Installation Guide

McAfee MOVE AntiVirus 4.6.0
COPYRIGHT
Copyright © 2017 McAfee, LLC

TRADEMARK ATTRIBUTIONS
McAfee and the McAfee logo, McAfee Active Protection, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundstone, McAfee LiveSafe, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, True Key, TrustedSource, VirusScan are trademarks or registered trademarks of McAfee, LLC 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

1 Planning your installation ........................................ 7
   System and hardware requirements ............................................ 7
   Supported McAfee management platform and software .................... 9
   Supported VMware management platform and software .................... 9
   Advantages of preconfiguring the product ............................. 11
   Are you ready to install? ..................................................... 11

2 Multi-Platform installation and configuration ...................... 13
   SVM assignment made easy .................................................. 13
      Multi-Platform deployment process using McAfee MOVE AntiVirus autoscaling with SVM Manager .......... 14
      Multi-Platform deployment process using McAfee ePO without SVM Manager ............................. 15
   Download software extensions and packages .............................. 16
      Check in the extensions and packages to McAfee ePO from the Software Manager ................. 16
   Install the product files on the management server ....................... 17
   Register a VMware vCenter account with McAfee ePO .................... 18
   Configure McAfee ePO details ............................................. 19
   Create or edit an infrastructure group in McAfee ePO for SVM Manager deployment ......................... 20
   Deploy the SVM Manager in VMware vCenter environment ................ 21
      Check in the SVM Manager OVF package using McAfee ePO ................................. 21
      Deploy the SVM Manager ................................................... 22
      Check the SVM Manager deployment status ................................ 23
   Deploy the SVM Manager in Hyper-V environment ......................... 25
   Set up the SVM Manager ................................................... 25
   Deploy the McAfee MOVE AntiVirus SVM ................................ 26
      Create an SVM deployment client task .................................... 26
      Assign an SVM deployment client task .................................. 27
      Configure VirusScan Enterprise policies for SVM ........................................... 27
   Assign the SVM Manager to an SVM ..................................... 28
   Configure an SVM assignment rule ....................................... 28
      Add or edit an SVM Manager assignment rule using IP address ................... 29
      Add or edit an SVM Manager assignment rule using McAfee ePO tag .................. 30
   Configuring an SVM OVF template for autoscaling ....................... 32
      Export an SVM OVF template ............................................ 32
      Check the SVM export status ............................................ 34
      Exporting an SVM OVF template using the export utility .................. 35
   Create or edit an infrastructure group in McAfee ePO for SVM autoscaling ..................................... 37
   Default rule vs custom rules (tag-based or IP-based) ...................... 39
   How autoscale SVM works ................................................. 40
   Enable and configure SVM autoscale settings ............................ 41
      Autoscale SVM details .................................................... 42
   Update the standby SVMs .................................................. 43
   Deploy the McAfee MOVE AntiVirus client ................................ 44
      Check the McAfee MOVE AntiVirus client deployment status .................. 45
   Generate certificates for McAfee MOVE AntiVirus ....................... 46
   Assign the SVM manually without SVM Manager ........................... 47
Deploy in a XenDesktop or VMware View environment ........................................ 47
Integrating TIE and Advanced Threat Defense .................................................. 48
   TIE and Advanced Threat Defense integration process .................................. 48
   Deploy the Data Exchange Layer client to McAfee MOVE AntiVirus SVM .......... 49
   Verify the TIE server installation ..................................................................... 49
   Create a new registered server ........................................................................ 50
   Enable TIE and Advanced Threat Defense protection for McAfee MOVE AntiVirus .... 50
   Verify the TIE server integration ..................................................................... 52
   Verify the Advanced Threat Defense integration ............................................ 52

3 Upgrading McAfee MOVE AntiVirus (Multi-Platform) ................................. 55
   Upgrading an existing version ......................................................................... 55
   Upgrade the extension ..................................................................................... 56
   Upgrade the SVM Manager ............................................................................. 56
   (If you are not using autoscale SVM) Upgrade the SVM with McAfee ePO .......... 57
   (If you are using autoscale SVM) Upgrade the SVM with McAfee ePO .......... 58
   Upgrade persistent virtual machines .............................................................. 59
   Upgrade non-persistent virtual machines ....................................................... 59
   Upgrade the McAfee MOVE AntiVirus client ............................................... 60

4 Uninstalling McAfee MOVE AntiVirus (Multi-Platform) .............................. 61
   Uninstall the client and SVM .......................................................................... 61
   Assign the uninstallation task to virtual systems ........................................... 62
   Remove the client or SVM package from McAfee ePO .................................... 62
   Remove the SVM Manager ............................................................................ 62
   Uninstall the extensions ................................................................................. 63

5 Agentless installation and configuration ......................................................... 65
   Advantages of using NSX Manager over vCNS ............................................... 65
   Setting up the SVM ........................................................................................ 66
   McAfee MOVE AntiVirus SVM deployment options ......................................... 66
   Download and check in software extensions and packages ........................... 66
   Check in the extensions and packages to McAfee ePO from the Software Manager .... 67
   Run security updates for McAfee MOVE AntiVirus SVM ............................... 67
   OVF properties .............................................................................................. 68
   Configure the SVM details in McAfee ePO ................................................... 69
   Deploying McAfee MOVE AntiVirus (Agentless) in an NSX environment .......... 70
   Deploying the McAfee MOVE AntiVirus service (NSX) .................................... 70
   Register vCenter Server with NSX Manager .................................................. 71
   Install the product files on the management server ........................................ 71
   Register a VMware vCenter account with McAfee ePO ............................... 72
   Set up a common configuration for deployment ............................................. 74
   Check in the McAfee MOVE AntiVirus SVM package to McAfee ePO .............. 74
   Validate your NSX Manager using McAfee ePO .......................................... 75
   Register the McAfee MOVE AntiVirus service with NSX Manager using McAfee ePO .... 76
   Deploy the McAfee MOVE AntiVirus service ................................................. 78
   Configuring the security group and security policy ....................................... 82
   Working with security tags ............................................................................ 85
   Service Composer scenarios .......................................................................... 86
   Deploying McAfee MOVE AntiVirus (Agentless) in vCNS environment ............ 91
   Deploying the McAfee MOVE AntiVirus service (vCNS) .................................. 91
   Install the product files on the management server ........................................ 91
   Register a VMware vCenter account with McAfee ePO ............................... 92
   Set up a common configuration for McAfee MOVE AntiVirus SVM deployment .... 93
   Check in the McAfee MOVE AntiVirus SVM package to McAfee ePO .............. 94
   Configure the IP Pool options ...................................................................... 95
6 Upgrading McAfee MOVE AntiVirus (Agentless) ............................................ 103
   Upgrading an existing version ...................................................................... 103
   Manually upgrade the McAfee MOVE AntiVirus SVM .................................. 104
   Upgrade the extension .................................................................................. 104
   Deploy a new McAfee MOVE AntiVirus SVM manually (version 4.0.0 only) .... 104
   Upgrade the McAfee MOVE AntiVirus SVM using the Debian package (version 4.5.0 only) .......................................................... 105
   Assign a policy .............................................................................................. 106
   Upgrade McAfee MOVE AntiVirus (Agentless) in an NSX environment ........... 106
   Upgrade McAfee MOVE AntiVirus in vCNS environment ............................... 107

7 Uninstalling McAfee MOVE AntiVirus (Agentless) ....................................... 109
   Uninstalling McAfee MOVE AntiVirus (Agentless) 4.5.1 in an NSX environment .......... 109
   Remove McAfee MOVE AntiVirus service from the cluster ............................ 109
   Unregister the VMware NSX Manager from McAfee ePO ............................. 109
   Remove the McAfee MOVE AntiVirus Guest Introspection Service from the security policy .............................................................. 110
   Remove NSX Manager details from McAfee ePO ........................................ 110
   Uninstall the extension .................................................................................. 110
   Uninstalling McAfee MOVE AntiVirus (Agentless) in a vCNS environment ........ 111
   Remove SVM using McAfee ePO .................................................................. 111
   Uninstall the extension .................................................................................. 112

Index ................................................................................................................. 113
Planning your installation

Your Security Virtual Machine (SVM) and virtual systems must have specific hardware and software to run McAfee® Management for Optimized Virtual Environments AntiVirus (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 ready to install?

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:

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Windows Server 2008 R2 SP1 (64-bit)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Windows Server 2008 SP2 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 R2 (64-bit)</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2016 (64-bit)</td>
</tr>
</tbody>
</table>

Make sure that the Windows security patches are up to date.

<table>
<thead>
<tr>
<th>CPU</th>
<th>CPU 4 vCPU, 2 GHz or higher</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory</td>
<td>6 GB RAM or higher</td>
</tr>
<tr>
<td>Hard disk space for SVM deployment</td>
<td>2 GB or higher</td>
</tr>
<tr>
<td>IP requirements</td>
<td>Static IP address (required for configuring policies with IP address)</td>
</tr>
</tbody>
</table>

McAfee MOVE AntiVirus requires Microsoft Visual C++ 2010 Runtime and it is bundled with SVM package.
SVM Manager details (Multi-Platform)

**Operating system**
Ubuntu 16.04

**Software**
- McAfee® Endpoint Security for Linux Threat Prevention
- McAfee Agent 5.0.5

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

All hypervisors are supported, but only those listed were tested.

**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 a 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 Endpoint Security for Linux Threat Prevention 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

  **Memory**
  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**
- Endpoint Security for Linux Threat Prevention
- McAfee Agent
- McAfee MOVE AntiVirus (Agentless)

Client system requirements

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

- McAfee MOVE AntiVirus requires Microsoft Visual C++ 2010 Runtime and it is bundled with client package.

  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)
(Agentless only) SLES 12 (64-bit)
(Agentless only) RHEL 7 (64-bit)
(Agentless only) Ubuntu 14.04 LTS (64-bit)

The minimum required version of VMware NSX Manager for Linux clients is 6.3.0.

## 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>McAfee ePO</td>
<td>5.1.3, 5.3.1, 5.3.2, or 5.9.0, 5.1.3, 5.3.1, 5.3.2, or 5.9.0</td>
</tr>
<tr>
<td>vSphere Connector</td>
<td>4.5.1 or later, 4.5.1 or later</td>
</tr>
<tr>
<td>McAfee Agent</td>
<td>5.0.3 or 5.0.4 (Version 5.0.4 is bundled with SVM package), 5.0.3, 5.0.4, 5.0.5, or 5.0.6 (Version 5.0.5 is bundled with SVM Manager package)</td>
</tr>
<tr>
<td>VirusScan Enterprise</td>
<td>NA, 8.8 or later</td>
</tr>
<tr>
<td>Endpoint Security for Linux Threat Prevention</td>
<td>10.2.0 (Part of SVM package), 10.2.0 (Part of SVM Manager package)</td>
</tr>
<tr>
<td>McAfee Threat Intelligence Exchange (TIE)</td>
<td>NA, 1.3.0, 2.0.0, or 2.1.0</td>
</tr>
<tr>
<td>McAfee Advanced Threat Defense</td>
<td>NA, 3.6.1, 3.6.2, 3.8.0, or 4.0.0</td>
</tr>
<tr>
<td>Virtual Advanced Threat Defense (vATD)</td>
<td>NA, 3.10</td>
</tr>
<tr>
<td>McAfee Data Exchange Layer (DXL)</td>
<td>NA, 2.0.1 or later</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>McAfee ePO</th>
<th>VMware vCloud Networking and Security Manager</th>
<th>VMware NSX Manager</th>
<th>VMware vCenter</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1.3, 5.3.1, 5.3.2</td>
<td>5.5.4</td>
<td>6.1.2 or later, 6.2.x, 6.3.x</td>
<td>5.5 u2 or later</td>
</tr>
<tr>
<td>5.9</td>
<td>5.5.4</td>
<td>6.2.4, 6.3.x</td>
<td>6.0 u2 or later</td>
</tr>
</tbody>
</table>
For information about the Guest VM operating systems that are supported for VMware vShield Endpoint, see the VMware documentation: https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1036847

For information about the Guest VM operating systems that are supported for NSX Manager, see the NSX Manager documentation: http://pubs.vmware.com/Release_Notes/en/nsx/6.3.0/releasenotes_nsx_vsphere_630.html#sysreqs

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</td>
<td>Configuration</td>
</tr>
<tr>
<td>Host</td>
<td>Configuration</td>
</tr>
<tr>
<td>Host</td>
<td>Configuration</td>
</tr>
<tr>
<td>Host</td>
<td>Configuration</td>
</tr>
<tr>
<td>Host</td>
<td>Configuration</td>
</tr>
<tr>
<td>Global</td>
<td>Licenses</td>
</tr>
<tr>
<td>Sessions</td>
<td>Validate session</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</td>
<td>Import</td>
</tr>
<tr>
<td>Datastore</td>
<td>Allocate Space</td>
</tr>
<tr>
<td>Network</td>
<td>Assign Network</td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>Configuration</td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>Interaction</td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>Interaction</td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>Configuration</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</td>
<td>Configuration</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>Virtual Machine</td>
<td>Interaction</td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>Guest Operations</td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>Guest Operations</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>Virtual Machine</td>
<td>Inventory</td>
</tr>
<tr>
<td>Note: To have permission to perform this operation, you must have this privilege assigned to both the object and its parent object.</td>
<td></td>
</tr>
</tbody>
</table>

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 when 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 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. |
| Management server | • Supported management platform is installed.  
• (Optional) You have preconfigured policy settings for product features. |
Planning your installation
Are you ready to install?
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
- Download software extensions and packages
- Install the product files on the management server
- Register a VMware vCenter account with McAfee ePO
- Configure McAfee ePO details
- Create or edit an infrastructure group in McAfee ePO for SVM Manager deployment
- Deploy the SVM Manager in VMware vCenter environment
- Deploy the SVM Manager in Hyper-V environment
- Set up the SVM Manager
- Deploy the McAfee MOVE AntiVirus SVM
- Assign the SVM Manager to an SVM
- Configure an SVM assignment rule
- Configuring an SVM OVF template for autoscaling
- Create or edit an infrastructure group in McAfee ePO for SVM autoscaling
- Default rule vs custom rules (tag-based or IP-based)
- Enable and configure SVM autoscale settings
- Update the standby SVMs
- Deploy the McAfee MOVE AntiVirus client
- Generate certificates for McAfee MOVE AntiVirus
- Assign the SVM manually without SVM Manager
- Deploy in a XenDesktop or VMware View environment
- Integrating TIE and Advanced Threat Defense

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. 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 turned off.
- **Ready** — Backup SVMs that are 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 turned 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 with SVM Manager**

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 the extensions on McAfee ePO.
2. Register a VMware vCenter account with McAfee ePO.
3. Install McAfee Agent on the endpoints.
4. Configure McAfee ePO details for deployment.
5. Create or edit the infrastructure group on McAfee ePO.
6. Deploy the SVM Manager.
7. Deploy the McAfee MOVE AntiVirus SVM.
8. Assign the SVM Manager to SVM.
9 Configure assignment rules in SVM Manager Settings policy.

