engine embedded within it for signature-based detection.
- It dynamically analyzes the file by executing it in a virtual sandbox environment. Based on how the file behaves, Advanced Threat Defense determines its malicious nature.
Scenarios for using Threat Intelligence Exchange

- **Immediately block a file** — Threat Intelligence Exchange alerts the network administrator of an unknown file in the environment. Instead of sending the file information to McAfee for analysis, McAfee MOVE AntiVirus blocks the file immediately. The administrator can then use Threat Intelligence Exchange to learn whether the file is a threat and how many systems ran the file.

- **Allow a custom file to run** — A company routinely uses a file whose default reputation is suspicious or malicious, for example a custom file created for the company. This file can override the reputation of a file on TIE server so that it is allowed to run in the environment.

- **Import known reputations** — A company has several files that are trusted and used regularly, and other files that are not allowed. Because the reputations are already known and set, the administrator can import a list of files and their reputations directly into the Threat Intelligence Exchange database. Those reputations are used immediately with no further action needed.

- **See additional information about a file** — Threat Intelligence Exchange notifies the network administrator of an unknown file. The administrator can see several details about the file, such as the file's parent process, company, hash information, and the systems that ran the file. The administrator can also see more detailed information about the file with VirusTotal, a free online service for scanning viruses, malware, and URLs.

How a reputation is determined

File and certificate reputation is determined when a file attempts to run on a managed system. These steps occur in determining a file or certificate's reputation.

1. A user or system attempts to run a file.

2. McAfee MOVE AntiVirus compares and inspects the file with local cache and can't determine its validity and reputation.

3. The client looks for the reputation in global cache in the SVM and can't find the reputation and then sends the file hashes to the SVM for TIE lookup based on the **Shared Cloud Solutions** policy assigned to the system.

4. The SVM checks the reputation cache for the file hash. If the file hash is found, the SVM gets the reputation data from the SVM cache and sends the reputation to the client and action is taken.

5. If the file hash is not found in the SVM cache and TIE server does not have the reputation:
   - (Advanced Threat Defense is present) If the policy on the endpoint determines that the file has to be sent to Advanced Threat Defense, the TIE server sends the file for further analysis. To send the file to Advanced Threat Defense, these requirements must meet:
     - **Advanced Threat Defense (ATD)** option is configured under **Shared Cloud Solutions** policy on the McAfee ePO server.
     - Size of the file is less than 10 MB.
     - The TIE server returns the file hash's reputation to the SVM once the data is received from Advanced Threat Defense after analysing the file. See the additional steps under *How Advanced Threat Defense works* in this guide.

6. The McAfee MOVE AntiVirus takes action based on the **Shared Cloud Solutions** policy assigned to the system that is running the file.

7. The SVM sends threat details as threat events to McAfee ePO.
Install the Threat Intelligence Exchange server appliance

Install and configure the Threat Intelligence Exchange server and the Data Exchange Layer brokers.

**Task**

1. Open the VMware vSphere client, then click **File | Deploy OVF Template**.

2. Browse to and select the **TIE.ova** file on your computer, then click **Next** to start the installation wizard.

3. Complete the steps in the wizard, accepting the default values or entering different values as needed.

4. When finished, select **Power On** to turn on the virtual machine and open a **Console** window to install the server appliance.

5. Read and accept the license agreement. Press **Enter** to view each page.
   When finished reading the license agreement, enter **Y** to accept the terms and continue.

6. Create a root password (at least nine characters) for the TIE appliance, then press **Y** to continue.

7. Enter the operational account name, real name, and password, then press **Y** to continue.
   The account name is typically something like **jsmith** and is used to log on to the server. The real name is your full name, for example, **John Smith**.

8. On the **Network Selection** page, enter **N** to continue.

9. Select a configuration type, then enter **Y** to continue.
   - **DHCP** — Enter **D**.
   - **Manual IP address** — Enter **M**, then enter the remaining information.

10. Enter the host name and domain name of the computer where you are installing the TIE server appliance. Enter **Y** to continue.

11. Enter up to three Network Time Protocol servers to synchronize the time of the TIE server. Use the default servers listed, or enter the address for up to three servers. Enter **Y** to continue.

12. Enter the IP address or fully qualified domain name, port, and account information for your McAfee ePO server. The user account must have administrator rights. Enter **Y** to continue.

13. Select the services to run on the TIE server, then enter **Y** to continue.
   The next page appears only if you selected the TIE Server option on the previous page.

Specify how to configure the primary and secondary servers. You can have only one primary server in your environment, but you can have several optional secondary servers. Install the primary server first.

- **Master** server replicates the Threat Intelligence Exchange database to all slave servers, if you have them. There can be only one Master server at a time.

- **Write-only Master** server doesn't process reputation requests or any non-essential functionality beyond writing and maintaining the database. Because a write-only master server doesn't process requests over the Data Exchange Layer, it increases system performance by replicating the database, leaving the Data Exchange Layer requests to the slave servers.
• **Slave** server processes Data Exchange Layer requests exactly like a master server, using a database that's replicated from the master database. Slave servers provide faster response time, and increased availability and scalability. The slave server must have access to the master server.

• **Reporter** is a slave server that provides data to McAfee ePO and does not process reputation requests. The Reporter does not serve queries or aggregate updates, but it has a complete copy of the database and reduces the load on the Master server.

14 Enter the Postgres database account information. The PostgreSQL account allows the McAfee ePO server to connect to and receive data from the TIE server. The information entered here is used in the McAfee ePO **Registered Servers** page.

   The account name and password can be anything you like in the stated parameters.

15 If the DXL broker is installed on the TIE server, then specify the port that the Data Exchange Layer uses. Use the default port, or enter a port number in the range shown, then enter \textit{Y} to continue.

16 When the logon screen appears, close it.

17 Verify that the TIE server is provisioned: open the System Tree in McAfee ePO and look in the domain where you installed the server appliance.

### Deploy the Data Exchange Layer client to McAfee MOVE AntiVirus SVM

You must deploy the DXL client to all your McAfee MOVE AntiVirus SVMs for TIE integration.

**Task**

For details about product features, usage, and best practices, click \textit{?} or \textit{Help}.

1 Log on to McAfee ePO as an administrator.

2 Select \textit{Menu} \mid \textit{Software} \mid \textit{Product Deployment}, then click \textit{New Deployment}.

3 Complete the new deployment information, then start the deployment.

4 After deploying the DXL client on the SVM, verify that the DXL **Connection Status** on McAfee ePO is Connected.

   \textbf{You must restart the McAfee MOVE AntiVirus SVM service if you deploy the DXL Client after deploying the McAfee MOVE AntiVirus SVM.}

   For details about deploying software from McAfee ePO, see the product documentation for your version of McAfee ePO.

### Verify the Threat Intelligence Exchange server installation

After installing the Threat Intelligence Exchange and Data Exchange Layer components, perform this task to verify the installation.
Task
For details about product features, usage, and best practices, click ? or Help.

1 Log on to McAfee ePO as an administrator.

2 In the System Tree, click the TIE server name, then click Products. Verify that the following components are listed with the corresponding version for the installation process.
   • McAfee DXL Broker
   • McAfee DXL Client
   • McAfee Threat Intelligence Exchange Server

3 In the System Tree, verify that the TIESERVER tag was applied to the system.

4 Select Menu | Configuration | Server Settings, click DXL ePO Client, then verify that the Connection State is Connected.

5 In the System Tree, select the TIE server, then from the Actions menu, select DXL | Lookup in DXL.

6 Verify that the Connection State is Connected.

7 Log on to the McAfee MOVE AntiVirus SVM system.

8 From system tray, click and select About... to open McAfee About... window.

9 Under McAfee Data Exchange Layer, verify that the DXL Connected Status is Connected.

The DXL broker and DXL client communication is now up and running. From McAfee ePO, you can select Menu | Systems Section | TIE Reputations to verify that you can search for files and certificates. It might take some time for reputation information to update the database.

Create a new registered server
To view TIE information in McAfee ePO reports and dashboards, create a new registered server in 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 | Configuration | Registered Servers, then click New Server.

3 In the Server type drop-down list, select Database Server.

4 Enter a Name, for example, TIE Server, then click Next.

5 On the Details page:
   • Select Make this the default database for the selected database type.
     This option is automatically selected when you create the first registered server. If you have more than one TIE database, select this option only for the database that you want as the default.
   • In the Database Vendor field, select TieServerPostgres.
   • In the Host name or IP address field, enter the IP address of the TIE server.
• Leave the Database server instance and Database server port fields blank (if they appear).
• For the Database name, enter tie.
• In the User name and password fields, enter the read-only postgress user name and password that you specified on the PosgresSQL page during the server installation.

6  Click Test Connection.
7  Click Save to save the newly configured Registered Server details.

McAfee ePO communicates with the server and retrieves data for the reports and dashboards.

Enable TIE and Advanced Threat Defense protection for McAfee MOVE AntiVirus

Files and certificates have threat reputations based on their content and properties. The Shared Cloud Solutions policy determines whether files and certificates are blocked or allowed on systems in your environment based on reputation levels.

Before you begin
• You installed TIE and Advanced Threat Defense to set up the requirements for integrating them with McAfee MOVE AntiVirus.
• You installed the McAfee MOVE AntiVirus extension on the McAfee ePO server.

