Product 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 **Overview of McAfee MOVE AntiVirus**  
   - Key features of McAfee MOVE AntiVirus ............................................ 6  
   - How McAfee MOVE AntiVirus works .................................................. 7  
     - Multi-Platform components ......................................................... 7  
     - Agentless components ................................................................ 8  
   - The role of the McAfee MOVE AntiVirus SVM (Multi-Platform) ............... 9  
   - The role of the McAfee MOVE AntiVirus SVM (Agentless) ..................... 9  
   - The role of the SVM Manager (Multi-Platform) .................................. 9  
   - The role of the security management platforms .................................. 9  

2 **Configuring McAfee MOVE AntiVirus** .............................................. 11  
   - The importance of creating a security strategy ................................ 11  
   - McAfee ePO features leveraged by McAfee MOVE AntiVirus ............... 12  
     - About the McAfee ePO System Tree ............................................. 13  
     - Using client tasks with McAfee MOVE AntiVirus .......................... 14  
   - Using policies in McAfee ePO .......................................................... 15  
     - Create a policy ............................................................................. 15  
     - Assign a policy ............................................................................ 16  
     - How the policy assignment works (Agentless) .............................. 16  
     - Configuring policies ..................................................................... 17  
   - Configuring permissions sets ............................................................ 17  
     - Using permission sets ................................................................... 18  
     - Configure permission sets ............................................................. 19  
     - Configuring McAfee MOVE AntiVirus settings ............................... 19  
   - Scanning for threats on client computers ........................................ 24  
     - Types of scans ............................................................................... 24  
     - How McAfee GTI works ............................................................... 24  
     - Configure common scan settings .................................................. 25  
     - On-access scanning ...................................................................... 26  
     - On-demand scanning ..................................................................... 31  
   - Configure deferred scan settings (Multi-Platform only) ...................... 37  
     - Client notifications for deferred scans .......................................... 38  
   - Scan Diagnosis ................................................................................ 38  
     - Identify frequently scanned items from McAfee ePO (Agentless) .... 38  
     - Identify frequently scanned items from command line (Agentless) ... 39  
     - Identify frequently scanned items from McAfee ePO (Multi-Platform) 41  
     - Identify frequently scanned items from command line (Multi-Platform) 41  

3 **Managing McAfee MOVE AntiVirus** ............................................... 45  
   - Keeping your protection up to date .................................................. 45  
   - Responding to detections ................................................................ 45  
     - Unwanted program detection ......................................................... 45  
     - On-access scan detections ............................................................. 46  
     - On-demand scan detections .......................................................... 46  
   - Quarantined items .......................................................................... 46
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the settings for quarantine</td>
<td>47</td>
</tr>
<tr>
<td>Restore quarantined items (Multi-Platform)</td>
<td>47</td>
</tr>
<tr>
<td>How quarantine works (Agentless)</td>
<td>48</td>
</tr>
<tr>
<td>Restore a file</td>
<td>50</td>
</tr>
<tr>
<td>How tagging works in an NSX environment (Agentless)</td>
<td>51</td>
</tr>
<tr>
<td>Self-protection</td>
<td>51</td>
</tr>
<tr>
<td>Events, responses, and McAfee MOVE AntiVirus</td>
<td>53</td>
</tr>
<tr>
<td>Analyzing your protection</td>
<td>53</td>
</tr>
<tr>
<td>Integrating TIE and Advanced Threat Defense</td>
<td>54</td>
</tr>
<tr>
<td>How Threat Intelligence Exchange works</td>
<td>54</td>
</tr>
<tr>
<td>How Advanced Threat Defense works</td>
<td>55</td>
</tr>
<tr>
<td>Scenarios for using Threat Intelligence Exchange</td>
<td>56</td>
</tr>
<tr>
<td>How a reputation is determined</td>
<td>56</td>
</tr>
<tr>
<td>Monitoring activity in your environment</td>
<td>59</td>
</tr>
<tr>
<td>Monitoring activity with McAfee ePO</td>
<td>59</td>
</tr>
<tr>
<td>McAfee MOVE AntiVirus dashboard</td>
<td>59</td>
</tr>
<tr>
<td>Check visibility and health details of the SVM</td>
<td>60</td>
</tr>
<tr>
<td>Check predefined queries</td>
<td>60</td>
</tr>
<tr>
<td>Predefined Multi-Platform queries</td>
<td>60</td>
</tr>
<tr>
<td>Predefined Agentless queries</td>
<td>63</td>
</tr>
<tr>
<td>McAfee MOVE AntiVirus server tasks</td>
<td>64</td>
</tr>
<tr>
<td>(Multi-Platform) MOVE AntiVirus : Generate Certificates</td>
<td>64</td>
</tr>
<tr>
<td>(Agentless) MOVE AntiVirus: Compute licensing information</td>
<td>64</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>65</td>
</tr>
<tr>
<td>Error codes</td>
<td>65</td>
</tr>
<tr>
<td>Product Area: McAfee MOVE AntiVirus extension</td>
<td>65</td>
</tr>
<tr>
<td>Product Area: McAfee MOVE AntiVirus client (Multi-Platform)</td>
<td>68</td>
</tr>
<tr>
<td>Product Area: McAfee MOVE AntiVirus SVM (Multi-Platform)</td>
<td>69</td>
</tr>
<tr>
<td>Product Area: McAfee MOVE AntiVirus SVM (Agentless)</td>
<td>73</td>
</tr>
<tr>
<td>Frequently asked questions</td>
<td>75</td>
</tr>
<tr>
<td>Index</td>
<td>83</td>
</tr>
</tbody>
</table>
Overview of McAfee MOVE AntiVirus