10 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.

11 Create or edit the infrastructure group on McAfee ePO.

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

13 Deploy the McAfee MOVE AntiVirus client using McAfee ePO.

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 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. 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 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.

**Multi-Platform deployment process using McAfee ePO without SVM Manager**

The overall McAfee MOVE AntiVirus SVM deployment of the Multi-Platform consists of the following tasks.

1 Install the Meta Package on McAfee ePO.

2 Install McAfee Agent on the endpoints.

3 Deploy the McAfee MOVE AntiVirus SVM.

4 Deploy the McAfee MOVE AntiVirus client.

5 Configure the McAfee MOVE AntiVirus SVM details in the Options policy.
Download software extensions and packages

If you do not have Software Manager, you can download these software extensions and product packages to the McAfee ePO server from the McAfee download site.

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

<table>
<thead>
<tr>
<th>Package name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOVE-AV_Meta_Package_Ext.zip</td>
<td>This main extension includes these extensions:</td>
</tr>
<tr>
<td></td>
<td>• McAfee MOVE AntiVirus Common — Extension for product installation and deployment.</td>
</tr>
<tr>
<td></td>
<td>• McAfee MOVE AntiVirus — Extension for configuring and managing policies.</td>
</tr>
<tr>
<td></td>
<td>• McAfee MOVE AntiVirus License — License extension; upgrades evaluation extension to a fully licensed extension.</td>
</tr>
<tr>
<td></td>
<td>• vSphere Connector — Data Center discovery software.</td>
</tr>
<tr>
<td></td>
<td>• McAfee Data Center Control — It is a dependency software for vSphere Connector.</td>
</tr>
<tr>
<td></td>
<td>• Multi-Platform client package — It is a McAfee MOVE AntiVirus client package.</td>
</tr>
<tr>
<td></td>
<td>• Multi-Platform SVM package — It is a McAfee MOVE AntiVirus SVM package.</td>
</tr>
<tr>
<td></td>
<td>• Multi-Platform SVM Manager Debian package</td>
</tr>
<tr>
<td></td>
<td>• Product Help extension</td>
</tr>
<tr>
<td>MOVE-AV-MP_SVM_Manager_OVF_4.6.0.zip</td>
<td>Multi-Platform SVM Manager OVF package</td>
</tr>
<tr>
<td>MOVE-AV-MP_SVM_OVF_Export_Utility_4.6.0.zip</td>
<td>Multi-Platform SVM OVF export utility</td>
</tr>
</tbody>
</table>

Tasks

- Check in the extensions and packages to McAfee ePO from the Software Manager on page 16
  If you have Software Manager, you can check in the software extensions and packages to the Master Repository without downloading them.

Check in the extensions and packages to McAfee ePO from the Software Manager

If you have Software Manager, you can check in the software extensions and packages to the Master Repository without downloading them.

Task

1. Log on to McAfee ePO as an administrator.
2. Select Menu | Software, then click Software Manager.
3. From Software (by Label) | Endpoint Security, select these extensions, then click Check In.
### Product and Component

<table>
<thead>
<tr>
<th>Product</th>
<th>Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee MOVE AntiVirus 4.6.0</td>
<td>MOVE-AV_Meta_Package_Ext.zip</td>
</tr>
</tbody>
</table>

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.
- vSphere Connector — Data Center discovery software.
- McAfee Data Center Control — It is a dependency software for vSphere Connector.
- Multi-Platform client package — It is a McAfee MOVE AntiVirus client package.
- Multi-Platform SVM package — It is a McAfee MOVE AntiVirus SVM package.
- Multi-Platform SVM Manager Debian package
- Product Help extension

All extensions and packages are checked in to the Master Repository from the Software Manager.


See also

*Download software extensions and packages on page 16*

## Install the product files on the management server

The McAfee MOVE AntiVirus Meta Package and VirusScan Enterprise extensions 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.

VirusScan Enterprise is only licensed for the SVM, not for other Windows systems in your environment.

(Optional) Install the Endpoint Security for Linux Threat Prevention extension to manage the Endpoint Security for Linux Threat Prevention policy on the SVM Manager. Endpoint Security for Linux Threat Prevention is only licensed for the SVM Manager, not for other Linux systems in your environment.

Installing the McAfee MOVE AntiVirus Meta Package extension installs McAfee Data Center Control, vSphere Connector, and McAfee MOVE AntiVirus specific extensions (MOVE AntiVirus, MOVE AntiVirus Common, Product Help) on the McAfee ePO server. It also checks in the McAfee MOVE AntiVirus SVM and Client packages to the Master Repository.

### Task

1. Log on to McAfee ePO as an administrator.
2. Select **Menu | Software | Extensions | Install Extension.**
### Extension Package name

<table>
<thead>
<tr>
<th>Extension</th>
<th>Package name</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee MOVE AntiVirus Meta Package</td>
<td>MOVE-AV_Meta_Package_Ext.zip</td>
</tr>
</tbody>
</table>
| VirusScan Enterprise | • VIRUSCAN8800<XXX>.zip  <br>• VIRUSCANREPORTS120<XXX>.zip  <br>• epo45_help_vse_880.zip  

<i><XXX> is your build number.</i> |
| (Optional) Endpoint Security for Linux Threat Prevention | ISecTP-10.2.0-707-HF1177340-ePO.zip  

<i>To install this Hotfix, you must install Endpoint Security Platform and Endpoint Security Threat Prevention extensions. For details, see Endpoint Security for Linux Threat Prevention Product Guide.</i> |

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
- You configured your VMware vCenter server that manages the ESXi servers, which host the guest VMs.
- You installed the McAfee MOVE AntiVirus Meta Package extension on the McAfee ePO server.

#### Task
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, select **VMware vSphere**, then click **OK**.
4. On the **vCenter Account Details** page, configure these options.
   - **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).

<i>You must have a vCenter Server user account with administrator rights to use the autoscale feature.</i>
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.

**Configure McAfee ePO details**

Before deploying SVM Manager, you must configure McAfee ePO details on the McAfee ePO server, so that you can deploy the SVM Manager.

**Before you begin**

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

**Task**

1 Log on to McAfee ePO as an administrator.

2 Select Menu | Automation | MOVE AntiVirus Deployment.
3 On the Configuration tab, click General and enter and confirm the password for the McAfee ePO administrator.

4 Click Save to store these configurations.

Create or edit an infrastructure group in McAfee ePO for SVM Manager deployment

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

Before you begin
- You installed the McAfee MOVE AntiVirus Meta Package extension on the McAfee ePO server.
- You registered your VMware vCenter account with McAfee ePO.

You can deploy the SVM Manager to any infrastructure group using McAfee ePO. With the Infrastructure Details option, you can create or edit a hypervisor-based or cluster-based infrastructure group. You can then customize and select the infrastructure group for SVM Manager deployment.

You can include individual infrastructure groups for SVM Manager deployment.

Task
1 Log on to McAfee ePO as an administrator.

2 Select Menu | Automation | MOVE AntiVirus Deployment.

3 On the Configuration tab, click Infrastructure Details.

4 Edit the default infrastructure group options, as needed.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>The name of the infrastructure group.</td>
</tr>
<tr>
<td>Cloud Account Name</td>
<td>The name of the registered vCenter account.</td>
</tr>
<tr>
<td>ESXi / Cluster</td>
<td>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>The name of the DHCP or IP Pool used in the infrastructure group. By default, DHCP is selected.</td>
</tr>
<tr>
<td>Provisioning Type</td>
<td>The provisioning type as Thin or Thick.</td>
</tr>
<tr>
<td>Network Name</td>
<td>The name of the management network used by the group.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Datastore Name</td>
<td>The name of the datastore used by the infrastructure group. By default, the datastore with the most free space is selected.</td>
</tr>
<tr>
<td>Action</td>
<td>• <strong>Edit</strong> — Click to edit the infrastructure group properties, as needed. • <strong>Delete</strong> — Click to delete any unused infrastructure groups.</td>
</tr>
<tr>
<td></td>
<td><img src="https://example.com/notice.png" alt="" /> You can't delete the Default Group.</td>
</tr>
</tbody>
</table>

5 (Optional) Click **Actions** | **Create** and configure properties for the custom infrastructure group. You don't need to configure the custom group options 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 on your hypervisor or cluster. If you are selecting <strong>Cluster Based</strong>, make sure that you configured a distribution switch for the hypervisor, which are under the selected cluster.</td>
</tr>
<tr>
<td>Select Host / Select Cluster</td>
<td>Select the IP address of your host or cluster.</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 <strong>Static</strong> or <strong>DHCP</strong>.</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 <strong>Thin</strong> or <strong>Thick</strong>.</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>

6 Click **Save** to store the infrastructure group details.

---

**Deploy the SVM Manager in VMware vCenter environment**

**Contents**
- Check in the SVM Manager OVF package using McAfee ePO
- Deploy the SVM Manager
- Check the SVM Manager deployment status

**Check in the SVM Manager OVF package using McAfee ePO**

Check in the SVM Manager OVF package to the McAfee ePO server, so that McAfee ePO can deploy it to your hypervisor.

**Before you begin**
You installed the McAfee MOVE AntiVirus Meta Package extension on the McAfee ePO server.
Task
1. Log on to McAfee ePO as an administrator.
2. Select Menu | Automation | MOVE AntiVirus Deployment.
3. On the Configuration tab, click SVM Manager Configuration to open the SVM Manager OVF Details page with these SVM Manager options.

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVM Manager OVF Name</td>
<td>Name of the SVM Manager OVF package checked in to the McAfee ePO server.</td>
</tr>
<tr>
<td>SVM Manager OVF Version</td>
<td>Version of the SVM Manager OVF package checked in to the McAfee ePO server.</td>
</tr>
<tr>
<td>Action</td>
<td>Delete — To remove a checked in SVM Manager OVF.</td>
</tr>
</tbody>
</table>

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

5. Under SVM Manager OVF Check-in, configure these options:
   - Select SVM Manager OVF (zip) file to check-in — Browse to and select the SVM Manager OVF package (MOVE-AV-MP_SVM_Manager_OVF_4.6.0.zip).
   - Specify the location of McAfee ePO system — Specify the SVM Manager OVF package location on the McAfee ePO server (for example, C:\SVM Manager). The package is taken from this location during deployment to the hypervisor.

6. Click OK to check in the package.

The SVM Manager OVF package appears in the specified folder on the McAfee ePO server. Also, the SVM Manager details appear on the SVM Manager OVF Details page.

Deploy the SVM Manager
Using the McAfee ePO console, deploy the SVM Manager to your hypervisors, so that it automatically assigns the SVM to a group of clients.

Before you begin
- You installed the McAfee MOVE AntiVirus Meta Package extension on the McAfee ePO server.
- You registered your VMware vCenter account with McAfee ePO.
- Make sure that your VMware vCenter account is synced successfully.
- You configured your McAfee ePO details on the General page under Menu | Automation | MOVE AntiVirus Deployment | Configuration.
- You configured your Infrastructure Group.
- You checked in the SVM Manager OVF package to the McAfee ePO server.

Task
1. Log on to McAfee ePO as an administrator.
2. Select Menu | Automation | MOVE AntiVirus Deployment.
   The default password for the SVM Manager svaadmin account is Svaadmin$1
   You can change the password from the SVM Manager (Multi-Platform) Configuration option under Menu | Automation | MOVE AntiVirus Deployment | Configuration | General.
3. On the Configuration tab, click SVM Manager Configuration to open the SVM Manager OVF Details page.
4 Under **Deployment Configuration**, configure these options.
   - **Infrastructure Group** — Select the **Default Group** or an infrastructure group you created. The SVM Manager is deployed on this infrastructure group.
   - **Checked-in OVF** — Select the SVM Manager OVF package that is checked in to the McAfee ePO server.
   - **SVM Manager Settings policy** — Select the SVM Manager Settings policy, so that it is assigned to the SVM Manager.

5 Click **Deploy SVM Manager** to open the **Confirm SVM Manager Deployment** dialog box.

6 Click **OK** to deploy the SVM Manager.

On a successful deployment, an **SVM-Manager** VM is created on the configured infrastructure group. Now, the SVM Manager service can communicate with McAfee ePO through the McAfee Agent. Also, the selected SVM Manager Settings policy is applied to the SVM Manager.

**Check the SVM Manager deployment status**
After deploying the SVM Manager, you can view the deployment details on the **Deployment Status** tab under **MOVE AntiVirus Deployment** wizard on the McAfee ePO server.

**Before you begin**
- You installed the McAfee MOVE AntiVirus Meta Package extension on the McAfee ePO server.
- You initiated the SVM Manager deployment using McAfee ePO.

**Task**
1 Log on to McAfee ePO as an administrator.
2 Select **Menu | Automation | MOVE AntiVirus Deployment**.
On the **Deployment Status** tab, view the SVM Manager deployment details.

Click any SVM Manager deployment job to view these **Task Status Details**.

### Table 2-1  Deployment status

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

### Table 2-2  Task status

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

### Task type and status details

These are the task types that specify the internal tasks of a deployment job. The task list for one job is displayed in sequence with **Start Time**, **End Time**, and **Failure Reasons**, if applicable.

### Table 2-3  During SVM Manager deployment

<table>
<thead>
<tr>
<th>Task type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploying SVM Manager</td>
<td>Indicates that the SVM Manager deployment is in progress.</td>
</tr>
<tr>
<td>Powering on SVM Manager</td>
<td>Specifies that the SVM Manager is turned on.</td>
</tr>
<tr>
<td>Registering SVM Manager with McAfee ePO</td>
<td>Registers the SVM Manager with McAfee ePO.</td>
</tr>
<tr>
<td>Assigning SVM Manager Settings policy to the SVM Manager node</td>
<td>Assigns the SVM Manager Settings policy to the SVM Manager node.</td>
</tr>
</tbody>
</table>

### Table 2-4  During rollback

<table>
<thead>
<tr>
<th>Task type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rollback: Returning Static IP to IP Pool</td>
<td>(If Static IP Pool is used) Rolls back the static IP to IP Pool, which was assigned to the deployed SVM Manager. (If DHCP is used) This task is skipped.</td>
</tr>
<tr>
<td>Rollback: Powering off SVM Manager</td>
<td>Rolls back the <strong>Powering on SVM Manager</strong> task.</td>
</tr>
<tr>
<td>Rollback: Remove SVM Manager</td>
<td>Rolls back the <strong>Deploying SVM Manager</strong> task.</td>
</tr>
</tbody>
</table>
Deploy the SVM Manager in Hyper-V environment

To deploy the SVM Manager on Hyper-V, you must convert the .vmdk file, part of SVM Manager appliance, into a .vhd file.