File and certificate reputation is determined when a file tries to run on a managed system. For details on how to install and set up the TIE requirements, see the product documentation for your version of TIE.

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 | Policy Catalog, select MOVE AntiVirus 4.5.0 from the Product drop-down list, then select Shared Cloud Solutions from the Category drop-down list.
3  From Enable TIE, select Enabled to determine file and certificate reputation when a Portable Executable (PE) file is accessed on a managed endpoint.
   PE file includes these formats: .cpl, .exe, .dll, .ocx, .sys, .scr, .drv, .efi, .fon
4  From TIE Non-PE Lookup, select Enabled to determine file and certificate reputation when a non-PE file is accessed on a managed endpoint.
   To enable TIE Non-PE Lookup, make sure that you selected Enable TIE option.
5  Under Threat Intelligence Exchange (TIE), configure these reputation settings for files and certificates.
Based on their TIE reputation score, the SVM performs threat detection responses specified in the On Access Scan or On Demand Scan policies for files above the reputation score that you have selected. The SVM performs scan action for selected files based on threat detection response specified in OAS/ODS policies.

6 From Advanced Threat Defense (ATD), select Submit files to ATD at and below to send files with these reputation scores to Advanced Threat Defense for further analysis.

- Most likely malicious
- Unknown
- Most likely trusted

For example, if the file hash is not found in the TIE server, the TIE server queries McAfee GTI for the file hash reputation. McAfee GTI sends the information that is available, for example "unknown reputation." The TIE server stores that information and sends the same to SVM.

If Submit files to ATD at and below option is enabled and the file is determined as Advanced Threat Defense candidate by TIE server, then SVM sends the file to Advanced Threat Defense through TIE server for analyzing.
If you are using TIE 2.0.0 version, then perform these actions to successfully send the file to Advanced Threat Defense through TIE server for analyzing:

a. Open the TIE 2.0.0 server console.

b. Run this command to open the TIE properties file: vi /opt/McAfee/tieserver/conf/tie.properties

c. Change the jetty.http.enabled value to true. By default this value is false.

```
# Jetty
#
jetty.http.enabled=true
jetty.http.port=993
jetty.http.enabled=true
#comme-separated list of strings used to match cipher names to be excluded. - can be used as wildcard
jetty.excludedCipherSuites=.*NULL.*,.*RC4.*,.*MD5.*,.*DES.*,.*DES.*,.*MD5_SHA$
#comme-separated list of strings used to match cipher names to be included. - can be used as wildcard
jetty.includedCipherSuites=TLS_DHE_RSA.*,TLS_ECDHE.*,TLS_RSA.*
jetty.minThreads=10
jetty.maxThreads=100
#
# REST support
#
```

Verify the TIE server integration
Verify the TIE integration before configuring and using the scan policies to detect malware.

Before you begin
You installed TIE server and configured Threat Intelligence Exchange (TIE) option under Shared Cloud Solutions policy on the McAfee ePO server.

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

1. Log on to the McAfee MOVE AntiVirus client system as an administrator.

2. Run an EICAR test.

3. Log on to McAfee ePO as an administrator.


5. Under Threat Type, verify that Virus detected using TIE appears.

Verify the Advanced Threat Defense integration
Verify the Advanced Threat Defense integration before configuring and using the scan policies to detect malware.

Before you begin
You installed Advanced Threat Defense and configured Advanced Threat Defense (ATD) option under Shared Cloud Solutions policy on the McAfee ePO server.
**Task**

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

1. Log on to the McAfee MOVE AntiVirus SVM machine.

2. Run this command: `mvadm stats`

3. Verify that **Total ATD candidates** and **Total ATD successful submissions** values appear.

   ![Command Output](image)

4. Log on to McAfee ePO as an administrator.

5. Select **Menu | Systems | TIE Reputations**.

6. Verify the Advanced Threat Defense reputation details for Advanced Threat Defense submitted files under **File Search | ATD Reputation**.
Preparing to upgrade McAfee MOVE AntiVirus (Multi-Platform)

Review this list before upgrading your environment.

- The McAfee MOVE AntiVirus 4.5.0 client and SVM packages upgrade over versions 3.5.x, 3.6.x, and 4.0.0.
- To upgrade McAfee MOVE AntiVirus (Multi-Platform), you need to install and upgrade these components in this order:
  1. Product extension
  2. Create the SVM Manager appliance (virtual machine) by deploying the SVM Manager OVF package and configuring a VM network for communication with the SVM Manager.
     - Create the SVM Manager appliance (virtual machine), see Set up the SVM Manager
     - Assign the SVM using SVM Manager, see Assign the SVM using SVM Manager
  3. SVM
     - VirusScan Enterprise 8.8 must be installed on the target system before you deploy the McAfee MOVE AntiVirus SVM package.

    Best practice: Upgrade the McAfee scanning engine to the latest 5800 engine that provides enhanced detection capabilities.

  4. McAfee MOVE AntiVirus client

    (For 3.5.1 and 3.6.1 only) You must upgrade the client to 4.5.0 to communicate with the McAfee MOVE AntiVirus 4.5.0 SVM.

    Make sure that you remove any Debian package deployment task from the client task catalog in McAfee ePO before upgrading to McAfee MOVE AntiVirus 4.5.0.

Install the extension

Version 4.5.0 of the McAfee MOVE AntiVirus extension upgrades the 4.0.0 extension on the McAfee ePO server. Version 4.5.0 of the McAfee MOVE AntiVirus extension coexists with the 3.5.x and 3.6.x extensions on the McAfee ePO server, so that you can perform the product migration using the migration utility. For details, see McAfee MOVE AntiVirus 4.5.0 Migration Guide.

Before you begin
The extension file is in an accessible location on the network.

All policies created in version 4.0.0 exists after you upgrade to version 4.5.0.

Use the Migration Utility to migrate the policies created in versions 3.5.x and 3.6.x after you upgrade to version 4.5.0. For details, see McAfee MOVE AntiVirus 4.5.0 Migration Guide.

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. Click Install Extension.
4. Browse to and select the extension file, then click OK.
5 After a confirmation message, click OK.

If you are upgrading from McAfee MOVE AntiVirus 4.0.0 and using Internet Explorer browser, refresh the policy pages or clear the cache files in the browser to update the policy pages to 4.5.0.

6 (For 3.5.x and 3.6.x only) Migrate your existing policies using the Migration Utility. For details, see *McAfee MOVE AntiVirus 4.5.0 Migration Guide*.

**Upgrade the McAfee MOVE AntiVirus SVM with McAfee ePO**

Version 4.5.0 of the McAfee MOVE AntiVirus SVM upgrades the 3.5.x, 3.6.x, and 4.0.0 SVMs.

**Best practice:** Stagger the SVM upgrades so that protection is maintained on the legacy client virtual machines. In environments that are made up primarily of persistent images, create additional versions of the 4.5.0 SVM rather than upgrading an existing SVM.

**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*, select *McAfee Agent | Product Deployment*, then click *Actions | New Task*.

3 Make sure that *Product Deployment* is selected, then click *OK*.

4 Type a name for the task you are creating and add any notes.

5 Next to *Target platforms*, select *Windows* as the type of platform to use for deployment.

6 Next to *Products and components*, set the following:
   - Select the product from the first drop-down list.
     The products listed are those for which you have already checked in a package to the Master Repository. If you do not see the product you want to deploy, you must first check in that product’s package.
   - Set the action to *Install*, then select the language of the package, and the branch.
   - To specify command-line installation options, type command-line options in the *Command line* text field.

7 (Windows only) Next to *Options*, select if you want to run this task for every policy enforcement process, then click *Save*.

8 Select *Menu | Systems | System Tree | Assigned Client Tasks*, then select the required group in the System Tree.

9 Select the *Preset* filter as *Product Deployment (McAfee Agent)*.

   Each assigned client task per selected category appears in the details pane.

10 Click *Actions | New Client Task Assignment* to open the Client Task Assignment Builder wizard.

11 On the Select Task page, select *McAfee Agent* for the product and *Product Deployment* for the task type, then select the task you created to deploy the product.

12 Next to *Tags*, select the platforms to which you are deploying the packages, then click *Next*. 
13 On the Schedule page, select whether the schedule is enabled, and specify the schedule details, then click **Next**.

14 Review the summary, then click **Save**.

**Upgrade persistent virtual machines**

Upgrading persistent virtual machines provides nearly seamless virus protection, but requires the overhead of duplicate SVMs during the upgrade process.

We recommend this method for environments made up primarily of persistent virtual machines, where the clients require support from the SVM during the client migration process.

**Task**

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

1 Log on to McAfee ePO as an administrator.

2 Install the McAfee MOVE AntiVirus 4.5.0 package and upgrade the McAfee MOVE AntiVirus extension in McAfee ePO.

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

4 Install SVM version 4.5.0 on the virtual server.

5 Create a new McAfee MOVE AntiVirus 4.5.0 policy that references the SVM you created, and assign it to the virtual machines being upgraded.

   The existing client policy configuration can be used during the upgrade. However, you use the new settings specified in the client's SVM assignment policy, you no longer can use the existing manual policy configuration.

6 Create a McAfee ePO client task to upgrade the McAfee MOVE AntiVirus clients to version 4.5.0.

   As the upgrade task is executed on virtual machines, the VMs begin to use the 4.5.0 SVM for file scanning.