McAfee® Management for Optimized Virtual Environments AntiVirus (McAfee® MOVE AntiVirus) is an anti-virus solution for virtual environments. It provides protection and performance for your organization without having to install an anti-virus application on every virtual machine (VM).

McAfee MOVE AntiVirus detects threats, then protects your environment based on settings that you configure.

You can configure the software as a standalone product, or you can use McAfee® ePolicy Orchestrator® (McAfee® ePO) to configure, manage, and enforce your policies. Once configured, you can use queries and dashboards to track activity and detections.

The software includes two deployment options, Multi-Platform and Agentless. Both options provide consistent protection and are managed and reported on by McAfee ePO.

Multi-Platform deployment

Multi-Platform is an agent-based deployment option that offloads all scanning to a dedicated Security Virtual Machine (SVM) that runs McAfee® VirusScan® Enterprise software. Guest VMs are no longer required to run anti-virus software locally, which improves performance for anti-virus scanning, and increases VM density per hypervisor.

Multi-Platform deployment:

- Supports on-access scanning and on-demand scanning to examine files for potential threats.
- Uses McAfee® Threat Intelligence Exchange (TIE) and McAfee® Advanced Threat Defense for in-depth analysis of suspect files using local, global, and enterprise-level caches, and to define threat reputation and respond to threats.
- Uses McAfee ePO to manage the McAfee MOVE AntiVirus configuration on client systems, McAfee MOVE AntiVirus SVM, and SVM Manager.
- Uses SVM Manager to automatically assign the SVM to the clients for simplified administrative management, monitoring the health of SVMs, and load-balancing of SVMs. See the installation guide for instructions about deploying and configuring the autoscale SVM.
- Uses McAfee® Agent for policy and event handling.
- Uses McAfee ePO for reports on viruses that are discovered on the VMs.

Agentless deployment

This deployment method integrates with VMware NSX Manager and VMware vShield. It protects your virtual environment from malware without a McAfee Agent for easy deployment and setup. This deployment provides virus protection for VMs on the hypervisor.
Agentless deployment:

- Uses the VMware vShield Endpoint API to receive scan requests from VMs on the hypervisor.
- Relies on McAfee® Endpoint Security for Linux Threat Prevention for SVM scanning and updates.
- Uses McAfee ePO to manage the McAfee MOVE AntiVirus configuration on the SVM.
- Uses McAfee Agent for policy and event handling.
- Uses McAfee ePO for reports on viruses that are discovered on the VMs.

Contents

- Key features of McAfee MOVE AntiVirus
- How McAfee MOVE AntiVirus works

Key features of McAfee MOVE AntiVirus

McAfee MOVE AntiVirus features are important for the security, protection, and performance of your enterprise systems.