Before you begin
Make sure the MOVE-AV-MP_SVM_Manager_OVF_4.6.0.zip file is in accessible location.

Task
1  Unzip the MOVE-AV-MP_SVM_Manager_OVF_4.6.0.zip file.
2  Using the Microsoft Virtual Machine Converter software, convert the .vmdk file into a .vhd file.
3  Attach the .vhd file as a hard disk to a new VM in Hyper-V.

Set up the SVM Manager

You must set up and configure the SVM Manager before deploying the SVM and assigning it to a group of clients. You can use this method for all type of hypervisors.

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_4.6.0) 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**

**Contents**
- Create an SVM deployment client task
- Assign an SVM deployment client task
- Configure VirusScan Enterprise policies for SVM

**Create an SVM deployment client task**
Create an SVM deployment client task, so that you can assign that task to virtual machines.

**Before you begin**
- You installed the McAfee MOVE AntiVirus Meta Package extension on the McAfee ePO server.
- The McAfee Agent and VirusScan Enterprise 8.8 are installed on the target virtual system.

**Task**
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 select **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 4.6.0** 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 an SVM deployment client task
After creating the SVM 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.

Task
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, then click Next.
6. 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.

Configure VirusScan Enterprise policies for SVM
You must configure VirusScan Enterprise policies and assign them to the McAfee MOVE AntiVirus SVM, so that the SVMs can protect the client systems.

Before you begin
• You installed the McAfee MOVE AntiVirus Meta Package extension on the McAfee ePO server.
• You deployed McAfee MOVE AntiVirus SVM to the target virtual system.
• You installed the VirusScan Enterprise 8.8 extension on the McAfee ePO server.

Task
1. Log on to McAfee ePO as an administrator.
2. Select Menu | Policy | Policy Catalog, select VirusScan Enterprise 8.8 from the Product drop-down list, then select On-Access Low-Risk Processes Policies from the Category drop-down list.
4. Open the duplicate On-Access Low-Risk Processes Policies policy and configure these options.
   • Settings for — Select Server.
   • From the Low-Risk Processes tab, add mvs.exe to the Low-Risk Processes list.
   • From the Scan Items tab, next to Scan files, disable When writing to disk and When reading from disk.
5. Click Save and assign the policy to the SVMs.
6. Select Menu | Policy | Policy Catalog, select VirusScan Enterprise 8.8 from the Product drop-down list, then select On-Access Default Processes Policies from the Category drop-down list.
7 Duplicate the On-Access Default Processes Policies policy.

8 Open the duplicate On-Access Default Processes Policies policy and configure these options.
   • Settings for — Select Server.
   • From the Low-Risk Processes tab, next to Process Settings, select Configure different scanning policies for high-risk, low-risk, and default processes.

9 Click Save and assign the policy to the SVMs.

**Assign the SVM Manager to an SVM**

Configure the SVM Manager details in McAfee MOVE AntiVirus Options policy and assign it to the SVMs, so that the SVM Manager and SVMs can communicate to each other.

**Before you begin**
- You installed the McAfee MOVE AntiVirus Meta Package extension on the McAfee ePO server.
- You deployed the McAfee MOVE AntiVirus SVM Manager.
- You deployed the McAfee MOVE AntiVirus SVM package to the target virtual systems.

**Task**

1 Log on to McAfee ePO as an administrator.

2 Click Menu | Policy | Policy Catalog, select MOVE AntiVirus 4.6.0 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.

5 Under SVM Assignment on the policy settings page, select Assign SVM using SVM Manager and configure the SVM Manager details, then click Save.
   • Enter the SVM Manager IP address or FQDN (domain name)
   • Enter the SVM Manager Port. Default is 8080.

6 Assign the configured policy to your SVMs.

The SVM Manager and the SVMs communicate, so that the clients can 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.

**Configure an SVM assignment rule**

**Contents**
- Add or edit an SVM Manager assignment rule using IP address
- Add or edit an SVM Manager assignment rule using McAfee ePO tag
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 multiple SVMs, so that those endpoints are protected by the SVM Manager assignment rule.

Before you begin

- You installed the McAfee MOVE AntiVirus Meta Package extension on the McAfee ePO server.
- You deployed the SVM Manager.
- You deployed the McAfee MOVE AntiVirus SVM package to the target virtual systems.

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

1. Log on to McAfee ePO as an administrator.
2. Select Menu | Policy | Policy Catalog, select MOVE AntiVirus 4.6.0 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, so that these endpoints can be protected by the SVM, which is specified in the SVM IP Address option.</td>
</tr>
<tr>
<td>SVM IP Addresses</td>
<td>Type the IP address of the SVM, so that this SVM can protect the endpoints, which are specified in the Client IP Address option.</td>
</tr>
</tbody>
</table>

If you are using the autoscale SVM feature, configure these settings.
For this option... | Do this...
---|---
Select and add to infrastructure groups | Select the Default Group or an infrastructure group you created using the Menu | Automation | MOVE AntiVirus Deployment | Configuration | Infrastructure Details option, so that SVM deployment can be done to a specific infrastructure group in your organization.

Customize SVM Settings | This is the SVM assignment rule specific to autoscale settings. 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.
- **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 McAfee MOVE AntiVirus SVMs automatically scale up and down depending on the number of endpoints connected.

Alarms | 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.

---

6 (Optional) Select **Enable to get SVM preference from the same subnet** to assign an SVM from the same subnet. For details, see *SVM preference*.

7 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 Meta Package extension on the McAfee ePO server.
- You deployed the SVM Manager.
- You deployed the McAfee MOVE AntiVirus SVM package to the target virtual systems.

**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 take priority over IP-based assignment rules.

**Task**
1 Log on to McAfee ePO as an administrator.
2 Select **Menu | Policy | Policy Catalog**, select MOVE AntiVirus 4.6.0 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 McAfee ePO tag names of the endpoints, so that these endpoints can</td>
</tr>
<tr>
<td></td>
<td>be protected by the SVM, which is specified in the Select and add to SVM tags option.</td>
</tr>
<tr>
<td>Select and add to SVM tags</td>
<td>Select the McAfee ePO tag name of the SVM, so that this SVM can protect the</td>
</tr>
<tr>
<td></td>
<td>endpoints, which are specified in the Select and add to client tags option.</td>
</tr>
</tbody>
</table>

If you are using the autoscale SVM feature, configure these settings.

<table>
<thead>
<tr>
<th>For this option...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select and add to infrastructure groups</td>
<td>Select the Default Group or an infrastructure group you created using the Menu</td>
</tr>
<tr>
<td>Customize SVM settings</td>
<td>This is the SVM assignment rule specific to autoscale settings. 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>Number of backup SVMs — Type the number of ready SVMs required for protecting 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.</td>
<td></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 (Optional) Select Enable to get SVM preference from the same subnet to assign an SVM from the same subnet. For details, see SVM preference.

7 Click OK to save your changes.

**SVM preference**

Selecting the Enable to get SVM preference from the same subnet option, you can assign an SVM to the clients from the same subnet when clients migrate from one hypervisor to another. You must define tag or IP-based rules specifying the SVM's IP address or tag of respective hypervisor/subnet.

For example, consider a scenario where:

• SVM-1, SVM-2, and SVM-3 are in ESXi-1, ESXi-2, and ESXi-3 servers respectively
• You have a client that keeps migrating from one hypervisor to another
• You want to protect the client by an SVM that belongs to the same subnet

With these assumptions, selecting the Enable to get SVM preference from the same subnet option, when the client migrates from one hypervisor to another, it is protected from an SVM that belongs to the same subnet.
Configuring an SVM OVF template for autoscaling

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 an SVM, you create a copy of the entire virtual machine, including its settings, installed software, and other configuration settings. 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 you 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.

You can configure an SVM OVF template using one of these options:

- **Export an existing SVM or create and export from a VM** — You can export a template from an SVM system or can create an SVM and export it to make a master image of the SVM, from which you can deploy many SVMs.

- **Specify the SVM OVF location available on the McAfee ePO system** — You can export an SVM OVF template using the export utility, then copy the exported SVM OVF template to the McAfee ePO server. Then specify the location of the SVM OVF template that is available on the McAfee ePO server, so that McAfee MOVE AntiVirus can deploy SVMs, as needed.

**See also**
- Export an SVM OVF template on page 32
- Exporting an SVM OVF template using the export utility on page 35

**Export an SVM OVF template**

Using the **Export an existing SVM or create and export from a VM** option, you can export a template from an SVM system or can create an SVM system, then export it to make a master image of an SVM, from which you can deploy...
many SVMs. When you use this option, McAfee MOVE AntiVirus installs VirusScan Enterprise and the SVM package (if they are not installed) on the VM, then exports it to the McAfee ePO server.

**Before you begin**

- You installed the McAfee MOVE AntiVirus 4.6.0 Meta Package extension on the McAfee ePO server.
- Make sure that your VMware vCenter account is synced successfully.
- (If you are creating and exporting from a VM) You have a VM with one of these Plain Vanilla Windows Server platforms: 2008 R2 SP1 (64-bit), 2008 SP2 (64-bit), 2012 R2 (64-bit), or 2016 (64-bit).
- (If you are exporting from an existing SVM) Make sure that the SVM package is upgraded to 4.6.0.
- The latest VMware Tools are installed on the VM: `C:\Program Files\VMware\VMware Tools \vmtoolsd.exe`.
- The VM is managed by McAfee ePO.
- The VM has no snapshots.
- The VM has only one hard disk.
- The VM is turned on.
- (If your environment includes more than one domain) Make sure that the VM is not part of any domain, so that the exported SVM template is a generic one and can be deployed to any domain.
- Do not configure the SVM Manager IP details under **SVM Manager Assignment** in **Options** policy until you create and export the SVM template.

**Task**

1. Log on to McAfee ePO as an administrator.
2. Select **Menu** | **Automation** | **MOVE AntiVirus Deployment**.
3. On the **Configuration** tab, under **Multi-Platform**, click **SVM Configuration** to open the **SVM OVF Details** page with these SVM OVF details and actions.

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVM OVF Name</td>
<td>Name of the McAfee MOVE AntiVirus SVM OVF template checked in to McAfee ePO.</td>
</tr>
<tr>
<td>SVM OVF Version</td>
<td>Version of the McAfee MOVE AntiVirus SVM OVF template checked in to McAfee ePO.</td>
</tr>
<tr>
<td>SVM OVF Use Count</td>
<td>Specifies the number of SVMs that are deployed for SVM autoscaling.</td>
</tr>
<tr>
<td>Action</td>
<td><strong>Delete</strong> — To remove an existing McAfee MOVE AntiVirus SVM OVF when it is not deployed to any hypervisor. You can delete the SVM OVF only when the SVM OVF Use Count is 0.</td>
</tr>
</tbody>
</table>

4. Click **Actions** | **Add SVM** to open the **Configure SVM OVF** page.
5 Under Configure SVM OVF template, select Export an existing SVM or create and export from a VM and configure these options.

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registered Cloud Account</td>
<td>Select a VMware vCenter account where the VM is present.</td>
</tr>
<tr>
<td>VM Name</td>
<td>Type the name of the VM.</td>
</tr>
<tr>
<td>Username</td>
<td>Type the user name of the VM.</td>
</tr>
<tr>
<td>Password</td>
<td>Type the password of the VM.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Retype the password.</td>
</tr>
<tr>
<td>SVM Location on McAfee ePO</td>
<td>Specify the location on the McAfee ePO server. This location is used to store the exported SVM OVF template.</td>
</tr>
<tr>
<td>SVM OVF Version</td>
<td>Type a version for the SVM OVF template, for example, 4.6.0.</td>
</tr>
<tr>
<td>SVM OVF Name</td>
<td>Type a name for the SVM OVF template, for example, ESVM 4.6.0.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Type details about the SVM OVF template, to help identify the SVM OVF template.</td>
</tr>
</tbody>
</table>

6 Click Export to open the Export SVM OVF Confirmation dialog box.

7 Click OK to create an SVM system and export it to make an SVM OVF template.

The SVM OVF template files (*.ovf and *.vmdk) are created on the McAfee ePO server. Also, the exported SVM OVF template details are available on the SVM OVF Repository page under MOVE AntiVirus Deployment | Configuration | Multi-Platform | SVM Configuration.

Check the SVM export status

After exporting an SVM, you can view the export details on the Deployment Status tab under MOVE AntiVirus Deployment wizard on the McAfee ePO server.

**Before you begin**

You initiated an SVM export using McAfee ePO.

**Task**

1 Log on to McAfee ePO as an administrator.

2 Select Menu | Automation | MOVE AntiVirus Deployment.
On the Deployment Status tab, view the SVM export details.

Click any Export SVM OVF template job to view these Task Status Details.

### Table 2-5 Deployment status

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypervisors/Hostname</td>
<td>Specifies the host name of the SVM.</td>
</tr>
<tr>
<td>vCenter Name/IP address</td>
<td>Specifies the name of the VMware vCenter account that is registered with McAfee ePO.</td>
</tr>
<tr>
<td>Deployment Type</td>
<td>Displays the deployment type as Export SVM OVF template.</td>
</tr>
<tr>
<td>Status</td>
<td>Specifies the deployment status such as Started, In Progress, Completed, and Failed.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Indicates the date and time when the SVM export job started.</td>
</tr>
<tr>
<td>End Time</td>
<td>Indicates the date and time when the SVM export job ended.</td>
</tr>
</tbody>
</table>

### Table 2-6 Task status

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node Type</td>
<td>Specifies whether the node is an SVM or endpoint.</td>
</tr>
<tr>
<td>Task Type</td>
<td>Specifies the set of internal tasks in an SVM export job. The task list for one job is displayed in sequence with Start Time, End Time, and Failure Reasons, if applicable.</td>
</tr>
<tr>
<td>Node Name</td>
<td>Displays the name of the VM.</td>
</tr>
<tr>
<td>Status</td>
<td>Specifies the task status: Started, In Progress, Completed, Skipped, and Failed.</td>
</tr>
<tr>
<td>Failure Reason</td>
<td>Specifies the reason for the failure of the task.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Indicates the date and time when the task started.</td>
</tr>
<tr>
<td>End Time</td>
<td>Indicates the date and time when the task ended.</td>
</tr>
</tbody>
</table>

### Exporting an SVM OVF template using the export utility

You can export an SVM OVF template using the export utility, then copy the exported SVM OVF template to the McAfee ePO server.