7 After all clients are upgraded to version 4.5.0, shut down the older versions of the SVM.

**Upgrade non-persistent virtual machines**

Upgrading non-persistent virtual machines does not require creating additional SVMs, although it might result in a window of time when virtual machines are unprotected.

We recommend that you perform this upgrade during scheduled downtime.

**Task**

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

1 Log on to McAfee ePO as an administrator.

2 Install the McAfee MOVE AntiVirus 4.5.0 client package and McAfee MOVE AntiVirus SVM packages and upgrade the extensions in McAfee ePO.

3 Create a new 4.5.0 client policy definition that references existing SVM systems.

   The existing client policy configuration can be used during the upgrade. However, you use the new settings specified in the client's SVM assignment policy, you no longer can use the existing manual policy configuration.
4 From the McAfee ePO console, upgrade all SVMs to version 4.5.0.

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

5 Change the master or golden image by deploying version 4.5.0 of the McAfee MOVE AntiVirus client from McAfee ePO, or by manually upgrading the client directly on the master image.

**Upgrading the McAfee MOVE AntiVirus client with McAfee ePO**

Upgrading McAfee MOVE AntiVirus clients from McAfee ePO requires two tasks. You must first create an upgrade client task, then assign that task to virtual machines.

- Create a McAfee MOVE AntiVirus client upgrade task, see *Create a product deployment client task*
- Assign the McAfee MOVE AntiVirus client upgrade task to virtual systems, see *Assign a client task*

**Upgrade McAfee MOVE AntiVirus (Multi-Platform) 2.6.2 to 4.5.0**

If you are using McAfee MOVE AntiVirus (Multi-Platform) 2.6.2, you must first upgrade the product extension to 3.5.1. You can then use the Migration Assistant to migrate the legacy policies and client tasks to 4.5.0.

**Before you begin**

- Make sure that the extension file is in an accessible location on the network.
- You have your policy assignment details of 3.5.1 **General** policy.

**Task**

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

1 Log on to McAfee ePO as an administrator.

2 Install the McAfee MOVE AntiVirus 3.5.1 extension.

3 Select **Menu | Policy | Policy Catalog**, then select **MOVE AV (Multi-Platform) Client 3.5.1** from the product list.

4 From the **Category** list, select **General**, then open the required custom policy.

5 From the **General** tab, note the offload scan server configuration details.

6 Select **Menu | Policy | Policy Catalog**, then select **MOVE AV (Multi-Platform) Client 3.5.1** from the product list.

7 From the **Category** list, select **Offload Scan Server Assignment**, then duplicate the **McAfee Default** policy.

8 Open the duplicate **Offload Scan Server Assignment** policy.

9 From **Offload Scan Server**, select **Assign Offload Scan Server manually** and configure these settings with the offload scan server details noted from the **General** policy.
   - IP Address, host name, or FQDN of Offload Scan Server
   - Port of Offload Scan Server

10 Assign the new policy to the VMs, which were assigned with **General** policy.

You can now migrate all your legacy policies and client tasks that are assigned to the client systems to 4.5.0 using Migration Assistant.
Uninstalling McAfee MOVE AntiVirus (Multi-Platform)

A full uninstall involves removing these components: McAfee MOVE AntiVirus client, McAfee MOVE AntiVirus SVM, and the McAfee MOVE AntiVirus extensions.

Uninstall the client and SVM
You must create an uninstallation task before you can apply it to systems and remove the software from the client.

Uninstalling the McAfee MOVE AntiVirus client with McAfee ePO requires two tasks. First create an uninstallation client task, then assign that task to virtual systems.

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. In the left column under McAfee Agent, select Product Deployment.
4. Click Actions | New Task, select Product Deployment, then click OK.
5. Type the name of the task, like Uninstall MOVE AV client on VM client, and an optional description.
6. Make sure that Windows is the only target platform selected.
7. For Products and components, select the following, then click Next.
   a. Select MOVE AV [Multi-Platform] client 4.5.0 or MOVE AV [Multi-Platform] SVM 4.5.0 from the first drop-down list.
   b. Set the action to Remove, set the language to Language Neutral, and set the branch to Current.
   c. Leave the Command Line setting blank.
8. Select the remaining options according to your environment’s best practices, then click Save.

The newly created task appears in the Client Task Catalog.

Assign the uninstallation task to virtual systems
The uninstallation task for client and McAfee MOVE AntiVirus SVM must be assigned to virtual systems to take effect.

Before you begin
The McAfee MOVE AntiVirus client is added to the Master Repository and your virtual systems are added to the System Tree.

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

1. Log on to McAfee ePO as an administrator.
2. Select a group in the System Tree.
3. Select Menu | Policy | Client Task Assignments, then click the Assigned Client Tasks tab.
4. Click Actions | New Client Task Assignment.
5  Configure these settings, then click Next.
   •  Product — McAfee Agent
   •  Task Type — Product Deployment
   •  Task Name — The name of the task you created earlier

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

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

The McAfee MOVE AntiVirus client is removed from every system in the selected group in the System Tree.

**Remove the client or SVM package from McAfee ePO**
Remove the client or McAfee MOVE AntiVirus SVM package from the 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 | Software | Master Repository.

3  Select MOVE AV [Multi-Platform] client 4.5.0 or MOVE AV [Multi-Platform] SVM 4.5.0, then click Delete.

**Uninstall the extensions**
Uninstall the McAfee MOVE AntiVirus extensions 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  From the Extensions tab under McAfee group, select Data Center Security.

4  Click Remove next to each extension.

   ![Warning]

   You must now uninstall both extensions for McAfee MOVE AntiVirus. MOVE AntiVirus extension must be removed first.

5  Delete reports and queries manually after uninstalling the extension.

**Uninstall the SVM Manager**
For a full uninstall of the product, you must uninstall the SVM Manager and remove its entry from the McAfee ePO server.

**Before you begin**
You must have sudo rights to perform these actions.
**Task**

1. Log on to SVM Manager appliance (virtual machine).
2. Run the `sudo poweroff` command, which shuts down the appliance.
3. Log on to the hypervisor that is hosting the SVM Manager appliance, then delete the SVM Manager VM.
4. Remove the SVM Manager entry from the McAfee ePO server.
Agentless installation and configuration

To set up your environment for McAfee MOVE AntiVirus (Agentless) deployment, you must 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 in the hypervisor
- As a filter driver in 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
- Setting up the SVM
- Manually configure the McAfee MOVE AntiVirus SVM
- OVF properties
- Configure the SVM details in McAfee ePO
- Deploying McAfee MOVE AntiVirus (Agentless) in an NSX environment
- Deploying McAfee MOVE AntiVirus (Agentless) in vCNS environment
- Preparing to upgrade McAfee MOVE AntiVirus (Agentless)
- Uninstalling McAfee MOVE AntiVirus (Agentless)
Setting up the SVM

You must deploy the OVF and configure the SVM before you can begin using the McAfee MOVE AntiVirus (Agentless) software.

McAfee MOVE AntiVirus SVM deployment options

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

Here are the three McAfee MOVE AntiVirus SVM deployment options.

• **VMware vCloud Networking and Security Manager-based deployment** — Check in the McAfee MOVE AntiVirus SVM package and use McAfee ePO to deploy it to one or more clusters. You can select one or more hosts, a group of hosts, or a whole vCenter to deploy and specify the schedule for deployment. This method allows you to deploy the McAfee MOVE AntiVirus SVM with all prerequisites.

• **VMware NSX Manager-based deployment** — 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** — Manually deploy the SVM to each hypervisor from the vSphere Client. The vSphere Client must be connected to a vCenter server, not directly to a hypervisor.

The manual deployment of the McAfee MOVE AntiVirus SVM is a legacy method. So, we recommend that you use McAfee MOVE AntiVirus (Agentless) in vCNS environment or McAfee MOVE AntiVirus (Agentless) in an NSX environment deployment method.

Here are the two configuration options.

• Automatic configuration

• Manual configuration

Manually configure the McAfee MOVE AntiVirus SVM

When you don’t provide the configuration information on the properties page for manual deployment of the McAfee MOVE AntiVirus SVM, you must manually configure the McAfee MOVE AntiVirus SVM.

• The McAfee MOVE AntiVirus 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
Security update for McAfee MOVE AntiVirus SVM

The source repository pulls the security updates directly from the Ubuntu repositories. The auto-update checks for security updates once per day. To manually check for the updates, perform these actions.

For details, see: https://help.ubuntu.com/community/Repositories/Ubuntu.

Run this command to update the local Ubuntu repository:

```
sudo apt-get update
```

Run this command to check whether the upgrades are taking place:

```
sudo unattended-upgrade --debug --dry-run
```

Run this command to manually install the security updates:

```
sudo unattended-upgrade -d
```

OVF properties

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

<table>
<thead>
<tr>
<th>Component</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>McAfee ePO</td>
<td>FIPS Mode</td>
<td>Specified if FIPS mode is enabled on the McAfee ePO server.</td>
</tr>
<tr>
<td>McAfee ePO</td>
<td>IP Address</td>
<td>The IP address or DNS name of the McAfee ePO server.</td>
</tr>
<tr>
<td>McAfee ePO</td>
<td>Password</td>
<td>The user’s password.</td>
</tr>
<tr>
<td>McAfee ePO</td>
<td>Port</td>
<td>The console-to-application server communication port used when connecting to the McAfee ePO server. Default is 8443.</td>
</tr>
<tr>
<td>McAfee ePO</td>
<td>User name</td>
<td>The user name used to access the McAfee ePO server.</td>
</tr>
<tr>
<td>Network</td>
<td>Type</td>
<td>How to configure the McAfee MOVE AntiVirus 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 McAfee MOVE AntiVirus SVM’s default gateway.*</td>
</tr>
<tr>
<td>Network</td>
<td>IP Address</td>
<td>The static IP Address of the McAfee MOVE AntiVirus SVM.*</td>
</tr>
<tr>
<td>Network</td>
<td>Netmask</td>
<td>The netmask for the McAfee MOVE AntiVirus SVM’s management network.*</td>
</tr>
</tbody>
</table>

![Information](https://help.ubuntu.com/community/Repositories/Ubuntu) You must have a valid McAfee ePO user name that uses McAfee ePO authentication. The user name should have administrator privileges.
<table>
<thead>
<tr>
<th>Component</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Network</td>
<td>The network for the McAfee MOVE AntiVirus 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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>the IP address and the Netmask.</td>
</tr>
<tr>
<td>SVM</td>
<td>Domain</td>
<td>The McAfee MOVE AntiVirus SVM's domain name and the default domain name for</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DNS queries.</td>
</tr>
<tr>
<td>SVM</td>
<td>Host name</td>
<td>The host name of the McAfee MOVE AntiVirus SVM.</td>
</tr>
<tr>
<td>SVM</td>
<td>Svaadmin$1</td>
<td>The password of the svaadmin account. This password can be changed from</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Menu</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 McAfee MOVE AntiVirus SVM with the</td>
</tr>
<tr>
<td>vCloud Networking and Security Manager</td>
<td>User name</td>
<td>The user name used to register the McAfee MOVE AntiVirus 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 AntiVirus in an NSX environment, make sure that you leave the NSX-specific deployment parameters blank under SVM.

---

**Configure the SVM details in McAfee ePO**

You must specify these details under SVM Configuration in the McAfee MOVE AntiVirus SVM Settings policy in McAfee ePO.

**Task**

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

1. Log on to the McAfee ePO as an administrator.

2. Select Menu | Policy | Policy Catalog, select MOVE AntiVirus 4.5.0 from the Product drop-down list, then select SVM Settings from the Category drop-down list.

3. Click New Policy or click the name of an existing policy to edit it.

4. Type a name for the new policy (for example, MOVE AV SVM Settings Policy), then click OK.

5. Under SVM Configuration, configure these settings as needed, then click Save.

   - **Hypervisor/vCenter Server** — Enter the valid IP address of either the hypervisor that the SVM resides on or the vCenter server.

   - **Protocol** — Select https or http, depending on the protocol the server uses to receive client requests.

   - **vCenter/ESXi Port** — Specify the port number of the SVM. The default port is 443.
Deploying McAfee MOVE AntiVirus (Agentless) in an NSX environment

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

Deploying the McAfee MOVE AntiVirus service (NSX)

The extensions for Cloud Workload Discovery and McAfee MOVE AntiVirus allow you to register the vCenter account and set up the NSX requirements. You must complete this process before deploying the McAfee MOVE AntiVirus 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.

The deployment process

1. Register vCenter Server with NSX Manager
2. Install the extensions
3. Register a VMware vCenter account with McAfee ePO
4. Set up a common configuration for McAfee ePO and SVM
5. Check in the SVM package to McAfee ePO
6. Validate the NSX Manager connection to the McAfee ePO server
7. Register the McAfee MOVE AntiVirus service with NSX Manager using McAfee ePO
8. Apply McAfee MOVE AntiVirus (Agentless) protection to your VMs
9. Deploy the McAfee MOVE AntiVirus service using vSphere Web Client
10. Apply the NSX Security Policy to the NSX Security Group
11. Create an NSX Security Group and Policy in the NSX Manager
12. Verify the policy export details in vSphere Web Client
The overall McAfee MOVE AntiVirus service deployment in an NSX environment consists of the following tasks.

1. Register vCenter Server with NSX Manager.
2. Install the extensions for Cloud Workload Discovery and McAfee MOVE AntiVirus on McAfee ePO in this order:
   - Cloud Workload Discovery
   - McAfee MOVE AntiVirus
3. Register a VMware vCenter account with McAfee ePO.
4. Set up a common configuration for McAfee ePO and McAfee MOVE AntiVirus SVM on the McAfee ePO server.
5. Check in the McAfee MOVE AntiVirus 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 needed.
7. Register the McAfee MOVE AntiVirus service with NSX Manager using McAfee ePO.
8. Verify the policy export details in vSphere Web Client.
10. Apply the NSX Security Policy to the NSX Security Group.
11. Deploy the McAfee MOVE AntiVirus service using vSphere Web Client.
12. Apply McAfee MOVE AntiVirus (Agentless) protection to your VMs.

**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 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, 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 product files on the management server

The product extensions for Cloud Workload Discovery, McAfee MOVE AntiVirus, and VirusScan Enterprise for Linux must be installed on the McAfee ePO server before you can manage McAfee MOVE AntiVirus on your virtual machines.

Before you begin
The extension files are in an accessible location on the network.

Install the VirusScan Enterprise for Linux extension to manage the VirusScan Enterprise for Linux policy on the SVM Manager. VirusScan Enterprise for Linux is only licensed for the SVM Manager, not for other Linux systems in your 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.
   You must install the product extensions in this order.

<table>
<thead>
<tr>
<th>Extension</th>
<th>Package name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Workload Discovery</td>
<td>Cloud_Workload_Discovery_Private_4.5.0.zip</td>
</tr>
<tr>
<td>McAfee MOVE AntiVirus extension</td>
<td>MOVE_AV_Ext_4.5.0_Licensed.Zip</td>
</tr>
<tr>
<td>VirusScan Enterprise for Linux extension</td>
<td>McAfeeVSEForLinux-2.0.3.-release-epo.zip</td>
</tr>
<tr>
<td>Product Help extension</td>
<td>MOVE_AV_HELP_EXT_4.5.0.Zip</td>
</tr>
</tbody>
</table>

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

Register a VMware vCenter account with McAfee ePO

To enable and manage the security of the virtual machines in your datacenter with McAfee 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
- You installed the Cloud Workload Discovery extension on the McAfee ePO server.
- You 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 Actions | Add Cloud Account to open the Add Cloud Account dialog box.

3 From the Choose Cloud Provider drop-down list on the Add Cloud Account dialog box, 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.
   • Sync Interval (In Minutes) — Specify the interval for running the next vCenter discovery (default value is 5 minutes).
   • Port — 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.

![System Tree Diagram]

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 deployment**

Before deploying McAfee MOVE AntiVirus SVM, configure these settings on the McAfee ePO server, so that they are retrieved and used for every McAfee MOVE AntiVirus SVM deployment.

**Before you begin**

You installed the McAfee MOVE AntiVirus extension on the 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 AntiVirus Deployment**.
3. On 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><strong>Password</strong></td>
<td>Type the password of the McAfee ePO console that the administrator has currently logged on.</td>
</tr>
<tr>
<td><strong>Confirm Password</strong></td>
<td>Retype the password.</td>
</tr>
</tbody>
</table>

Once the McAfee MOVE AntiVirus (Agentless) product setup is done and running, you must not delete the Registered Cloud Account.
Table 3-2 McAfee MOVE AntiVirus SVM configuration

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname Prefix</td>
<td>Type a unique prefix that is added to the host name of the McAfee MOVE AntiVirus SVM. The prefix can include characters a–z, A–Z, 0–9, and [-], without space.</td>
</tr>
</tbody>
</table>
| Password           | Type a password to be used as the McAfee MOVE AntiVirus 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). |
| Confirm Password   | Retype the password.                                                         |

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

Check in the McAfee MOVE AntiVirus SVM package to McAfee ePO

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

Before you begin

You installed the McAfee MOVE AntiVirus extension on the McAfee ePO server.

For a successful check-in, do not change the file name of the McAfee MOVE AntiVirus 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 AntiVirus Deployment.

3 On the Configuration tab, click SVM Repository to open the SVM Repository page with these McAfee MOVE AntiVirus 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 McAfee MOVE AntiVirus SVM package checked in to McAfee ePO.</td>
</tr>
<tr>
<td>SVM Version</td>
<td>Version of the McAfee MOVE AntiVirus 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 McAfee MOVE AntiVirus SVM.</td>
</tr>
<tr>
<td>Action</td>
<td>• Delete — To remove an existing McAfee MOVE AntiVirus 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 under SVM Repository Details, browse to and select the McAfee MOVE AntiVirus SVM package, then click OK. This action checks in the McAfee MOVE AntiVirus SVM package to McAfee ePO.

You can check in up to three versions of McAfee MOVE AntiVirus SVM starting from 3.6.
Validate your NSX Manager using McAfee ePO

The Cloud Workload Discovery extension automatically detects and sends the details of your NSX Managers to the McAfee ePO server. But, these NSX servers are not yet registered with McAfee ePO.

**Before you begin**

- You created and configured NSX Manager.
- You registered the vCenter account with NSX Manager.
- You installed the McAfee MOVE AntiVirus extension on the McAfee ePO server.