Then you can specify the location of the SVM OVF template that is available on the McAfee ePO server, so that McAfee MOVE AntiVirus can deploy SVMs, as needed.

### 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 has no snapshots.
- (If more than one domain is there in your environment) 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 to any domain.
- Do not configure the SVM Manager IP details under SVM Manager Assignment in Options policy until you create and export the SVM template.
Task
1. Create an SVM.
   - Use the static IP address for the SVM where 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 where you take the template.

3. Copy and extract the MOVE-AV-MP_SVM_OVF_Export_Utility_4.6.0.zip file to any Windows system. These two files are present in the extracted MOVE-AV-MP_SVM_OVF_Export_Utility_4.6.0.zip folder:
   - config.ini
   - svm-export.exe
   - Do not change the script files in the Autoconfig_scripts folder. If you do so, script does not run.

4. Using any word editor, open the config.ini file and configure these settings:
   - [vcenter-info]
     - vCenter host name/IP address
     - vCenter user name
     - vCenter password
   - [svm-info]
     - SVM name as displayed in vCenter
     - User name and password of SVM, which is created in step 1. This user account must have local administrator rights.
   - [ovf-info]
     - The directory where the exported SVM OVF template is saved.

5. Double-click the svm-export.exe file to run the program.
   A command-line window displays 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.

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

Before you begin
- You installed the McAfee MOVE AntiVirus Meta Package extension on the McAfee ePO server.
- The exported SVM OVF template is copied to the system where your McAfee ePO server is installed.
Task
1. Log on to McAfee ePO as an administrator.
2. Select Menu | Automation | MOVE AntiVirus Deployment.
3. On the Configuration tab, under Multi-Platform, click SVM Configuration to open the SVM OVF Details page with these SVM details and actions:

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVM OVF Name</td>
<td>Name of the McAfee MOVE AntiVirus SVM package checked in to McAfee ePO.</td>
</tr>
<tr>
<td>SVM OVF Version</td>
<td>Version of the McAfee MOVE AntiVirus SVM package checked in to McAfee ePO.</td>
</tr>
<tr>
<td>SVM OVF Use Count</td>
<td>Specifies the number of SVMs that 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. You can delete the SVM only when the SVM Use Count is 0.</td>
</tr>
</tbody>
</table>

4. Click Actions | Add SVM to open the Configure SVM OVF page.
5. Under Configure SVM OVF template, select Specify the SVM OVF location available on the McAfee ePO system and configure these options, then click OK.

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVM Location on McAfee ePO</td>
<td>Specify the location on the McAfee ePO server. This location is used to store the exported template.</td>
</tr>
<tr>
<td>SVM OVF Version</td>
<td>Specify the version of the template, for example, 4.6.0.</td>
</tr>
<tr>
<td>SVM OVF Name</td>
<td>Specify the name of the template, for example, ESVM 4.6.0.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Type details about the template, to help identify the SVM OVF template.</td>
</tr>
</tbody>
</table>

The SVM OVF package is taken from this location during the deployment to the hypervisor.

Create or edit an infrastructure group in McAfee ePO for SVM autoscaling

After registering your vCenter account, your default group is added to the MOVE AntiVirus Deployment wizard when you access the Infrastructure Details option under Multi-Platform. 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 Multi-Platform.

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. You can select and include individual infrastructure groups for SVM deployment.
Task
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></td>
<td>The name of the default group can't be edited.</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></td>
<td>If you are selecting Infrastructure Type as Cluster Based, make sure that you configured a distribution switch for the hypervisors, which are under the selected cluster.</td>
</tr>
<tr>
<td>IP Pool Name</td>
<td>Specifies the name of the DHCP or IP Pool used in the infrastructure group. By default, DHCP is selected.</td>
</tr>
<tr>
<td></td>
<td>To configure AD server, Static IP Pool must be selected.</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. By default, the datastore with the most free space is selected.</td>
</tr>
<tr>
<td>Action</td>
<td>• Edit — Click to edit the infrastructure group properties, as needed.</td>
</tr>
<tr>
<td></td>
<td>• Delete — Click to delete any unused infrastructure groups.</td>
</tr>
<tr>
<td></td>
<td>You can't delete the Default Group.</td>
</tr>
</tbody>
</table>
4 Click Actions | Create and configure these properties for the custom infrastructure group details. You don’t need 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></td>
<td>If you are selecting Cluster Based, make sure that you configured a distribution switch for the hypervisor, which are under the selected cluster.</td>
</tr>
<tr>
<td>Select Host (Cluster)</td>
<td>Select the IP address of your host or cluster.</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.

**Default rule vs custom rules (tag-based or IP-based)**

After registering your vCenter account, your default infrastructure group is added to the MOVE AntiVirus Deployment wizard when you access the Infrastructure Details option under Multi-Platform.

Based on the specified SVMs value under Customize SVM Settings, a default SVM pool is created, then Ready and Standby SVMs are deployed to the default infrastructure group for the default SVM assignment rule.

When you create SVM assignment rules (tag-based or IP-based), you can specify the number of backup SVMs for the rule, then new SVMs are deployed to the selected infrastructure group. The infrastructure group can be default group or user-defined group.

The clients that are not under a tag-based or IP-based rule are protected by the default SVM pool corresponding to the default SVM assignment rule.

- If you bring up the client system that is not part of the SVM assignment rules (tag-based or IP-based), the client system is protected by the SVM pool that is created for the default SVM assignment rule.

- If you bring up the client system that is part of the SVM assignment rules (tag-based or IP-based), the client system is protected by the SVM pool that is created for the custom SVM assignment rule.

Creating more rules consumes more computing resources for deploying SVMs. For example, if you create 10 SVM assignment rules (tag-based or IP-based) specifying backup SVMs as 2, then 2 Ready and 1 Standby SVMs are deployed for each rule.
**How autoscale SVM works**

A default infrastructure group is added to the MOVE AntiVirus Deployment wizard when you access the Infrastructure Details option under Multi-Platform.

When you enable the autoscale SVM feature, based on the specified SVM’s value under Customize SVM Settings, a default SVM pool is created then Ready and Standby SVMs are deployed to the default infrastructure group for the default SVM assignment rule (The SVM assignment rule is created by default for the clients that are not part of user-defined SVM assignment rules. The default SVM assignment rule does not appear on the McAfee ePO page).

For user-defined SVM assignment rule, the number of backup SVMs can be specified on the Add/Edit SVM Tag Assignment Rule or Add/Edit SVM IP Assignment Rule dialog box under Customize SVM Settings.

**Example 1**

Consider a scenario where:
- The number of clients — X
- The number of Ready SVMs specified in McAfee ePO — Y
- The number of Standby SVMs — Z

Depending on the value Y, the time it takes to start protecting the X number of clients varies. If the value of Y is less (considering each SVM protects 250 clients), then for the first time, it takes more time to protect the X clients because that number of required SVMs must be deployed. But eventually all X clients are protected.

You can also bring all these X clients to the McAfee MOVE AntiVirus environment in different batches. For example, if you have 10000 clients in your environment, you can bring them in 2 batches (5000 clients in each batch), so that there is no gap in protecting the clients by SVMs.

**Example 2**

Consider a scenario where:
- The total number of client systems — 15000
- The number of static client systems (All time turned on) — 6000
- The number of dynamic clients (Keep turned on and off when needed) — 9000
  These 9000 clients are part of 3 SVM assignment rules (a default, one tag-based, and one IP-based rule) — 3000 client systems per each rule
- The number of client systems with a tag-based SVM assignment rule — 3000
- The number of client systems with an IP-based SVM assignment rule — 3000
- The number of client systems with a default SVM assignment rule — 9000 (3000 dynamic and 6000 static)

These 9000 dynamic client systems need immediate protection when they are up and running. These 9000 dynamic client systems can be protected by using the autoscale SVM feature.

You configured the number of Ready SVMs as 4 and the number of Standby SVMs as 2 for each SVM assignment rule (default, tag-based, and IP-based) to protect these 9000 dynamic client systems.

With these 4 Ready and 2 Standby SVMs, dynamic and static client systems must be protected.
Protecting dynamic client systems

• During the peak time, say 9000 client systems are up and running, then first 3000 clients (1000 clients per each rule) are protected immediately [As the 12 Ready SVMs (4 Ready SVMs of each rule) would immediately transition to Running state and protect the first 3000 clients]. But for next 6000 dynamic clients, the new Ready SVMs need to be deployed and they keep transitioning from Standby -> Ready -> Running state depending on the client load. It takes some time to protect these 6000 dynamic client systems. So to keep protecting the total 9000 dynamic clients, 36 Running SVMs (12 SVMs per each rule) are required.

• When clients systems are turned off, the corresponding Running SVMs are transitioned to Standby state so that the computing resources are saved.

Protecting static client systems

These 6000 static clients are protected by the respective SVM pool that is created for the corresponding SVM assignment rule (default, tag-based, and IP-based).

• To protect 6000 static client systems, 24 Running SVMs (6000/250 = 24 Running SVMs) are required.

• These initial 24 Running SVMs creation takes some time, as this is an initial setup and fresh Ready and Standby SVMs need to be deployed. The transition from Standby -> Ready -> Running happens in phase by phase manner. But eventually all X clients are protected.

To protect 12,000 static clients at once, you can also bring all these 12,000 clients to the McAfee MOVE AntiVirus environment in different batches, for example, you can bring them in 12 batches (1000 clients per batch) so that there is no gap in protecting the clients by SVMs.

Enable and configure SVM autoscale settings

Create and assign a policy that specifies which SVM an infrastructure group uses.

Before you begin

You can define the autoscale settings for the McAfee MOVE AntiVirus SVM so that its deployment starts automatically, depending on the number of clients connecting to it for protection.

• You installed the McAfee MOVE AntiVirus Meta Package extension on the McAfee ePO server.

• You configured your McAfee ePO details on the General page under Automation | MOVE AntiVirus Deployment | Configuration.

• You deployed the SVM Manager.

• You exported an SVM OVF template.

• (If you exported an SVM OVF using export utility tool) You specified the McAfee MOVE AntiVirus SVM OVF template path in McAfee ePO.

• You configured the VirusScan Enterprise policies for the SVM on the McAfee ePO server. For details, see Configure VirusScan Enterprise policies for SVM.

You can track the status of the SVM deployment on the Deployment Status page on the McAfee ePO server.

Task

1 Log on to McAfee ePO as an administrator.

2 Select Menu | Policy | Policy Catalog, select MOVE AntiVirus 4.6.0 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.
   - SVM Port — Specify the port for the SVM to communicate to SVM Manager. Default is 8443.
   - Client Port — Specify the port for the client system to communicate to SVM Manager. Default is 8080.

6 From SVM Autoscale Settings, select Enable auto scaling of SVMs.
   Enabling the Enable auto scaling of SVMs option deletes all manually deployed SVMs after the new SVMs are deployed. The new SVMs are ready to protect the client systems. Disabling the Enable auto scaling of SVMs option deletes all ready and standby SVMs, but the running SVMs continue to protect the client systems.

7 Under SVM Autoscale Settings, 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. The backup SVMs are the ready SVMs, which enable faster protection for new client systems that might be added during peak hours or during a cloud burst.
   - 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.
    
8 Click Show Advanced and configure the Assignment Rules options as needed, then click Save.

See also
Configure VirusScan Enterprise policies for SVM on page 27

Autoscale SVM details
When you define the autoscale SVM 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 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>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 multiple 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>
</tbody>
</table>
### SVM Mode

Specifies the mode of the deployed SVM:

- **Standby** — Standby SVMs are created and 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.

- **Ready** — 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. These SVMs are powered on, but are not protecting the client systems.

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

### SVM Status

Specifies whether the SVMs are running.

### Action

- **Delete** — Deletes the selected SVMs.

- **Upgrade Standby SVMs** — Removes the existing standby SVMs and deploys the new standby SVMs with the latest OVF template.

## Update the standby SVMs

When the latest SVM OVF template is configured in McAfee ePO, you can deploy it from McAfee ePO to all standby SVMs. This is only true for standby SVMs, not for ready and running SVMs.

**Before you begin**

You created your latest SVM OVF template.

When you click **Update Standby SVMs**, the existing standby SVMs are purged and new standby SVMs are deployed.

When you define the 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 SVM deployment mode, its status, and the purging details on the **Autoscale SVM Details** page.

**Task**

1. Log on to McAfee ePO as an administrator.
2. Select **Menu | Automation | MOVE AntiVirus Deployment**.
3. On the **Configuration** tab, click **Autoscale SVM Details** to open the **Autoscale SVM Details** page with the autoscale SVM deployment details.
4. Click **Actions | Update Standby SVMs**.

This action removes the existing standby SVMs and deploys the new standby SVMs with the latest SVM OVF template.
Deploy the McAfee MOVE AntiVirus client

Deploy the client package to virtual machines using McAfee ePO, so that McAfee ePO can manage the McAfee MOVE AntiVirus configuration on client systems.

Before you begin

- The McAfee Agent must already be deployed to target virtual systems.
- You installed the McAfee MOVE AntiVirus Meta Package extension on the McAfee ePO server.
- Make sure that your VMware vCenter account is synced successfully.
- You deployed the SVM Manager using McAfee ePO.
- (If you are using autoscale SVM) You exported an SVM OVF template and configured SVM autoscale settings.
- (If you are not using autoscale SVM) You deployed the McAfee MOVE AntiVirus SVM package to target virtual systems.
- Make sure that the SVMs are communicating with the SVM Manager and are ready to protect new clients.
- Make sure that your virtual machines are turned on where you want to deploy McAfee MOVE AntiVirus client.

Task

1. Log on to McAfee ePO as an administrator.
2. Select **Menu | Systems | System Tree**.
3. In the **System Tree**, select the virtual machines where you want to deploy the client package.
4. From **Actions**, select **MOVE | Deploy Client [Multi-Platform]** to open the **Client Deployment Configuration** page.
5. Under **Client Configuration** for **Client Package**, select **MOVE AV [Multi-Platform] Client 4.6.0**.
   You can view all the SVM Assignment Rules, if the selected client systems are part of the assignment rules.
6. Click **Proceed** to open the **Deployment Confirmation** dialog box.
   A message shows the number of systems that are compatible and non-compatible for the client deployment.
7. Review the message, then click **OK** to deploy the client package to the compatible client systems.
   A deployment task is created for all selected systems. Go to **Deployment Status** tab under the **MOVE AntiVirus Deployment** wizard to view the **Passed** or **Failed** tasks with their details.
   If you click **Cancel**, the deployment task is created only for the non-compatible client systems, and the failure reasons can be viewed on the **Deployment Status** tab under the **MOVE AntiVirus Deployment** wizard.