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 AntiVirus Deployment**.
3. On 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>vCenter Account</td>
<td>Displays the name of the registered vCenter account.</td>
</tr>
<tr>
<td>NSX Manager Name</td>
<td>Displays the name of your NSX Manager.</td>
</tr>
<tr>
<td>Configuration Status</td>
<td>Specifies whether the NSX Manager is configured.</td>
</tr>
<tr>
<td>Action</td>
<td><strong>Edit</strong> — 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></td>
<td><strong>Do not include spaces.</strong></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>

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 McAfee MOVE AntiVirus service with NSX Manager using McAfee ePO

After registering your vCenter account details on NSX Manager and McAfee ePO, use McAfee ePO to enable the registration of McAfee MOVE AntiVirus (Agentless) as a service in NSX Manager.

The details of the registered vCenter, SVM, and NSX Manager are automatically retrieved and displayed on the McAfee ePO server. But you must register the McAfee MOVE AntiVirus service with the vCenter account using McAfee ePO. This registration permits the deployment of the McAfee MOVE AntiVirus service to the ESXi servers.

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 AntiVirus Deployment.

3 On 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 McAfee MOVE AntiVirus SVM package 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 McAfee MOVE AntiVirus service is registered and ready for deployment.</td>
</tr>
<tr>
<td></td>
<td>• Not Registered — Indicates that the McAfee MOVE AntiVirus service is not registered.</td>
</tr>
<tr>
<td></td>
<td>• Registration Failed — Indicates that the McAfee MOVE AntiVirus service failed.</td>
</tr>
<tr>
<td></td>
<td>• Register — Click to select the latest McAfee MOVE AntiVirus 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 McAfee 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 McAfee MOVE AntiVirus service.</td>
</tr>
</tbody>
</table>

4 Click Register under Actions to open the MOVE Service Registration dialog box.

Make sure that you have checked in the latest McAfee MOVE AntiVirus SVM required for the upgrade. Otherwise, the existing McAfee MOVE AntiVirus service is deployed to the ESXi servers.
5 Select the latest McAfee MOVE AntiVirus SVM and click OK. The McAfee MOVE AntiVirus service is now registered with the vCenter account that is registered with your NSX Manager.

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

The On Access Scan policies from McAfee ePO are exported to NSX in real time.

**On-access scan policy export to NSX**

After you register the McAfee MOVE AntiVirus service on McAfee ePO server, the On Access Scan policies for McAfee MOVE AntiVirus 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.

Only the On Access Scan policies are exported from McAfee ePO to NSX Manager. If you need to assign the On Demand Scan policies, assign them manually on McAfee ePO.

When you create or change an On Access Scan 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.

Changes to On Access Scan policy names in McAfee ePO are not updated in NSX. You must manually update the name changes in NSX.

When you delete an On Access Scan policy from McAfee ePO, it is deleted from NSX Manager if it is not included in any of the NSX security policies.

**Best practice:** Verify the security policy in NSX before deleting any On Access Scan policy from McAfee ePO.
You can't delete the exported **On Access Scan** 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 McAfee MOVE AntiVirus service**

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

### Before you begin
- The host, where you are deploying the SVM using NSX Manager, is part of a cluster.
- The datacenter is using a vSphere Distributed Switch (vDS).
- Guest Introspection service is installed on all ESXi servers.
- Virtual machines have the latest VMware Tools installed, including the vShield Driver.
- 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 McAfee 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. When a new cluster is added, deploy the McAfee MOVE AntiVirus SVM again.

### 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] 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 McAfee MOVE AntiVirus service, then click **Next**.
5 From **Select storage and Management Network**, for each cluster, select a datastore on which to store the McAfee MOVE AntiVirus SVM, the network (the distributed port group used by the vDS on the datacenter), and the IP assignment for the McAfee 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 McAfee 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 McAfee MOVE AntiVirus and Introspection service VMs are not activated and they can't 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 Icon]

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 McAfee MOVE AntiVirus service. When deployment is complete, the McAfee 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.

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 McAfee 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 McAfee MOVE AntiVirus service is stopped.</td>
</tr>
</tbody>
</table>

The McAfee 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 the security policy and apply it to the security group of VMs that you want to protect.

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

#### Create an NSX security policy in the NSX Manager

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

**Before you begin**

- You installed the McAfee MOVE AntiVirus extension on the McAfee ePO server.
- The McAfee MOVE AntiVirus service is 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.
Click the green plus sign to add a Guest Introspection Service. Provide a name for the Guest Introspection Service and define these 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 McAfee MOVE AntiVirus service.</td>
</tr>
<tr>
<td>Description</td>
<td>Type some details about the McAfee 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_[Policy Name]-XX (Anti Virus)  
These are the profile configurations exported from McAfee ePO. If you create a policy or change an existing On Access Scan policy using McAfee ePO, it is immediately exported and available here to include for creating the security policy. But, any change to the name and description is not updated to NSX. You must manually update them, if needed. |
| State       | • Enabled — Select this to enable the service.  
              • Disabled — Select this to disable the service. |
| Enforce     | Yes |

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

You have created your NSX security policy for deploying McAfee MOVE AntiVirus (Agentless).
Create a global Security Group
Select the needed datacenters or their clusters from the available vCenter and configure them as a security group. This configuration allows you to assign the security policy to the group and protect its VMs.

**Before you begin**
- You installed the McAfee MOVE AntiVirus extension on the McAfee ePO server.
- VMware vSphere 5.5 is installed and added to the cluster.
- The McAfee 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 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.
6. Select the objects to exclude, then click Next to open the Ready to complete page.
   - **Warning:** 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 contains the virtual machines to be protected from the selected cluster.

**Apply the NSX security policy to the NSX security group**
Apply the security policy to the security group of VMs that you want to protect.

**Before you begin**
- You installed the McAfee MOVE AntiVirus extension on the McAfee ePO server.
- The McAfee MOVE AntiVirus service is registered with McAfee ePO.

Map a security policy (for example, SP1) to a security group (for example, SG1). The McAfee 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.
3. On 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 that you want to protect, then 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 On Access Scan policy that is exported from McAfee ePO.

**Working with security tags**
To define the assets that you want to protect, begin by creating a security group.

Security groups might be static (including specific virtual machines) or dynamic where membership is 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).
McAfee MOVE AntiVirus (Agentless) tag

After installing the McAfee MOVE AntiVirus extension and registering the McAfee MOVE AntiVirus service in McAfee ePO, the tag applied in your environment appears with details about the virtual machines where the tag was applied. **MCAFEE.MOVE.unprotected=yes** is the McAfee 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 **On Access Scan** and **On Demand Scan** policies with the configurations required for high security.

**Before you begin**

- You have registered the McAfee MOVE AntiVirus service with McAfee ePO.
- You specified your vCenter details under *SVM Configuration* in the McAfee MOVE AntiVirus SVM Settings policy in McAfee ePO.

Registering the McAfee MOVE AntiVirus service exports all **On Access Scan** policies of McAfee MOVE AntiVirus 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 AntiVirus Deployment.
3. On the Configuration tab, click Server Settings 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.
   - **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 McAfee 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 McAfee MOVE AntiVirus **On Access 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.

**Before you begin**

- You registered the McAfee MOVE AntiVirus service with McAfee ePO.
- You enabled the NSX tagging option in McAfee ePO.

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

Make sure that you have configured the scan policies available under MOVE AntiVirus 4.5.0 in McAfee ePO. This setting enforces unique scan policies to different groups, resource pool, or specific virtual machines protected by McAfee MOVE AntiVirus SVM on a hypervisor, even when McAfee Agent is not deployed to the client systems.

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

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

---

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

1. Install the McAfee MOVE AntiVirus extension on the McAfee ePO server.

2. Register and deploy the McAfee MOVE AntiVirus service.

3. 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>
<tr>
<td></td>
<td>These are the profile configurations exported from McAfee ePO. If you create an On Access Policy or change it using McAfee ePO, it is immediately exported and available here to include for creating the NSX security policy.</td>
</tr>
<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.

4. 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.
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>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>
<tr>
<td>Service Profile</td>
<td>McAfee MOVE AV_Scan All-xx (Quarantine)</td>
</tr>
<tr>
<td></td>
<td>Make sure that this MOVE AntiVirus policy is configured for high security with settings like:</td>
</tr>
<tr>
<td></td>
<td>• On-Demand Scanning — Enabled.</td>
</tr>
<tr>
<td></td>
<td>• File types to scan — All files.</td>
</tr>
<tr>
<td></td>
<td>• Quarantine configuration — Enabled.</td>
</tr>
<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 Add the Firewall Rules, as needed. Do not add any firewall or network introspection services.

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

5 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.

6 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.

7 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 McAfee 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.

   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.

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


    This mapping 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 On Access Scan policy of McAfee MOVE AntiVirus in McAfee ePO is assigned to these infected VMs.
Deploying McAfee MOVE AntiVirus (Agntless) in vCNS environment

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

Deploying the McAfee MOVE AntiVirus service (vCNS)

The extensions for Cloud Workload Discovery and McAfee MOVE AntiVirus are installed on the McAfee ePO server for registering the VMware vCenter account and setting up the vCNS requirements. This is needed before deploying the McAfee MOVE AntiVirus service and configuring the policies.