For compatible client systems, the SVM Manager IP address is updated in the respective **Options** policy, then the SVM Manager assigns an SVM for the clients to protect them.

Tasks

- **Check the McAfee MOVE AntiVirus client deployment status on page 45**
  After deploying McAfee MOVE AntiVirus client, you can view the deployment details on the **Deployment Status** tab under **MOVE AntiVirus Deployment** wizard on the McAfee ePO server.
Check the McAfee MOVE AntiVirus client deployment status
After deploying McAfee MOVE AntiVirus client, you can view the deployment details on the Deployment Status tab under MOVE AntiVirus Deployment wizard on the McAfee ePO server.

**Before you begin**
- You installed the McAfee MOVE AntiVirus Meta Package extension on the McAfee ePO server.
- You initiated the McAfee MOVE AntiVirus client deployment using McAfee ePO.

**Task**
1. Log on to McAfee ePO as an administrator.
2. Select **Menu | Automation | MOVE AntiVirus Deployment**.
3. On the Deployment Status tab, you can view the McAfee MOVE AntiVirus client deployment details.
4. Click any of the **Deploy client and enable protection** jobs to view these Task Status Details.

**Table 2-7 Job status**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypervisors/Hostname</td>
<td>Specifies the host name of the McAfee MOVE AntiVirus client system.</td>
</tr>
<tr>
<td>vCenter Name/IP address</td>
<td>Specifies the IP address of the McAfee MOVE AntiVirus client system.</td>
</tr>
<tr>
<td>Deployment Type</td>
<td>Displays the McAfee MOVE AntiVirus client deployment type as <strong>Deploy client and enable protection</strong>.</td>
</tr>
<tr>
<td>Status</td>
<td>Specifies the deployment status such as <strong>Started</strong>, <strong>In Progress</strong>, <strong>Completed</strong>, and <strong>Failed</strong>.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Indicates the date and time when the McAfee MOVE AntiVirus client deployment started.</td>
</tr>
<tr>
<td>End Time</td>
<td>Indicates the date and time when the McAfee MOVE AntiVirus client deployment ended.</td>
</tr>
</tbody>
</table>

**Table 2-8 Task status**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node Type</td>
<td>Specifies the node type as <strong>Endpoint</strong>.</td>
</tr>
<tr>
<td>Task Type</td>
<td>Specifies the set of internal tasks that happen in a deployment job. The task list for one job is displayed in sequence with <strong>Start Time</strong>, <strong>End Time</strong>, and <strong>Failure Reasons</strong>, if applicable.</td>
</tr>
<tr>
<td>Node Name</td>
<td>Displays the host name of the McAfee MOVE AntiVirus client system.</td>
</tr>
<tr>
<td>Status</td>
<td>Specifies the task status such as <strong>Started</strong>, <strong>In Progress</strong>, <strong>Completed</strong>, <strong>Skipped</strong>, and <strong>Failed</strong>.</td>
</tr>
<tr>
<td>Failure Reason</td>
<td>Specifies the reason for the failure of the task.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Indicates the date and time when the task started.</td>
</tr>
<tr>
<td>End Time</td>
<td>Indicates the date and time when the task ended.</td>
</tr>
</tbody>
</table>
**Task type and status details**

These are the task types that specify the internal tasks of a deployment 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>Task type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploying client</td>
<td>Indicates that the McAfee MOVE AntiVirus client deployment is in progress.</td>
</tr>
<tr>
<td>Updating Options policy</td>
<td>Updates the IP address of the SVM Manager in the respective Options policies that are assigned to the clients.</td>
</tr>
<tr>
<td>Connecting to SVM Manager</td>
<td>Specifies that the McAfee MOVE AntiVirus client is communicating to the SVM Manager.</td>
</tr>
<tr>
<td>Assigning SVM to endpoint</td>
<td>Assigns the McAfee MOVE AntiVirus SVM to the client system.</td>
</tr>
<tr>
<td>Connecting to SVM</td>
<td>Specifies that the client is communicating to the McAfee MOVE AntiVirus SVM.</td>
</tr>
<tr>
<td>Testing EICAR</td>
<td>Tests EICAR on the McAfee MOVE AntiVirus client system on which the McAfee MOVE AntiVirus client deployment is successful.</td>
</tr>
</tbody>
</table>

**Generate certificates for McAfee MOVE AntiVirus**

If there is a connectivity issue with the SVM Manager, you must generate the certificates for McAfee MOVE AntiVirus, so that the SVM and SVM Manager communicate and authenticate each other properly.

**Before you begin**

McAfee MOVE AntiVirus uses secure https protocol for communication between McAfee MOVE AntiVirus SVM and SVM Manager. For secure https protocol, you must generate the McAfee MOVE AntiVirus certificates when the McAfee ePO certificate is changed, so that the change is reflected in the McAfee MOVE AntiVirus policies.

- You installed the McAfee MOVE AntiVirus Meta Package extension on the McAfee ePO server.
- You deployed the SVM Manager.
- You deployed the McAfee MOVE AntiVirus SVM package to the target virtual systems.
- You deployed the McAfee MOVE AntiVirus client package to client systems.
- You configured your McAfee ePO details on the **General** page under **Automation | MOVE AntiVirus Deployment | Configuration**.

**Task**

1. Log on to McAfee ePO as an administrator.
2. Select **Menu | Automation | Server Tasks** to open **Server Tasks** page.
3. Select **MOVE AntiVirus : Generate Certificates** query and click **Run** to generate the McAfee MOVE AntiVirus certificates.
4. Select **Menu | Systems | System Tree**.
5. In the **System Tree**, select the group containing the virtual machines where you want to apply the McAfee MOVE AntiVirus 4.6.0 policies.
6. To apply the policy immediately, send an agent wake-up call to the client system.
7. Log on to the client system as an administrator.
8 Run an EICAR test.
9 Verify that the SVM sends threat details as threat events to McAfee ePO.

McAfee MOVE AntiVirus certificates are generated successfully and McAfee MOVE AntiVirus SVM and SVM Manager are communicating properly.

Assign the SVM manually without SVM Manager

If you are not using SVM Manager, configure the SVM settings in the McAfee MOVE AntiVirus Options policy and assign it to the clients, so that the SVMs can protect the clients.

Before you begin
- You installed the McAfee MOVE AntiVirus Meta Package extension on the McAfee ePO server.
- You deployed the McAfee MOVE AntiVirus SVM package to the target virtual systems.
- You deployed the McAfee MOVE AntiVirus client package to the client systems.

Task
1 Log on to McAfee ePO as an administrator.
2 Click Menu | Policy | Policy Catalog, select MOVE AntiVirus 4.6.0 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.
5 Under SVM Assignment on the policy settings page, configure these options, then click Save.
   - Select Assign SVM manually and configure the SVMs details:
     - Enter IP Address or FQDN (domain name) of SVM-1, and the SVM-1 Port. Default is 9053.
     - Enter IP Address or FQDN (domain name) of SVM-2, and the SVM-2 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 are protected by the SVMs.

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 on-demand scan 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**

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.

**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 TIE server appliance.
2. Deploy the Data Exchange Layer client to McAfee MOVE AntiVirus SVM.
3. Verify the TIE 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.

**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**
1 Log on to McAfee ePO as an administrator.
2 Select **Menu | Software | Product Deployment**, then click **New Deployment**.
3 Complete the new deployment information, then start the deployment.
4 Verify that the DXL **Connection Status** on McAfee ePO is **Connected**.

> 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 TIE server installation**

After installing the Threat Intelligence Exchange and Data Exchange Layer components, verify the installation.

**Before you begin**

You installed the TIE server appliance. For installing and setting-up TIE, see the installation guide for your version of TIE.

**Task**
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 and DXLBROKER tags were 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 the system tray, click ![About] and select **About** to open the 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
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 postgres user name and password that you specified on the PosgresSQL page during the server installation.
6 Click Test Connection.
7 Click Save.

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 integrate 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 about how to install and set up the TIE requirements, see the product documentation for your version of TIE.

Task
1 Log on to McAfee ePO as an administrator.
2 Select Menu | Policy | Policy Catalog, select MOVE AntiVirus 4.6.0 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.

<table>
<thead>
<tr>
<th>Select this...</th>
<th>To do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Known malicious</td>
<td>Perform scan action for Known malicious, Most likely malicious, Might be malicious, Unknown, Might be trusted, and Most likely trusted files based on threat detection response specified in On Access Scan or On Demand Scan policies.</td>
</tr>
</tbody>
</table>
| Most likely malicious | • Perform threat detection response actions specified in On Access Scan or On Demand Scan policies for files Known malicious based on their TIE reputation score.  
| | • Perform scan action for Most likely malicious, Might be malicious, Unknown, Might be trusted, and Most likely trusted files based on threat detection response specified in On Access Scan or On Demand Scan policies. |
| Might be malicious | • Perform threat detection response actions specified in On Access Scan or On Demand Scan policies for files Known malicious and Most likely malicious based on their TIE reputation score.  
| | • Perform scan action for Might be malicious, Unknown, Might be trusted, and Most likely trusted files based on threat detection response specified in On Access Scan or On Demand Scan policies. |
| Unknown | • Perform threat detection response actions specified in On Access Scan or On Demand Scan policies for files Known malicious, Most likely malicious, and Might be malicious based on their TIE reputation score.  
| | • Perform scan action for Unknown, Might be trusted, and Most likely trusted files based on their TIE reputation score. |
| Might be trusted | • Perform threat detection response actions specified in On Access Scan or On Demand Scan policies for files Known malicious, Most likely malicious, Might be malicious, and Unknown based on their TIE reputation score.  
| | • Perform scan action for Might be trusted and Most likely trusted files based on threat detection response specified in On Access Scan or On Demand Scan policies. |
| Most likely trusted | • Perform threat detection response actions specified in On Access Scan or On Demand Scan policies for files Known malicious, Most likely malicious, Might be malicious, Unknown, and Might be trusted based on their TIE reputation score.  
| | • Perform scan action for Most likely trusted files based on threat detection response specified in On Access Scan or On Demand Scan policies. |

Based on the file TIE reputation score, the SVM performs threat detection responses specified in the On Access Scan or On Demand Scan policies for files the TIE reputation score is higher than the threshold defined in OAS/ODS policy. The SVM performs the scan action for selected files based on the 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 is enabled and the file is determined as an Advanced Threat Defense candidate by TIE server, SVM sends the file to Advanced Threat Defense through the TIE server for analyzing.

**Verify the TIE server integration**

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

Before you begin

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

**Task**

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 the Advanced Threat Defense (ATD) option under the Shared Cloud Solutions policy on the McAfee ePO server.

**Task**

1. Log on to the McAfee MOVE AntiVirus SVM.
2. Run this command:

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

4 Log on to McAfee ePO as an administrator.

5 Select Menu | Systems | TIE Reputations.

6 From the File Search tab, under ATD Reputation, verify the Advanced Threat Defense reputation details for the files those were submitted to Advanced Threat Defense.
Upgrading McAfee MOVE AntiVirus (Multi-Platform)

Review this list before upgrading your environment.

- The McAfee MOVE AntiVirus 4.6.0 client and SVM packages upgrade over versions 4.0.0 and 4.5.0.
- To upgrade McAfee MOVE AntiVirus (Multi-Platform), install and upgrade these components in this order:
  1. Product extension
  2. SVM Manager
  3. SVM
  
  **Best practice:** Upgrade the McAfee scanning engine to the latest 5900 engine that provides enhanced detection capabilities.

  4. McAfee MOVE AntiVirus client

- Make sure that you remove any Debian package deployment task from the client task catalog in McAfee ePO before upgrading to McAfee MOVE AntiVirus 4.6.0.

Contents

- Upgrading an existing version
- Upgrade the extension
- Upgrade the SVM Manager
- (If you are not using autoscale SVM) Upgrade the SVM with McAfee ePO
- (If you are using autoscale SVM) Upgrade the SVM with McAfee ePO
- Upgrade persistent virtual machines
- Upgrade non-persistent virtual machines
- Upgrade the McAfee MOVE AntiVirus client

Upgrading an existing version

If a supported version of McAfee MOVE AntiVirus is installed in your environment, you can upgrade to McAfee MOVE AntiVirus 4.6.0.

Upgrading from McAfee MOVE AntiVirus 4.0.0, 4.5.0, or 4.5.1

Install the McAfee MOVE AntiVirus 4.6.0 Meta Package extension to upgrade the previous version of McAfee MOVE AntiVirus. When the McAfee MOVE AntiVirus 4.6.0 is installed, the older product version is removed.

Upgrading from McAfee MOVE AntiVirus 3.5.1 or 3.6.1

You must upgrade your existing version (3.5.1 or 3.6.1) to 4.0.0, 4.5.0, or 4.5.1 then you can upgrade to 4.6.0.
Upgrade the extension

Version 4.6.0 of the McAfee MOVE AntiVirus Meta Package extension upgrades the 4.0.0, 4.5.0, or 4.5.1 extension on the McAfee ePO server.

Before you begin
The extension file (MOVE-AV_Meta_Package_Ext.zip) is in an accessible location on the network.

All policies created in version 4.0.0, 4.5.0, or 4.5.1 exist after you upgrade to version 4.6.0.

Task
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.

Upgrade the SVM Manager

Version 4.6.0 of the SVM Manager upgrades the 4.5.0 SVM Manager on your hypervisor. If you are using 4.0.0 SVM Manager, a new SVM Manager is deployed to your hypervisor. Once the new SVM Manager is up and running, the existing SVM Manager 4.0.0 is turned off.

Before you begin
• Make sure that your VMware vCenter account is synced successfully.
• You configured your Infrastructure Group. For details, see Create or edit an infrastructure group in McAfee ePO for SVM Manager deployment.
• The SVM Manager OVF package (MOVE-AV-MP_SVM_Manager_OVF_4.6.0.zip) is in an accessible location on the network.

Task
1. Log on to McAfee ePO as an administrator.
2. Select Menu | Automation | MOVE AntiVirus Deployment.
3. On the Configuration tab, click SVM Manager Configuration to open the SVM Manager OVF Repository page.
4 Perform these tasks to check in the SVM Manager OVF package.
   a Click Actions | Add SVM Manager to open the Check-in SVM Manager OVF (zip) File page.
   b Under SVM Manager OVF Check-in, configure these options:
      • Select SVM Manager OVF (zip) file to check-in — Browse to and select the SVM Manager OVF package
        (MOVE-AV-MP_SVM_Manager_OVF_4.6.0.zip).
      • Specify the location of McAfee ePO system — Specify the SVM Manager OVF package location on the
        McAfee ePO server (for example, C:\SVM Manager). The package is taken from this location during
        deployment to the hypervisor.
   c Click OK to check in the package. The OVF check in might take a few minutes to complete.

5 On the Configuration tab, click SVM Manager Configuration to open the SVM Manager OVF Details page.

6 Under Deployment Configuration, configure these options.
   • Infrastructure Group — Select the Default Group or an infrastructure group you created.
   • Checked-in OVF — Select the SVM Manager OVF package that is checked in to the McAfee ePO server.
   • SVM Manager Settings policy — Select the SVM Manager Settings policy, so that it is applied to the SVM
     Manager.

7 Click Upgrade SVM Manager to open the Confirm SVM Manager Deployment dialog box.

8 Click OK to upgrade the SVM Manager.
   You can check the upgrade status on the Deployment Status tab under MOVE AntiVirus Upgrade wizard on the
   McAfee ePO server.

See also
Create or edit an infrastructure group in McAfee ePO for SVM autoscaling on page 37

(If you are not using autoscale SVM) Upgrade the SVM with McAfee ePO

Version 4.6.0 of the McAfee MOVE AntiVirus SVM upgrades the 4.0.0 and 4.5.0 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 4.6.0 SVM
rather than upgrading an existing SVM.

Task
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.
   a Make sure that Product Deployment is selected, then click OK.
   b Type a name for the task you are creating and add any notes.
   c Next to Target platforms, select Windows as the type of platform to use for deployment.
d) Next to **Products and components**, set the following:
   - Select the product from the first drop-down list. The products listed are those where you 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 them in the **Command line** text field.

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

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

4) Select the **Preset** filter as **Product Deployment (McAfee Agent)**. Each assigned client task for each selected category appears in the details pane.

5) Click **Actions | New Client Task Assignment** to open the Client Task Assignment Builder wizard.
   - 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.
   - Next to **Tags**, select the platforms where you are deploying the packages, then click **Next**.
   - On the Schedule page, select whether the schedule is enabled, and specify the schedule details, then click **Next**.

6) Review the summary, then click **Save**.

---

(If you are using autoscale SVM) **Upgrade the SVM with McAfee ePO**

You must export an SVM OVF template with 4.6.0 SVM installed on it, so that your master image of the SVM has latest version.

**Before you begin**
- Make sure that your SVM Manager upgrade is successful.
- You exported your latest SVM OVF template and checked in to the McAfee ePO server and the SVM OVF details appear on the **SVM OVF Details** page under **MOVE AntiVirus Deployment** wizard. For details, see Configuring an SVM OVF template for autoscaling.
- You configured your Infrastructure Group. For details, see Create or edit an infrastructure group in McAfee ePO for SVM autoscaling.

**Task**
1) Log on to McAfee ePO as an administrator.
2) Select **Menu | Policy | Policy Catalog**, then select **MOVE AntiVirus 4.6.0** from the Product list.
3) From the **Category** list, select **SVM Manager Settings**.
4) Click the name of the policy that you are currently using for SVM autoscaling.
5 From SVM Autoscale Settings, deselect Enable auto scaling of SVMs.

Disabling this option disappears all running, ready, and standby SVMs from the Autoscale SVM Details page under MOVE AntiVirus Deployment wizard. Also, deletes all ready and standby SVMs, but the running SVMs continue to protect the client systems.

6 Select Menu | Systems | System Tree.

7 Identify the VM or SVM that you used to export SVM OVF template, then delete it.

8 From SVM Autoscale Settings, again select Enable auto scaling of SVMs.

The new ready and standby SVMs are deployed. Once the new ready and standby SVMs are up, the existing running SVMs are deleted.

See also
Create or edit an infrastructure group in McAfee ePO for SVM autoscaling on page 37

**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**

1 Log on to McAfee ePO as an administrator.

2 Check in and install the McAfee MOVE AntiVirus 4.6.0 Meta Package extension in McAfee ePO.

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

4 Install SVM version 4.6.0 on the virtual server.

5 Create a new McAfee MOVE AntiVirus 4.6.0 policy that references the SVM you created, and assign it to the virtual machines being upgraded.

6 Create a McAfee ePO client task to upgrade the McAfee MOVE AntiVirus clients to version 4.6.0.

   As the upgrade task is executed on virtual machines, the VMs begin to use the 4.6.0 SVM for file scanning.

7 After all clients are upgraded to version 4.6.0, 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**

1 Log on to McAfee ePO as an administrator.

2 Install the McAfee MOVE AntiVirus 4.6.0 client package and McAfee MOVE AntiVirus 4.6.0 SVM packages and upgrade the extensions in McAfee ePO.
3 Create a new 4.6.0 client policy definition that references existing SVM systems.

4 From the McAfee ePO console, upgrade all SVMs to version 4.6.0.

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

5 Change the master image by deploying version 4.6.0 of the McAfee MOVE AntiVirus client from McAfee ePO, or by manually upgrading the client directly on the master image.

---

### Upgrade the McAfee MOVE AntiVirus client

Version 4.6.0 of the McAfee MOVE AntiVirus client upgrades the 4.0.0 and 4.5.0 clients.

**Before you begin**

- Make sure that your VMware vCenter account is synced successfully.
- Make sure that your client systems are turned on where you want to deploy McAfee MOVE AntiVirus client.

You can also upgrade clients by creating an upgrade client task and assigning that task to virtual machines.

**Task**

1 Log on to McAfee ePO as an administrator.

2 Select Menu | Systems | System Tree.

3 In the System Tree, select the virtual machines where you want to deploy the client package.

4 From Actions, select MOVE | Deploy Client [Multi-Platform] to open the Client Deployment Configuration page.


You can view all the SVM Assignment Rules, if the selected client systems are part of the assignment rules.

6 Click Proceed to open the Deployment Confirmation dialog box.

A message shows the number of systems that are compatible and non-compatible for the client deployment.

7 Review the message, then click OK to deploy the client package to the compatible client systems.

A deployment task is created for all selected systems. Go to Deployment Status tab under the MOVE AntiVirus Deployment wizard to view the Passed or Failed tasks with their details.

If you click Cancel, the deployment task is created only for the non-compatible client systems, and the failure reasons can be viewed on the Deployment Status tab under the MOVE AntiVirus Deployment wizard.

For the compatible client systems, the SVM Manager IP address is updated in the respective Options policy, then the SVM Manager assigns an SVM for the clients to protect them.

**See also**

*Check the McAfee MOVE AntiVirus client deployment status on page 45*
Uninstalling McAfee MOVE AntiVirus (Multi-Platform)

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

Contents
- Uninstall the client and SVM
- Assign the uninstallation task to virtual systems
- Remove the client or SVM package from McAfee ePO
- Remove the SVM Manager
- Uninstall the extensions

Uninstall the client and SVM

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
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 4.6.0 or MOVE AV [Multi-Platform] SVM 4.6.0 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 the 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**

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.
   a. **Product** — McAfee Agent
   b. **Task Type** — Product Deployment
   c. **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**

1. Log on to McAfee ePO as an administrator.
2. Select Menu | Software | Master Repository.
3. Select MOVE AV [Multi-Platform] client 4.6.0 or MOVE AV [Multi-Platform] SVM 4.6.0, then click Delete.

Remove the SVM Manager

Remove the SVM Manager from the McAfee ePO server.

**Task**

1. Log on to McAfee ePO as an administrator.
2. Select Menu | Automation | MOVE AntiVirus Deployment.
3 On the Configuration tab, click SVM Manager Configuration to open the SVM Manager OVF Details page.

4 Under Deployment Configuration, click Delete SVM Manager.

You can check the deletion status on the Deployment Status tab under MOVE AntiVirus Deployment wizard on the McAfee ePO server.

Uninstall the extensions

Uninstall the McAfee MOVE AntiVirus extensions from McAfee ePO.

Task

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 in this order.
   - MOVE AntiVirus
   - MOVE AntiVirus Common
   - vSphere Connector
   - MDCC

5 From the Extensions tab under McAfee group, select Help Content.

6 Click Remove next to the mvav_help extension.
Uninstalling McAfee MOVE AntiVirus (Multi-Platform)

Uninstall the extensions
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
- Advantages of using NSX Manager over vCNS
- Setting up the SVM
- Download and check in software extensions and packages
- Run security updates for 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

Advantages of using NSX Manager over vCNS

These are some of the advantages of using VMware NSX Manager-based deployment over VMware vCloud Networking and Security Manager-based deployment.

- 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. McAfee MOVE AntiVirus is certified for integrating NSX Manager from VMware.
- When a new scan policy is added or an existing scan policy is changed, all updates are immediately exported to NSX.
- Using McAfee ePO, On Access Scan and On Demand Scan policies can be created with the configurations required for high security. Tagging options can also be configured under NSX tagging, including NSX Virus Found Tag and NSX Unprotected Tag. Once tagging is configured, when malware is detected, the affected VM is tagged with ANTI_VIRUS.VirusFound.threat=high and when VM is not protected, then it is tagged with MCAFEE.MOVE.unprotected=yes. Tagged VMs are displayed on the NSX Manager.
- VMware has announced the End of Availability (EOA) and End of General Support (EOGS) of VMware vCloud Networking and Security 5.5.x. For details, see the VMware documentation, VMwareKB2144733
- For details about implementation of vShield Endpoint beyond EOA of vCNS, see the VMware documentation: VMwareKB2110078
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 SVM provided with McAfee MOVE AntiVirus must be deployed to each hypervisor to protect the associated VMs.

You can deploy the SVM using any of these methods.

• VMware vCloud Networking and Security Manager 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 the SVM. You can also create a schedule to deploy the SVM later.

• VMware NSX Manager deployment — Register the SVM with VMware NSX Manager and deploy it automatically to one or more clusters. You can select one or more Network & 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.

For each deployment method, you can configure the options automatically or manually.

• Automatic configuration

• Manual configuration

Download and check in software extensions and packages

If you do not have Software Manager, you can download these software extensions and product packages to the McAfee ePO server from the McAfee download site.

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

<table>
<thead>
<tr>
<th>Package name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOVE-AV_Meta_Package_Ext.zip</td>
<td>This main extension includes these extensions:</td>
</tr>
<tr>
<td></td>
<td>• McAfee MOVE AntiVirus Common — Extension for product installation and deployment.</td>
</tr>
<tr>
<td></td>
<td>• McAfee MOVE AntiVirus — Extension for configuring and managing policies.</td>
</tr>
<tr>
<td></td>
<td>• McAfee MOVE AntiVirus License — License extension; upgrades evaluation extension to a fully licensed extension.</td>
</tr>
<tr>
<td></td>
<td>• vSphere Connector — Data Center discovery software.</td>
</tr>
<tr>
<td></td>
<td>• McAfee Data Center Control — It is a dependency software for vSphere Connector.</td>
</tr>
<tr>
<td></td>
<td>• Product Help extension</td>
</tr>
<tr>
<td>MOVE-AV-AL_SVM_OVF_4.5.1.zip</td>
<td>Agentless SVM OVF package</td>
</tr>
</tbody>
</table>
## Package name Description

<table>
<thead>
<tr>
<th>Package name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOVE-AV-AL_SVM_Pkg_4.5.1.zip</td>
<td>Agentless SVM package — McAfee ePO deployable package</td>
</tr>
<tr>
<td>MOVE-AV-AL_RestoreTool_4.5.1.zip</td>
<td>Agentless restore tool</td>
</tr>
<tr>
<td>MOVE-AV_DOCS_4.6.0.zip</td>
<td>Product documentation package</td>
</tr>
</tbody>
</table>

### Tasks

- **Check in the extensions and packages to McAfee ePO from the Software Manager on page 67**
  If you have Software Manager, you can check in the software extensions and packages to the Master Repository without downloading them.

### Check in the extensions and packages to McAfee ePO from the Software Manager

If you have Software Manager, you can check in the software extensions and packages to the Master Repository without downloading them.

#### Task

1. Log on to McAfee ePO as an administrator.

2. Select `Menu | Software`, then click `Software Manager`.

3. From `Software (by Label) | Endpoint Security`, select these extensions, then click `Check In`.

<table>
<thead>
<tr>
<th>Product Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee MOVE AntiVirus 4.6.0</td>
<td>MOVE-AV_Meta_Package_Ext.zip</td>
</tr>
<tr>
<td></td>
<td>This main extension includes these extensions:</td>
</tr>
<tr>
<td></td>
<td>• McAfee MOVE AntiVirus Common — Extension for product installation and deployment.</td>
</tr>
<tr>
<td></td>
<td>• McAfee MOVE AntiVirus — Extension for configuring and managing policies.</td>
</tr>
<tr>
<td></td>
<td>• McAfee MOVE AntiVirus License — License extension; upgrades evaluation extension to a fully licensed extension.</td>
</tr>
<tr>
<td></td>
<td>• vSphere Connector — Data Center discovery software.</td>
</tr>
<tr>
<td></td>
<td>• McAfee Data Center Control — It is a dependency software for vSphere Connector.</td>
</tr>
<tr>
<td></td>
<td>• Product Help extension</td>
</tr>
</tbody>
</table>

All extensions and packages are checked in to the Master Repository from the Software Manager.


### Run security updates for McAfee MOVE AntiVirus SVM

Run security updates 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, you can perform these actions.

Task
1 Run this command to update the local Ubuntu repository:
   
   sudo apt-get update

2 Run this command to check whether the upgrades are taking place:
   
   sudo unattended-upgrade --debug --dry-run

3 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. You must have a valid McAfee ePO user name that uses McAfee ePO authentication. The user name must have administrator rights.</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>
<tr>
<td>Network</td>
<td>Network</td>
<td>(Optional) The network for the McAfee MOVE AntiVirus SVM's static IP address.* If this setting remains blank, it is created from the IP address and the Netmask.</td>
</tr>
</tbody>
</table>
### Component Setting Description

<table>
<thead>
<tr>
<th>Component</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVM</td>
<td>Domain</td>
<td>The domain name of McAfee MOVE AntiVirus SVM and the default domain name for 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 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 vCloud Networking and Security Manager.</td>
</tr>
<tr>
<td>vCloud Networking and Security Manager</td>
<td>User name</td>
<td>The user name used to register the McAfee MOVE AntiVirus SVM with the vCloud Networking and Security Manager.</td>
</tr>
</tbody>
</table>

* 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**

1. Log on to McAfee ePO as an administrator.

2. Select Menu | Policy | Policy Catalog, select MOVE AntiVirus 4.6.0 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.
   - Username — Enter the user name credentials to connect with the server.