The deployment process

1. Install the Cloud Workload Discovery and McAfee MOVE AntiVirus extensions on the McAfee ePO server.

   If you install the McAfee MOVE AntiVirus extension before installing the Cloud Workload Discovery extension and registering the vCenter account, the hypervisors do not appear under the MOVE AntiVirus Deployment 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 McAfee MOVE AntiVirus SVM package to McAfee ePO.

5. Configure the IP Pool details.

Using McAfee ePO, you can register the McAfee MOVE AntiVirus SVM with vCNS, and configure 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 McAfee MOVE AntiVirus service deployment in a vCNS environment can be simplified into the following steps. The whole deployment process is only for vCNS environment and not for NSX environment.
6 Edit vShield Manager configuration.
7 Deploy SVM using McAfee ePO.

**Install the product files on the management server**

The product extensions for Cloud Workload Discovery, McAfee MOVE AntiVirus, and VirusScan Enterprise for Linux must be installed on the McAfee ePO server before you can manage McAfee MOVE AntiVirus on your virtual machines.

**Before you begin**
The extension files are in an accessible location on the network.

Install the VirusScan Enterprise for Linux extension to manage the VirusScan Enterprise for Linux policy on the SVM Manager. VirusScan Enterprise for Linux is only licensed for the SVM Manager, not for other Linux systems in your 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**.
   You must install the product extensions in this order.

<table>
<thead>
<tr>
<th>Extension</th>
<th>Package name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Workload Discovery</td>
<td>Cloud_Workload_Discovery_Private_4.5.0.zip</td>
</tr>
<tr>
<td></td>
<td>Make sure that you installed Common UI Core extension before installing Cloud Workload Discovery.</td>
</tr>
<tr>
<td>McAfee MOVE AntiVirus extension</td>
<td>MOVE-AV_Ext_4.5.0_Licensed.Zip</td>
</tr>
<tr>
<td>VirusScan Enterprise for Linux</td>
<td>McAfeeVSEForLinux-2.0.3.-release-epo.zip</td>
</tr>
<tr>
<td>Product Help extension</td>
<td>MOVE-AV_HELP_EXT_4.5.0.Zip</td>
</tr>
<tr>
<td></td>
<td>If you are upgrading from 4.0.0 version, remove the 4.0.0 Help extension manually.</td>
</tr>
</tbody>
</table>

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

**Register a VMware vCenter account with McAfee ePO**

To use McAfee MOVE AntiVirus to manage the security of the virtual machines in your datacenter, you must first add your VMware vCenter to the McAfee ePO server.

**Before you begin**
- Note that registering VMware vCenter account is not mandatory if you are not using autoscale SVM feature.
- You configured your VMware vCenter server that manages the ESXi servers, which host the guest VMs.
- You installed the Cloud Workload Discovery extension on the 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 | Configuration | Registered Cloud Accounts, then click Add Cloud Account to open the Add Cloud Account dialog box.

3 From the Choose Cloud Provider drop-down list on the Add Cloud Account dialog box, 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 Username — (Required) User name of the available VMware vCenter account.
   - vCenter Password — (Required) Password of the available VMware vCenter account.
   - Sync Interval (In Minutes) — Specify the interval for running the next vCenter discovery (default value is 5 minutes).
   - Port — 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 same organization as the 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 To verify that the VMs were imported, select Menu | Systems | System Tree.
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 the System Tree.

Set up a common configuration for McAfee MOVE AntiVirus SVM deployment

Before deploying the McAfee MOVE AntiVirus SVM, configure these settings on the McAfee ePO server, so that they are retrieved and used for every McAfee MOVE AntiVirus SVM deployment, from the same McAfee ePO server.

**Before you begin**
You installed the McAfee MOVE AntiVirus extension on the 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 AntiVirus Deployment.
3. On the Configuration tab, click General and configure these details:

<table>
<thead>
<tr>
<th>Table 3-3 McAfee ePO credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Options</strong></td>
</tr>
<tr>
<td>Password</td>
</tr>
<tr>
<td>Confirm Password</td>
</tr>
</tbody>
</table>
Table 3-4 McAfee MOVE AntiVirus SVM Configuration

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname Prefix</td>
<td>Type a unique prefix that is added to the host name of the McAfee MOVE AntiVirus SVM. The prefix can include characters a–z, A–Z, 0–9, and [-], without space.</td>
</tr>
</tbody>
</table>
| Password       | Type a password to be used as McAfee MOVE AntiVirus 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). |
| Confirm Password| Retype the password of the available McAfee MOVE AntiVirus SVM. |

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

Check in the McAfee MOVE AntiVirus SVM package to McAfee ePO

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

Before you begin
You installed the McAfee MOVE AntiVirus extension on the McAfee ePO server.

For a successful check-in, do not change the file name of the McAfee MOVE AntiVirus 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 AntiVirus Deployment.

3 On the Configuration tab, click SVM Repository to open the SVM Repository 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 McAfee MOVE AntiVirus SVM package checked in to McAfee ePO.</td>
</tr>
<tr>
<td>SVM Version</td>
<td>Version of the McAfee MOVE AntiVirus 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 McAfee MOVE AntiVirus 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 under SVM Repository Details, browse to and select the McAfee MOVE AntiVirus SVM package, then click OK. This action checks in the McAfee MOVE AntiVirus SVM package to McAfee ePO.

You can check in up to three versions of McAfee MOVE AntiVirus SVM starting from 3.6.

Configure the IP Pool details

An IP Pool is a range of IP addresses within the network. When you deploy the McAfee MOVE AntiVirus SVM, you can configure the IP addresses of the McAfee MOVE AntiVirus 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
MOVE AntiVirus SVM deployment, so that any unused IP address of the IP Pool is automatically assigned to the McAfee MOVE AntiVirus SVM.

**Before you begin**
- You installed the McAfee MOVE AntiVirus extension on the McAfee ePO server.
- You installed the Cloud Workload Discovery extension on the McAfee ePO server.

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 McAfee MOVE AntiVirus 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 AntiVirus Deployment**.
3. On 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>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>
<tr>
<td>Action</td>
<td>• <strong>Edit</strong> — Use this option to edit the IP Pool details.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Delete</strong> — Use this option to delete the IP Pool when its IP addresses are not in use.</td>
</tr>
</tbody>
</table>
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 configured and registered the vShield Manager account.
- The vShield Manager account has **vShield Administrator** permissions.
Using this configuration available on the McAfee ePO 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 AntiVirus Deployment**.
3. On 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>Configuration Status</td>
<td>Displays these registration statuses:</td>
</tr>
<tr>
<td></td>
<td>• Configured — Indicates that the vShield Manager is registered and ready for deployment.</td>
</tr>
<tr>
<td></td>
<td>• Not Configured — Indicates that the vShield Manager is not registered.</td>
</tr>
<tr>
<td></td>
<td>• Credentials unknown — Indicates that the vShield Manager is registered with VMware vCenter, but the credentials are unknown.</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 McAfee MOVE AntiVirus SVM to your hypervisors. This deployment provides virus protection for virtual machines on the hypervisor.

**Before you begin**
- You installed the McAfee MOVE AntiVirus extension on the McAfee ePO server.
- You checked in the McAfee MOVE AntiVirus SVM package to McAfee ePO.
You have appropriate permissions for the VMware vCenter account.

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 AntiVirus Deployment | Configuration | vShield Manager.

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.

Your McAfee ePO and client systems are in the domain. They must be able to communicate using their FQDN.

You manually synchronize the vCenter account using McAfee ePO. This action is important because the McAfee MOVE AntiVirus SVM deployment using McAfee ePO depends on the latest synchronization status provided by Cloud Workload Discovery. For details, see the product documentation for Cloud Workload Discovery.

You have appropriate permission to perform the McAfee MOVE AntiVirus 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 rollback functionality is available while deploying and upgrading the McAfee MOVE AntiVirus SVM. For example, if the McAfee MOVE AntiVirus 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 AntiVirus Deployment.
3. On the Service tab, click vCNS then 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.
   - Deployment Type — Displays the SVM deployment status as Install or Upgrade.
4. From the Selection page, select the required hypervisor to deploy the McAfee MOVE AntiVirus 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 McAfee MOVE AntiVirus SVM.
   - SVM Host Name — Displays the name of the McAfee MOVE AntiVirus SVM host.
   - Datastore (Free Space) — Specifies the free space present in the datastore, where the McAfee MOVE AntiVirus 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 one hypervisor.

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

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**
- **Provision Type**
- **IP Configuration**
5 Click Save and review the configurations of the hypervisor and McAfee MOVE AntiVirus SVM, then click Next to view the validation of these components and their status.

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

You can view these Validation Statuses:

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

6 From the **Verification** page, click **Deploy** to start the McAfee MOVE AntiVirus SVM deployment.

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

### View the McAfee MOVE AntiVirus SVM deployment details

After deploying or upgrading McAfee MOVE AntiVirus SVM, you can view the **Job Status Details** and **Task Status Details** for the deployment on the McAfee ePO server.

#### Before you begin

- You installed the McAfee MOVE AntiVirus extension on the McAfee ePO server.
- You have initiated the McAfee MOVE AntiVirus 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 AntiVirus Deployment**.
On the Job Status tab, you can view the McAfee MOVE AntiVirus SVM deployment or upgrade details.

Click any of the McAfee MOVE AntiVirus SVM deployment jobs to view these Job Status Details and its Task Status Details.