   The user account requires at least read access to the vCenter server or the ESXi host. Domain-based credentials are supported only when the vCenter server or the ESXi host has been configured to support domain-based authentication.
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 McAfee MOVE AntiVirus Meta Package extension allows 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 Meta Package on McAfee ePO
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
   - Validate the NSX Manager connection to the McAfee ePO server
   - Register the McAfee MOVE AntiVirus service with NSX Manager using McAfee ePO
6. Apply McAfee MOVE AntiVirus (Agentless) protection to your VMs
7. Deploy the McAfee MOVE AntiVirus service using vSphere Web Client
8. Apply the NSX Security Policy to the NSX Security Group
9. Create an NSX Security Group and Policy in the NSX Manager
10. Verify the policy export details in vSphere Web Client

After you save and reopen the SVM Settings policy, the vCenter Password field appears blank. Though it appears blank, the password is saved in the policy settings. You must retype the password to test connection settings.

- **Password** — Enter the password associated with the user.
- **Confirm password** — Retype the password.
- **SVM Time Zone** — Select your local time zone from the drop-down list.

6. Click Test connection settings to test the connection to the hypervisor.
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 on McAfee ePO.
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 McAfee MOVE AntiVirus Meta Package extension 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.
(Optional) Install the Endpoint Security for Linux Threat Prevention extension to manage the Endpoint Security for Linux Threat Prevention policy on the SVM. Endpoint Security for Linux Threat Prevention is only licensed for the SVM, not for other Linux systems in your environment.

Installing the McAfee MOVE AntiVirus Meta Package extension installs McAfee Data Center Control, vSphere Connector, and McAfee MOVE AntiVirus specific extensions on the McAfee ePO server, and also checks in the McAfee MOVE AntiVirus client package to the Master Repository.

Task
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>McAfee MOVE AntiVirus Meta Package</td>
<td>MOVE-AV_Meta_Package_Ext.zip</td>
</tr>
<tr>
<td>(Optional) Endpoint Security for Linux Threat Prevention</td>
<td>ISecTP-10.2.0-707-HF1177340-ePO.zip</td>
</tr>
</tbody>
</table>

   To install this Hotfix, you must install Endpoint Security Platform and Endpoint Security Threat Prevention extensions. For details, see Endpoint Security for Linux Threat Prevention Product Guide.

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 McAfee MOVE AntiVirus Meta Package extension on the McAfee ePO server.
   • You configured your VMware vCenter server that manages the ESXi servers, which host the guest VMs.

Task
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, configure these options.
   • 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.

Once the McAfee MOVE AntiVirus (Agentless) product is set up and running, you must not delete the Registered Cloud Account.
Set up a common configuration for deployment

Before deploying McAfee MOVE AntiVirus SVM, configure 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**

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 options.

<table>
<thead>
<tr>
<th>Table 5-1</th>
<th>McAfee ePO credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Options</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Password</td>
<td>Type the password of the McAfee ePO console that the administrator has currently logged on.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Retype the password.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 5-2</th>
<th>McAfee MOVE AntiVirus SVM configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Option</strong></td>
<td><strong>Description</strong></td>
</tr>
<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.  
  • 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.

**Task**

1. Log on to McAfee ePO as an administrator.
2. Select **Menu | Automation | MOVE AntiVirus Deployment**.
3. On the **Configuration** tab under **Agentless**, click **SVM Repository** to open the **SVM OVF Details** page with these McAfee MOVE AntiVirus SVM OVF options:
<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVM OVF Name</td>
<td>Name of the McAfee MOVE AntiVirus SVM package checked in to McAfee ePO.</td>
</tr>
<tr>
<td>SVM OVF Version</td>
<td>Version of the McAfee MOVE AntiVirus SVM package checked in to McAfee ePO.</td>
</tr>
<tr>
<td>SVM OVF 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 OVF (zip) file page.

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

You can check in up to three versions of McAfee MOVE AntiVirus SVM starting from 4.0.0.

**Validate your NSX Manager using McAfee ePO**

The vSphere Connector extension automatically detects and sends the details of your NSX Managers to the McAfee ePO server. You must now register these NSX servers 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 Meta Package 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. You can also register your vCenter server with NSX Manager.

**Task**

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 displays these options.

<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>Edit — Click to edit and validate the credentials and other details of the NSX Managers, which are automatically detected and sent to McAfee ePO.</td>
</tr>
</tbody>
</table>

Agentless installation and configuration
Deploying McAfee MOVE AntiVirus (Agentless) in an NSX environment
4. Click **Edit** under **Action** to open the **Edit NSX Manager Details** dialog box and edit these NSX Manager account options.

   ![Info icon](image)

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

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

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. This registration permits the deployment of the service to the ESXi servers.

**Task**

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 options.

<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>
</tbody>
</table>
Option | Description
--- | ---
Service Registration Status | Displays registration status values **Registered**, **Not Registered**, and **Registration Failed**.
Actions | • **Register** — Click to select the latest McAfee MOVE AntiVirus SVM and register it to the vCenter that is added to your NSX Manager.

• **Unregister** — Click to unregister the McAfee MOVE AntiVirus service and to remove it from the vCenter.

• **Upgrade** — Click to upgrade the McAfee MOVE AntiVirus service.

Make sure that you 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.

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

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 the 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 sets 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 configurations 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.
- 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 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 vSphere distributed switch 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 IP addresses are not on the same network as McAfee ePO or the NSX Manager.

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

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

   ![Warning](image)

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

7. Review the settings and click **Finish** to complete the deployment of McAfee MOVE AntiVirus service.

   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.

   ![Warning](image)

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

8. View these **Service status** details on the VMware vSphere Web Client console.
Service Status | ID | Description
--- | --- | ---
UNKNOWN | 3 | Specifies that the McAfee MOVE AntiVirus service status is unknown.
UP | N/A | Not applicable.
DOWN | 1 | Specifies that the McAfee MOVE AntiVirus service is stopped.

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.

<table>
<thead>
<tr>
<th>Before you begin</th>
</tr>
</thead>
<tbody>
<tr>
<td>• You installed the McAfee MOVE AntiVirus extension on the McAfee ePO server.</td>
</tr>
<tr>
<td>• The McAfee MOVE AntiVirus service is registered with McAfee ePO.</td>
</tr>
</tbody>
</table>

Task

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

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

3. Click the green plus sign to add a Guest Introspection Service. Provide a name for the Guest Introspection Service and define 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 details about the McAfee MOVE AntiVirus service, which help you to identify the SVM.</td>
</tr>
<tr>
<td>Action</td>
<td>• Apply — Select this to apply the SVM.</td>
</tr>
<tr>
<td></td>
<td>• Block — Select this to block the SVM.</td>
</tr>
<tr>
<td>Service Type</td>
<td>From the drop-down list, select Anti Virus.</td>
</tr>
<tr>
<td>Service Name</td>
<td>From the drop-down list, select McAfee MOVE AV.</td>
</tr>
</tbody>
</table>
### Service Profile

McAfee MOVE AV [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.

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

### Enforce

Yes

---

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

You have created your NSX security policy for deploying 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.

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.

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

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 (for example, **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 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.
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

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 **MCAFEE.MOVE.unprotected=yes** can be moved into a dynamic security group that you configure (for example, **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.
- Make sure that you configured the scan policies available under **MOVE AntiVirus 4.6.0** in McAfee ePO.

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

Policies 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 5-1  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.
   a. 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.
   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.

a 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 .

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>Option</td>
<td>Value</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------------------------------------------------------------</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 the 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, then 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**.

8. **Map DesktopPolicy** policy to **DesktopSecurityGroup**.
   a. On the **Security Policies** tab, ensure that **DesktopPolicy** is selected.
   b. Click the **Apply Security Policy** icon and select **DesktopSecurityGroup**.
   c. Click **OK**.

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

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

10. **Map QuarantinePolicy** to **QuarantineSecurityGroup**.

    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 (Agentless) 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 McAfee MOVE AntiVirus Meta Package extension is 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 extensions on the McAfee ePO server.
2. Register a VMware vCenter account with McAfee ePO.
3. Set up a common configuration for McAfee ePO and SVM on the McAfee ePO server.
4. Check in the SVM package to McAfee ePO.
5. Configure the IP Pool details.
6. Edit vShield Manager configuration using McAfee ePO.
7. Deploy SVM using McAfee ePO.

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 process. The whole deployment process is only for vCNS environment and not for NSX environment.

1. Install the extensions on the McAfee ePO server.
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.
6. Edit vShield Manager configuration.
7. Deploy SVM using McAfee ePO.

Install the product files on the management server

The McAfee MOVE AntiVirus Meta Package extension 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.
(Optional) Install the Endpoint Security for Linux Threat Prevention extension to manage the Endpoint Security for Linux Threat Prevention policy on the SVM. Endpoint Security for Linux Threat Prevention is only licensed for the SVM, not for other Linux systems in your environment.

Installing the McAfee MOVE AntiVirus Meta Package extension installs McAfee Data Center Control, vSphere Connector, and McAfee MOVE AntiVirus specific extensions on the McAfee ePO server, and also checks in the McAfee MOVE AntiVirus client package to the Master Repository.

**Task**

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>McAfee MOVE AntiVirus Meta Package</td>
<td>MOVE-AV_Meta_Package_Ext.zip</td>
</tr>
<tr>
<td>(Optional) Endpoint Security for Linux Threat Prevention</td>
<td>ISecTP-10.2.0-707-HF1177340-ePO.zip</td>
</tr>
</tbody>
</table>

To install this Hotfix, you must install Endpoint Security Platform and Endpoint Security Threat Prevention extensions. For details, see *Endpoint Security for Linux Threat Prevention Product Guide*.

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**

- You configured your VMware vCenter server that manages the ESXi servers, which host the guest VMs.
- You installed the McAfee MOVE AntiVirus Meta Package extension on the McAfee ePO server.

**Task**

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, select **VMware vSphere**, then click **OK**.

4. On the **vCenter Account Details** page, configure these options.
   - **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.

![System Tree](image)

**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
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 options.

Table 5-3 McAfee ePO credentials

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

Table 5-4 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>
<tr>
<td>Password</td>
<td>Type a password to be used as McAfee MOVE AntiVirus SVM password during deployment.</td>
</tr>
<tr>
<td></td>
<td>• The password must be at least 6 characters.</td>
</tr>
<tr>
<td></td>
<td>• The password must contain at least one uppercase letter (A–Z) and one numeral (0–9).</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Retype the password of the available McAfee MOVE AntiVirus SVM.</td>
</tr>
</tbody>
</table>

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
1. Log on to McAfee ePO as an administrator.
2. Select Menu | Automation | MOVE AntiVirus Deployment.
3. On the Configuration tab, under Agentless, click SVM Repository to open the SVM OVF Details page with these SVM OVF options and action.

<table>
<thead>
<tr>
<th>Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVM OVF Name</td>
<td>Name of the McAfee MOVE AntiVirus SVM package checked in to McAfee ePO.</td>
</tr>
<tr>
<td>SVM OVF Version</td>
<td>Version of the McAfee MOVE AntiVirus SVM package checked in to McAfee ePO.</td>
</tr>
</tbody>
</table>
### Configure the IP Pool options

An IP Pool is a range of IP addresses in 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 Meta package extension on the McAfee ePO server.

An IP Pool's range cannot overlap one another, so 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

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 options 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 host name-to-IP address resolution.</td>
</tr>
<tr>
<td>Secondary DNS</td>
<td>(Optional) Type the IP address of the Secondary DNS server for host name-to-IP address resolution.</td>
</tr>
</tbody>
</table>
Options | Description
--- | ---
Used / Total | 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.
Action | • Edit — Use this option to edit the IP Pool details.
  • Delete — Use this option to delete the IP Pool when its IP addresses are not in use.

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 can view the registration status of the vShield Manager and take the required action, as appropriate.

**Task**

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 options.

<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>
</tbody>
</table>
| Configuration Status | Displays these registration statuses:
  • Configured — Indicates that the vShield Manager is registered and ready for deployment.
  • Not Configured — Indicates that the vShield Manager is not registered. Click Edit and configure it before deployment.
  • Credentials unknown — Indicates that the vShield Manager is registered with VMware vCenter, but the credentials are unknown. Click Edit and configure it before deployment. |
| Action | Edit — Click to edit and validate the existing vShield Manager configuration. |
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.

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 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 vSphere Connector. For details, see the product documentation for Cloud Workload Security.
- 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
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 options.
   - 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 options.
   - 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
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, vShield Manager, host, VMTools, and Endpoint version
- The available datastore space

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

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.
Check the McAfee MOVE AntiVirus SVM deployment status

After deploying or upgrading McAfee MOVE AntiVirus SVM, you can view the Deployment Status 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 initiated the McAfee MOVE AntiVirus SVM deployment using McAfee ePO.

Task

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

Table 5-5  Job status

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypervisors</td>
<td>Specifies the name of the hypervisor.</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>Deployment Type</td>
<td>Displays whether the McAfee MOVE AntiVirus SVM deployment type is Deploy, Upgrade, 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>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>
</tbody>
</table>

Table 5-6  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, or a VM.</td>
</tr>
<tr>
<td>Task Type</td>
<td>Specifies the set of internal tasks that happen in 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.</td>
</tr>
<tr>
<td>Node Name</td>
<td>Displays the McAfee MOVE AntiVirus SVM VM name, or Hypervisor name, or the guest VM name.</td>
</tr>
<tr>
<td>Status</td>
<td>Specifies the task status such as Started, Completed, Skipped, Failed, and In Progress.</td>
</tr>
<tr>
<td>Failure Reason</td>
<td>Specifies the reason for the failure of the task.</td>
</tr>
<tr>
<td>Start Time</td>
<td>Indicates the date and time when the task started.</td>
</tr>
<tr>
<td>End Time</td>
<td>Indicates the date and time when the task ended.</td>
</tr>
</tbody>
</table>

The rollback functionality is available while deploying and upgrading the 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 5-7  During McAfee MOVE AntiVirus SVM deployment**

<table>
<thead>
<tr>
<th>Task type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing vShield Endpoint</td>
<td>Indicates that the vShield Endpoint installation is in progress.</td>
</tr>
<tr>
<td>Deploying SVM</td>
<td>Indicates that the McAfee MOVE AntiVirus SVM deployment is in progress.</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 address 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 5-8  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 address 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 IP Pool</td>
<td>Returns the used Static IP address to the IP Pool.</td>
</tr>
</tbody>
</table>

**Table 5-9  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>
<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>
</tbody>
</table>

When the latest McAfee MOVE AntiVirus SVM is already deployed to the hypervisor, the **Deploying SVM** task is skipped. Hence, other McAfee MOVE AntiVirus SVM-related tasks do not start.
### Table 5-9  During MOVE AntiVirus SVM upgrade (continued)

<table>
<thead>
<tr>
<th>Task type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clearing SVM IP and Port from VSM</td>
<td>Removes the IP address and port 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>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 address 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 5-10  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 IP Pool</td>
<td>Rolls back the static IP address to IP Pool, which was assigned to the deployed McAfee MOVE AntiVirus SVM.</td>
</tr>
</tbody>
</table>
Upgrading McAfee MOVE AntiVirus (Agentless)

Deploying a new SVM to the hypervisor in the previous version of McAfee MOVE AntiVirus (Agentless) requires that you 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.