<table>
<thead>
<tr>
<th>Table 3-5  Job status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item</td>
</tr>
<tr>
<td>Hypervisors</td>
</tr>
<tr>
<td>vCenter Name</td>
</tr>
<tr>
<td>Deployment Type</td>
</tr>
<tr>
<td>Status</td>
</tr>
<tr>
<td>Start Time</td>
</tr>
<tr>
<td>End Time</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 3-6  Task status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item</td>
</tr>
<tr>
<td>Node Type</td>
</tr>
<tr>
<td>Task Type</td>
</tr>
<tr>
<td>Node Name</td>
</tr>
<tr>
<td>Status</td>
</tr>
<tr>
<td>Failure Reason</td>
</tr>
<tr>
<td>Start Time</td>
</tr>
<tr>
<td>End Time</td>
</tr>
</tbody>
</table>

The rollback functionality is available while deploying and upgrading the McAfee MOVE AntiVirus SVM. For example, if the McAfee MOVE AntiVirus 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 internal tasks of a deployment or an upgrade job. The task list for one job is displayed in sequence with Start Time, End Time, and Failure Reasons, if applicable.

<table>
<thead>
<tr>
<th>Table 3-7  During McAfee MOVE AntiVirus SVM deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task type</td>
</tr>
<tr>
<td>Installing vShield Endpoint</td>
</tr>
<tr>
<td>Deploying SVM</td>
</tr>
<tr>
<td>Powering on SVM</td>
</tr>
<tr>
<td>Registering SVM with McAfee ePO</td>
</tr>
</tbody>
</table>
### Table 3-7  During McAfee MOVE AntiVirus SVM deployment (continued)

<table>
<thead>
<tr>
<th>Task type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validating MOVE Service Status</td>
<td>Validates the status of the McAfee MOVE AntiVirus 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 McAfee MOVE AntiVirus SVM IP and Port to vShield Manager.</td>
</tr>
<tr>
<td>Activating SVM (Enabling security)</td>
<td>Specifies that the McAfee MOVE AntiVirus 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 systems on which vShield Driver installation is successful.</td>
</tr>
</tbody>
</table>

### Table 3-8  During McAfee MOVE AntiVirus 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 McAfee MOVE AntiVirus 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 McAfee MOVE AntiVirus SVM from the vShield Manager.</td>
</tr>
<tr>
<td>Unregistering solution from VSM</td>
<td>Removes the registration of the McAfee MOVE AntiVirus 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 McAfee MOVE AntiVirus SVM is turned off.</td>
</tr>
<tr>
<td>Removing SVM</td>
<td>Removes the turned off McAfee MOVE AntiVirus 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 3-9  During MOVE AntiVirus SVM upgrade

<table>
<thead>
<tr>
<th>Task type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploying SVM</td>
<td>Indicates that the McAfee MOVE AntiVirus SVM deployment is in progress.</td>
</tr>
</tbody>
</table>

When the latest McAfee MOVE AntiVirus SVM is already deployed on the hypervisor, the Deploying SVM task is skipped. Hence, other McAfee MOVE AntiVirus SVM-related tasks do not start.

<table>
<thead>
<tr>
<th>Task type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 McAfee MOVE AntiVirus 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 McAfee MOVE AntiVirus SVM from the vShield Manager.</td>
</tr>
<tr>
<td>Unregistering solution from VSM</td>
<td>Removes the registration of the McAfee MOVE AntiVirus 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 McAfee MOVE AntiVirus SVM is turned off.</td>
</tr>
</tbody>
</table>
### Table 3-9 During MOVE AntiVirus SVM upgrade (continued)

<table>
<thead>
<tr>
<th>Task type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Renaming SVM</td>
<td>Renaming the old turned off McAfee MOVE AntiVirus SVM.</td>
</tr>
<tr>
<td>Renaming SVM</td>
<td>Renaming the newly deployed McAfee MOVE AntiVirus SVM.</td>
</tr>
<tr>
<td>Powering on SVM</td>
<td>Specifies that the McAfee MOVE AntiVirus SVM is turned on.</td>
</tr>
<tr>
<td>Registering SVM with McAfee ePO</td>
<td>Registers the McAfee MOVE AntiVirus SVM with McAfee ePO.</td>
</tr>
<tr>
<td>Validating MOVE Service Status</td>
<td>Validates the status of the McAfee MOVE AntiVirus 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 McAfee MOVE AntiVirus SVM IP and Port to vShield Manager.</td>
</tr>
<tr>
<td>Activating SVM (Enabling security)</td>
<td>Specifies that the McAfee MOVE AntiVirus 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 systems on which vShield Driver installation is successful.</td>
</tr>
</tbody>
</table>

### Table 3-10 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 McAfee MOVE AntiVirus SVM task.</td>
</tr>
<tr>
<td>Rollback: Remove SVM</td>
<td>Rolls back the Deploying McAfee MOVE AntiVirus 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 McAfee MOVE AntiVirus SVM.</td>
</tr>
</tbody>
</table>

---

### Preparing to upgrade McAfee MOVE AntiVirus (Agentless)

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

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

- The McAfee MOVE AntiVirus 4.5.0 extension upgrades the 3.5.x, 3.6.x, and 4.0.0 extensions on the McAfee ePO server.

- (For 3.5.x and 3.6.x only) Quarantine settings and policy assignments are not migrated. You can use the Migration Utility to migrate the quarantine settings and policies.
Manual upgrade of the McAfee MOVE AntiVirus SVM

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

Install the extension

Version 4.5.0 of the McAfee MOVE AntiVirus extension upgrades the 4.0.0 extension on the McAfee ePO server. Version 4.5.0 of the McAfee MOVE AntiVirus extension coexists with the 3.5.x and 3.6.x extensions on the McAfee ePO server, so that you can perform the product migration using the migration utility. For details, see McAfee MOVE AntiVirus 4.5.0 Migration Guide.

Before you begin

The extension files are in an accessible location on the network.

All policies created in version 4.0.0 exists after you upgrade to version 4.5.0.

Use the Migration Utility to migrate the policies created in versions 3.5.x and 3.6.x after you upgrade to version 4.5.0. For details, see McAfee MOVE AntiVirus 4.5.0 Migration Guide.

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 McAfee MOVE AntiVirus extension file, then click OK.
5. After a confirmation message, click OK.

If you are upgrading from McAfee MOVE AntiVirus 4.0.0 and using Internet Explorer browser, refresh the policy pages or clear the cache files in the browser to update the policy pages to 4.5.0.

6. (For 3.5.x and 3.6.x only) Migrate your existing policies using the Migration Utility. For details, see McAfee MOVE AntiVirus 4.5.0 Migration Guide.

Deploy a new McAfee MOVE AntiVirus SVM manually

You can manually deploy McAfee MOVE AntiVirus SVM to each hypervisor.

Before you begin

Unregister the 4.0.0 McAfee MOVE AntiVirus SVM before deploying the new 4.5.0 SVM.

For a successful check-in, do not change the file name of the McAfee MOVE AntiVirus SVM package.

Task

1. From the McAfee download site, download MOVE-AV-AL_SVM_OVF_4.5.0.Zip
2. Log on to the existing McAfee MOVE AntiVirus SVM.
3. Run sudo /opt/McAfee/move/bin/sva-config.
4. Enter Yes to register or unregister this McAfee MOVE AntiVirus SVM with vCloud Networking and Security Manager.
Enter u to unregister.

Turn off the McAfee MOVE AntiVirus SVM.
Do not delete this McAfee MOVE AntiVirus SVM until the 4.5.0 version is successfully deployed. This MOVE AntiVirus SVM can be used to troubleshoot deployment issues.

Deploy a new McAfee MOVE AntiVirus SVM to the hypervisor.
For details about other methods to deploy the McAfee MOVE AntiVirus SVM, see Deploying McAfee MOVE AntiVirus (Agentless) in vCNS environment or Deploying McAfee MOVE AntiVirus (Agentless) in an NSX environment.

Run the sva-config script to register the SVM with vCloud Networking and Security Manager and McAfee ePO.

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

1 Log on to McAfee ePO as an administrator.

2 Select Menu | Systems | System Tree | Assigned Policies, then select MOVE AntiVirus 4.5.0.

   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 McAfee MOVE AntiVirus (Agentless) in an NSX environment
Use McAfee ePO and VMware vSphere Web Client to upgrade McAfee MOVE AntiVirus (Agentless) 3.5.x, 3.6.x, and 4.0.0 to McAfee MOVE AntiVirus 4.5.0.

Before you begin
- Your NSX Manager is registered with your vCenter account.
- You remove the existing dummy policy template that is included in the security policy.
- Use the Migration Utility to migrate the policies created in versions 3.5.x and 3.6.x before you upgrade the SVM. For details, see McAfee MOVE AntiVirus 4.5.0 Migration Guide.
McAfee MOVE AntiVirus 4.5.0 supports upgrading or migrating these components of 3.5.x, 3.6.x, and 4.0.0:

- McAfee MOVE AntiVirus (Agentless) extension
- NSX Manager details
- McAfee MOVE AntiVirus service
- McAfee MOVE AntiVirus SVM

**Task**

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

2. Select the security policy, which has the McAfee MOVE AntiVirus global policy, and click Actions | Edit | Guest Introspection Services, then delete McAfee MOVE AntiVirus global policy.
3. On McAfee ePO, upgrade the Cloud Workload Discovery and MOVE AntiVirus (Agentless) extensions to McAfee MOVE AntiVirus 4.5.0.