The McAfee MOVE AntiVirus SVM upgrade from 4.5.0 to 4.5.1 is supported using the Debian package.

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 4.6.0 extension upgrades the 4.0.0, 4.5.0, or 4.5.1 extensions on the McAfee ePO server.

Contents

- Upgrading an existing version
- Manually upgrade the McAfee MOVE AntiVirus SVM
- Upgrade McAfee MOVE AntiVirus (Agentless) in an NSX environment
- Upgrade McAfee MOVE AntiVirus in vCNS environment

Upgrading an existing version

If a supported version of McAfee MOVE AntiVirus is installed in your environment, you can upgrade to McAfee MOVE AntiVirus 4.6.0.

Upgrading from McAfee MOVE AntiVirus 4.0.0, 4.5.0, or 4.5.1

Install the McAfee MOVE AntiVirus 4.6.0 Meta Package extension to upgrade the previous version of McAfee MOVE AntiVirus. When the McAfee MOVE AntiVirus 4.6.0 is installed, the older product version is removed.

Upgrading from McAfee MOVE AntiVirus 3.5.1 or 3.6.1

You must upgrade your existing version (3.5.1 or 3.6.1) to 4.0.0, 4.5.0, or 4.5.1 then you can upgrade to 4.6.0.

• Install the McAfee MOVE AntiVirus 4.0.0, 4.5.0, or 4.5.1 product and migration extensions to access the installation wizard.

• Migrate the policy settings from the previous versions of McAfee MOVE AntiVirus to 4.0.0, 4.5.0, or 4.5.1.

For details, see McAfee MOVE AntiVirus 4.0.0, 4.5.0, or 4.5.1 product documentation.
Manually upgrade 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.

Upgrade the extension

Version 4.6.0 of the McAfee MOVE AntiVirus extension upgrades the 4.0.0, 4.5.0, or 4.5.1 extension on the McAfee ePO server.

Before you begin

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

All policies created in version 4.0.0, 4.5.0, or 4.5.1 exist after you upgrade to version 4.6.0.

Task

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.

Deploy a new McAfee MOVE AntiVirus SVM manually (version 4.0.0 only)

The operating system for McAfee MOVE AntiVirus SVM is upgraded to Ubuntu 16.04. You need to manually deploy version 4.5.1 of the McAfee MOVE AntiVirus SVM to each hypervisor.

Before you begin

Unregister the 4.0.0 McAfee MOVE AntiVirus SVM before deploying the new 4.5.1 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_4.5.1.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.
5. Enter u to unregister.
6. Turn off the McAfee MOVE AntiVirus SVM.
    Do not delete this McAfee MOVE AntiVirus SVM until the 4.5.1 version is successfully deployed. This MOVE AntiVirus SVM can be used to troubleshoot deployment issues.
7. Deploy a new McAfee MOVE AntiVirus SVM to the hypervisor.
8. Run the sva-config script to register the SVM with vCloud Networking and Security Manager and McAfee ePO.
See also
Deploying McAfee MOVE AntiVirus (Agentless) in an NSX environment on page 70
Deploying McAfee MOVE AntiVirus (Agentless) in vCNS environment on page 91

Upgrade the McAfee MOVE AntiVirus SVM using the Debian package (version 4.5.0 only)

For upgrading McAfee MOVE AntiVirus SVM from 4.5.0 to 4.5.1, you need to first upgrade the product extension, then the McAfee MOVE AntiVirus SVM using the Debian package. This upgrades McAfee MOVE AntiVirus Agentless and also VirusScan Enterprise for Linux to Endpoint Security for Linux Threat Prevention.

Task

1. Check in the McAfee MOVE AntiVirus SVM Debian package to the Master Repository using one of these methods.

   **Method 1**
   1. Log on to McAfee ePO as an administrator.
   2. Select **Menu | Software**, then click **Software Manager**.
   3. From the **Software (by Label) | Messaging & Web Security**, select **MOVE-AV-AL_SVM_DEB_4.5.1.zip** package, then click **Check In**.

   **Method 2**
   From **epo.properties** file on the McAfee ePO server, increase the **file.upload.limit** value to 300 to check in the Debian package to the Master Repository.

   The reason to change this value is that the McAfee MOVE AntiVirus SVM Debian package size is about 270 MB. The default file size limit to check in the software package to the Master Repository is 250 MB.

   1. Log on to McAfee ePO as an administrator.
   2. From **C:\Program Files (x86)\McAfee\ePolicy Orchestrator\Server\conf\epo** location, open **epo.properties** file.
   3. Change the **file.upload.limit** value to **300**.
   4. Click **Save** button to save the changes.
   5. Restart the McAfee ePO service to effect the changes.
   6. Download the Debian package (**MOVE-AV-AL_SVM_DEB_4.5.1.zip**) from Software Manager to the accessible location.
   7. Check in the Debian package to the Master Repository.

2. Deploy the software package and assign it to the existing McAfee MOVE AntiVirus SVM using the product deployment task in McAfee ePO.

   Make sure you select the **Target platforms** as **Linux** while creating the deployment task.

3. Enforce the policy.

   After a successful deployment, you can verify the SVM and Endpoint Security for Linux Threat Prevention version in System Tree.
   - SVM version — 4.5.1
   - Endpoint Security for Linux Threat Prevention version — 10.2.0
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
1. Log on to McAfee ePO as an administrator.
2. Select Menu | Systems | System Tree | Assigned Policies, then select MOVE AntiVirus 4.6.0.
   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) 4.0.0 and 4.5.0 to McAfee MOVE AntiVirus 4.5.1.

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.

McAfee MOVE AntiVirus 4.5.1 supports upgrading or migrating these components of 4.0.0 and 4.5.0:
• McAfee MOVE AntiVirus extension
• NSX Manager details
• McAfee MOVE AntiVirus service
• McAfee MOVE AntiVirus SVM

Task
2. On McAfee ePO, upgrade the McAfee MOVE AntiVirus extension to McAfee MOVE AntiVirus 4.6.0.
   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 McAfee MOVE AntiVirus extension.
3. Check in the McAfee MOVE AntiVirus SVM 4.5.1 package to McAfee ePO.
4. From McAfee ePO, select **Menu** | **Automation** | **MOVE AntiVirus Deployment** | **Configuration** | **General** and complete the common configuration.

5. On the **Service** tab on McAfee ePO, click **NSX Manager** to open the **MOVE Service Registration** page.

6. Under **Actions**, click **Upgrade** to open the **MOVE Service registration** dialog box.

7. 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**.

   ![Image](https://example.com/image.png)

8. Verify that the McAfee MOVE AntiVirus 4.6.0 **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 an ID and description.

   ![Image](https://example.com/image.png)

9. Deploy the latest McAfee MOVE AntiVirus service using the **Upgrade** button under **Installation** | **Service Deployments** in **vSphere Web Client**.

---

**Upgrade McAfee MOVE AntiVirus in vCNS environment**

Use McAfee ePO to upgrade McAfee MOVE AntiVirus 4.0.0 and 4.5.0 to McAfee MOVE AntiVirus 4.5.1.

McAfee MOVE AntiVirus 4.5.1 supports upgrading these components of 4.0.0 and 4.5.0:

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

**Task**

1. Upgrade the McAfee MOVE AntiVirus extension to 4.6.0.

   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 McAfee MOVE AntiVirus Meta Package extension.

2. Check in the McAfee MOVE AntiVirus SVM 4.5.1 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) 4.5.1 in an NSX environment
- Uninstalling McAfee MOVE AntiVirus (Agentless) in a vCNS environment

Uninstalling McAfee MOVE AntiVirus (Agentless) 4.5.1 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.
From the **Actions** column on the **MOVE Service configuration** page, click **Unregister** for the registered NSX Manager. A confirmation dialog box appears.

Click **OK** to confirm.

**Remove the McAfee MOVE AntiVirus Guest Introspection Service from the security policy**

Use the VMware vCenter Web Client console to remove the McAfee MOVE AntiVirus Guest Introspection Service from the security policy.

**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 needed, 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**

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**

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 in this order.
   - MOVE AntiVirus
   - MOVE AntiVirus Common
   - vSphere Connector
   - MDCC
From the Extensions tab under McAfee group, select Help Content.

Click Remove next to the mvav_help 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 registered the vCenter with vShield Manager.

Task
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 Deployment Status Details and Task Status Details for the removal on the McAfee ePO server.

Table 7-1 Deployment 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>
</tbody>
</table>
Table 7-1 Deployment status (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Name</td>
<td>Specifies the name of VMware vCenter account that is registered with McAfee ePO.</td>
</tr>
<tr>
<td>Hypervisors</td>
<td>Specifies the name of the hypervisor.</td>
</tr>
</tbody>
</table>

Table 7-2 Task status

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node Type</td>
<td>Specifies whether the node is a McAfee MOVE AntiVirus SVM or a hypervisor.</td>
</tr>
<tr>
<td>Task Type</td>
<td>Specifies the set of internal tasks that happen in 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.</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>
<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**

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 in this order.
   - MOVE AntiVirus
   - MOVE AntiVirus Common
   - vSphere Connector
   - MDCC

5. From the **Extensions** tab under **McAfee** group, select **Help Content**.

6. Click **Remove** next to the **mvav_help** extension.
Index

A
- account 92
  - NSX Manager 75
  - registering 18, 72
  - VMware vCenter 72
  - vShield Manager 96
- Agentless
  - configuration 65
  - deployment 70
  - installation 65
- assignment
  - rules, infrastructure group 37
  - SVM Manager 30
- ATD
  - enabling and configuring 50
- autoscale
  - enabling option 41
- autoscale SVMs
  - update 43
  - upgrading 58
- autoscaling
  - configuring 41
  - SVM 14

C
- checking in
  - SVM 94
  - SVM Manager 21
- client
  - creating uninstallation task 61
  - deploy to XenDesktop 47
  - deployment 44
  - removing 62
  - uninstall task, create and assign 62
- client deployment
  - viewing details 45
- client tasks
  - assign uninstall task 62
  - assigning 27
  - create client upgrade task 60
  - create SVM deployment task 26
  - creating client uninstallation task 61
- common configuration
  - setting up 74, 93
- configuration
  - IP Pool 95
  - McAfee ePO details 19
  - security tags 85
  - SVM OVF template 32, 35
  - tagging 86
  - TIE and ATD 50
  - VSE policies 27
- connector, choosing 18, 72, 92

D
- deployment
  - McAfee ePO 91
  - McAfee MOVE AntiVirus 44
  - McAfee MOVE AntiVirus service 78
  - MOVE AntiVirus service 70
  - Multi-Platform 15
  - options 66
  - overview 14, 15, 70
  - SVM 97
  - SVM Manager, Hyper-V environment 25
  - SVM Manager, VMware ESXi environment 22
- deployment type
  - client 45
  - MOVE AntiVirus SVM 100
  - SVM Manager 23
  - download locations 16, 66, 67

E
- export utility
  - OVF template 35
- extensions
  - installing 17, 71, 91, 104
  - removing 110, 112
  - uninstalling 63
  - upgrading 56

H
- hypervisors 18, 72, 92
infrastructure group
creating 20, 37
installation
agentless 65, 70
client deployment overview 44
deploy to XenDesktop 47
download software 16, 66, 67
Multi-Platform 13
upgrade ePolicy Orchestrator extension 56
upgrade scenario 59
installing
extension 17, 71, 91, 104
integration
TIE 48
IP Pool
configuring 95

LDAP server
configuring and registering 91

McAfee ePO
installation 17, 71, 91
McAfee MOVE AntiVirus
Agentless 109
deploying 44
Generate certificates 46
removing 62
software packages 16, 66, 67
uninstalling 111
upgrade strategies 55
McAfee MOVE AntiVirus service
deploying 78
removing 109
MOVE AntiVirus service
deploying 70
registering 76
upgrading 106, 107
MOVE AntiVirus SVM
checking in 74
Multi-Platform
configuration 13
deployment 15
installation 13

NSX Manager
editing 75
editing registration 75
removing 110

NSX tagging
enabling 85, 86

open virtualization format
deployment options 66
properties 68
overview
deployment 14, 15
deployment process 70

permission sets
McAfee ePO 97
permissions
VMware vCenter 91
policy
assigning 28–30, 41, 47, 106
policy export
on-access scan 77

registering
account 92
registration
MOVE AntiVirus service 76
vCenter server 71
VMware vCenter account 18, 92
requirements
system and hardware 7
rollback, SVM deployment 100

scan policies
exporting 77
scenario
service composer 86
security group
applying security policy 84
configuring 82
creating 83
security policy
assigning to security group 84
configuring 84
creating 82
security tags
enabling 85
security updates, SVM 67
security virtual appliance
deploying 104
SVM
assigning 13, 28, 47
autoscaling 14
SVM (continued)
checking in 94
deploying 37, 70, 97
export utility 35
security updates 67
upgrading 57, 104
uploading 36
SVM deployment
rollback 100
viewing details 100
SVM export
viewing details 34
SVM Manager
adding and editing 30
checking in 21
deploying 20
deployment, Hyper-V environment 25
deployment, VMware ESXi environment 22
removing 62
setting up 25
SVM Manager assignment
adding 29
SVM Manager deployment
viewing details 23
SVM OVF template
creating 32, 35
T
tags
defining 18, 72, 92
TIE
enabling and configuring 50
integrating 48
U
uninstallation process 109 (continued)
extension 63
McAfee MOVE AntiVirus 61, 111
update task
autoscale SVMs 43
upgrade scenarios
create client upgrade task 60
ePolicy Orchestrator extension 56
higher downtime scenario 59
higher resource scenario 59
non-persistent VM 59
persistent VM 59
strategy 55
SVM 57, 58
upgrade task
create and assign 60
manually 104
SVM 104
V
virtual machines
boot status 18, 72, 92
virtual properties, displaying 18, 72, 92
VMware vCenter
registering 91
VMware vCenter account configuration
Agentless installation in NSX environment 72
Agentless installation in vCNS environment 92
Multi-Platform installation 18
vShield Manager
configuring and registering 91
editing 96
editing registration 96
X
XenDesktop
deploy client 47