   Version 4.5.0 extension of Cloud Workload Discovery is a minimum requirement for upgrading to McAfee MOVE AntiVirus 4.5.0 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 Cloud Workload Discovery extension. You should then upgrade your McAfee MOVE AntiVirus (Agentless) extension.

4. Check in the McAfee MOVE AntiVirus SVM 4.5.0 package to McAfee ePO.
5. From McAfee ePO, select Menu | Automation | MOVE AntiVirus Deployment | Configuration | General and complete the common configuration.
6. On 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 McAfee MOVE AntiVirus SVM and click OK. The latest McAfee MOVE AntiVirus service is now registered with the vCenter account that is registered with NSX Manager.

The Upgrade option for McAfee MOVE AntiVirus service is available under Installation | Service Deployments in vSphere Web Client.

9. Verify that the McAfee MOVE AntiVirus 4.5.0 On Access 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 McAfee MOVE AntiVirus On Access 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 McAfee MOVE AntiVirus service using the Upgrade button available under Installation | Service Deployments in vSphere Web Client.
Upgrade McAfee MOVE AntiVirus in vCNS environment

Use McAfee ePO to upgrade McAfee MOVE AntiVirus (Agentless) 3.5.x, 3.6.x, and 4.0.0 to McAfee MOVE AntiVirus 4.5.0.

**Before you begin**
Use the Migration Utility to migrate the policies created in versions 3.5.x and 3.6.x before you upgrade the SVM. For details, see *McAfee MOVE AntiVirus 4.5.0 Migration Guide*.

McAfee MOVE AntiVirus 4.5.0 supports upgrading these components of 3.5.x, 3.6.x, and 4.0.0:

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

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

1. Upgrade the Cloud Workload Discovery and McAfee MOVE AntiVirus (Agentless) extensions to 4.5.0.

   Version 4.5.0 extension of Cloud Workload Discovery is a minimum requirement for upgrading to McAfee MOVE AntiVirus 4.5.0 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 Cloud Workload Discovery extension.

2. Check in the McAfee MOVE AntiVirus SVM 4.5.0 package to McAfee ePO.

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

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

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

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

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

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

Uninstalling McAfee MOVE AntiVirus (Agentless)

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

**Contents**

- Uninstalling McAfee MOVE AntiVirus (Agentless) 4.5.0 in an NSX environment
- Uninstalling McAfee MOVE AntiVirus (Agentless) in a vCNS environment
Uninstalling McAfee MOVE AntiVirus (Agentless) 4.5.0 in an NSX environment

A full uninstallation involves removing these components: McAfee MOVE AntiVirus service, McAfee MOVE AntiVirus SVM, NSX Manager details, and the McAfee MOVE AntiVirus extension.

Remove McAfee MOVE AntiVirus service from the cluster

Using the vSphere Web Client console, you can remove the McAfee MOVE AntiVirus 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 McAfee MOVE AntiVirus service is removed from all clusters.

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 AntiVirus Deployment | NSX Manager. 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 the McAfee MOVE AntiVirus Guest Introspection Service from the security policy

Remove the McAfee MOVE AntiVirus 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 McAfee MOVE AntiVirus Guest Introspection Service, then click the Delete icon.
5. Click Finish. This action removes the McAfee MOVE AntiVirus Guest Introspection Service.
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 | MOVE AntiVirus Deployment | NSX Manager. This action lists all NSX Managers registered in McAfee ePO.
3 Select the existing NSX Manager that you want to remove, then click Actions | Delete. A confirmation dialog box appears.
4 Click Yes to confirm.

Uninstall the extension
Uninstall the McAfee MOVE AntiVirus extensions 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 From the Extensions tab under McAfee group, select Data Center Security.
4 Click Remove next to each extension.

You must now uninstall both extensions for McAfee MOVE AntiVirus. MOVE AntiVirus extension must be removed first.

5 Delete reports and queries manually after uninstalling the extension.

Uninstalling McAfee MOVE AntiVirus (Agentless) in a vCNS environment
A full uninstallation involves removing these components: McAfee MOVE AntiVirus service, McAfee MOVE AntiVirus SVM, vShield Manager details, and the McAfee MOVE AntiVirus extensions.

Remove SVM using McAfee ePO
Using the McAfee ePO console, remove the McAfee MOVE AntiVirus SVM from one or more hypervisors.

Before you begin
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 AntiVirus Deployment.
3 On 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 McAfee MOVE AntiVirus SVM is already deployed.
   • vCenter Account — Displays the name of the VMware vCenter account that is registered with McAfee ePO.
   • SVM Version — Displays the McAfee MOVE AntiVirus SVM version.
4 From the Selection page, select the required hypervisors from where you want to remove the McAfee MOVE AntiVirus 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 McAfee MOVE AntiVirus SVM.
   • SVM VM Name — Displays the name of the McAfee MOVE AntiVirus SVM host.
   • Validation Status — Displays the validation status that specifies whether the McAfee MOVE AntiVirus SVM can be removed.
5 Click Remove to remove the McAfee MOVE AntiVirus SVM from the selected hypervisors.

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

**Table 3-11  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 McAfee MOVE AntiVirus SVM deployment started.</td>
</tr>
<tr>
<td>End Time</td>
<td>Indicates the date and time when the McAfee MOVE AntiVirus SVM deployment ended.</td>
</tr>
<tr>
<td>Deployment Type</td>
<td>Displays the McAfee MOVE AntiVirus 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 3-12  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 a McAfee MOVE AntiVirus 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 McAfee MOVE AntiVirus SVM.</td>
</tr>
<tr>
<td>Status</td>
<td>Specifies the task status such as Started, Completed, Failed, and Skipped.</td>
</tr>
<tr>
<td>Failure Reason</td>
<td>Specifies the reason for the failure of the task. Example:</td>
</tr>
<tr>
<td></td>
<td>• SVMs are still registered</td>
</tr>
<tr>
<td></td>
<td>• Returning DHCP IP is not applicable</td>
</tr>
</tbody>
</table>
### Table 3-12  Task status (continued)

<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 task started.</td>
</tr>
<tr>
<td>End Time</td>
<td>Indicates the date and time when the task ended.</td>
</tr>
</tbody>
</table>

**Uninstall the extension**

Uninstall the McAfee MOVE AntiVirus extensions 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. From the **Extensions** tab under **McAfee** group, select **Data Center Security**.
4. Click **Remove** next to each extension.
   - You must now uninstall both extensions for McAfee MOVE AntiVirus. MOVE AntiVirus extension must be removed first.
5. Delete reports and queries manually after uninstalling the extension.
Index

A
about this guide 7
account 20, 87
    NSX Manager 71
    registering 67
    VMware vCenter 67
    vShield Manager 91
agentless
    configuration 61
    deployment 65
    installation 61
assignment
    SVM Manager 29
assignment rules
    infrastructure group 38
ATD
    enabling and configuring 49
autoscaling
    configuring 39
    SVM 18

C
checking in
    SVM 90
client
    checking in 25
    creating uninstallation task 57
    deploy to XenDesktop 42
    deployment 25
    install manually 31
    removing 58
    uninstall task, create and assign 57
client tasks
    assign uninstall task 57
    assigning 24, 26
    create product deployment task 24, 26
    creating client uninstallation task 57
common configuration
    setting up 69, 89
configuration
    security tags 80
    tagging 82
    TIE and ATD 49
configuring
    IP Pool 90
    SVM template 32, 33
connector, choosing 20, 67, 87
conventions and icons used in this guide 7
creating SVM template 33

D
deployment
    McAfee ePO 86
    McAfee MOVE AntiVirus 25
    McAfee MOVE AntiVirus service 74
    MOVE AntiVirus service 65
    options 62
    overview 18, 65
    SVM 92
deployment type
    MOVE AntiVirus SVM 95
documentation
    audience for this guide 7
    product-specific, finding 8
typographical conventions and icons 7
download locations 14

E
editing registration
    NSX Manager 71
    vShield Manager 91
enabling option
    autoscale 39
    vApp 35
export utility
    OVF template 32
extension 61
extensions
    installing 19, 67, 86, 87, 99
    removing 104, 106
    uninstalling 58
    upgrading 53

H
hypervisors 20, 67, 87
uninstallation process 103 (continued)
  creating client uninstallation task 57
  extension 58
  McAfee MOVE AntiVirus 57, 104
upgrade scenarios
  ePolicy Orchestrator extension 53
  higher downtime scenario 55
  higher resource scenario 55
  non-persistent VM 55
  persistent VM 55
  strategy 53
  SVM 54
upgrade task
  manually 99
  SVM 99

V
vApp
  enabling 35
vApp options
  enabling 36
virtual machines
  boot status 20, 67, 87
virtual properties, displaying 20, 67, 87
VMware vCenter
  registering 86
VMware vCenter account
  defining 20, 67, 87
  registering 20, 67, 87
vShield Manager
  configuring and registering 86
  editing 91
X
XenDesktop
  deploy client 42

T
tags
  defining 20, 67, 87
technical support, finding product information 8
TIE
  enabling and configuring 49
  integrating 43

U
uninstallation process 103
  assign client task 57