Some features are shared by the Multi-Platform and Agentless deployment options, and some features apply to only one option.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Multi-Platform</th>
<th>Agentless</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized management</td>
<td>McAfee MOVE AntiVirus integrates fully into McAfee ePO for automated security reporting, monitoring, deployment, and policy administration.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Data Center visibility</td>
<td>vSphere Connector, part of the Data Center Security suite, provides a complete view into virtual datacenters and imports key properties like servers, hypervisors, and VMs through McAfee ePO.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>On-access scanning</td>
<td>Examine files as they are accessed, providing continuous, real-time detection of threats.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>On-demand scanning</td>
<td>Examine all files on VMs to find potential threats any time or on a schedule.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Targeted on-demand scanning</td>
<td>Optimize file scanning for files where the previous scanning is timed out for reasons such as large file size, file structure, and file composition.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SVM Manager</td>
<td>Automatically assign the SVM to Multi-Platform clients for simplified administrative management, monitoring the health of SVMs, and load-balancing of SVMs.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>SVM autoscaling</td>
<td>The SVMs automatically scale up and down depending on the number of endpoints connected. 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.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Scan diagnostics</td>
<td>Run the scan diagnostic tool to easily find frequently scanned files, extensions, and VMs, then use the results to exclude them from being scanned, improving performance.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Multi-Platform</td>
<td>Agentless</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------</td>
<td>-----------</td>
</tr>
<tr>
<td>RAM disk for scanning</td>
<td>RAM disk is used by the OSS for file scanning and it significantly reduces the disk I/O on the offline scan server. By default, RAM disk is enabled in the McAfee ePO server. RAM disk is created by the OSS and it improves the OSS performance by enhancing the scan time.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Threat Intelligence Exchange</td>
<td>Determine a file's reputation risk score with seamless integration of TIE, McAfee ePO, and McAfee MOVE AntiVirus.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Advanced Threat Defense integration</td>
<td>Protect your client systems and network against malware and Advanced Persistent Threats (APTs) with the multi-level threat detection capabilities of ATD.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Optimized scanning</td>
<td>Minimize the performance impact on virtual servers with enhanced scan avoidance and scanning based on overall workload of the hypervisor.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NSX Manager-based deployment</td>
<td>Register the SVM with VMware NSX Manager and automatically deploy it to a host to provide virus protection for VMs on a new hypervisor when the hypervisor is added to the cluster.</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>VMware vCNS-based deployment</td>
<td>Deploy the SVM to hypervisor or hypervisors in vCNS environment to provide virus protection for VMs on a hypervisor.</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Endpoint Scan and Security reports</td>
<td>With the vSphere Connector software, quickly retrieve Endpoint Scan Report and Endpoint Security Report of all registered endpoints.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

How McAfee MOVE AntiVirus works

McAfee MOVE AntiVirus detects, resolves, and logs information about detected threats. The software is installed on McAfee MOVE AntiVirus Security Virtual Machine (SVM) to perform these tasks.

The software includes two deployment options, Multi-Platform and Agentless. Both options provide consistent protection and are managed and reported on by McAfee ePO.

Multi-Platform components

Each component performs specific functions to keep your environment protected.

**ePolicy Orchestrator** — A management platform that communicates with the McAfee Agent, manages the Multi-Platform configuration, and provides reports on malware discovered in your virtual environment.

**Hypervisor** — A virtual operating platform that allows multiple operating systems to run concurrently on a hosted system and manages the execution of the guest operating system.

**McAfee Agent** — A client-side component that communicates with McAfee ePO, applies policies to each VM, and deploys the McAfee MOVE AntiVirus client.

**McAfee MOVE AntiVirus client** — The client software that allows VMs to work with the Security Virtual Machine (SVM) for file scanning and malware detection. Enforces actions on the client when a threat is detected.

**McAfee MOVE AntiVirus SVM** — The Security Virtual Machine VM that provides offloaded scanning support for VMs, minimizing the performance impact on virtual desktops.

**SVM Manager** — A load balancing component that automatically assigns SVM to Multi-Platform clients based on configurable parameters like scan server load, McAfee ePO tags, and IP address ranges.
**McAfee MOVE AntiVirus Meta Package extension** — The product extension that provides policies and controls for configuring and managing the self-protection for the product’s command line interface. You can enable events and logging details of the McAfee MOVE AntiVirus client through McAfee ePO. It provides policies and controls for configuring and managing components such as SVM Manager, SVM Settings, on-access and on-demand scanning, and shared cloud solutions. It provides the configurations required for managing the McAfee MOVE AntiVirus SVM through McAfee ePO.

**VirusScan Enterprise** — Anti-virus software that enables anti-virus scanning for the SVM virtual machine and communicates with the McAfee GTI servers.

**vSphere Connector** — A Data Center Connector that helps you discover and import your virtual infrastructure using McAfee ePO. You can also view the virtualization properties and protection status of your virtual machines, and manage them.

### Agentless components

Each component performs specific functions to keep your environment protected.

**ePolicy Orchestrator** — A management platform that allows you to configure policies to manage Agentless configuration and provides reports on malware discovered in your virtual environment.

**Security Virtual Machine (SVM)** — The McAfee MOVE AntiVirus service package that provides anti-virus protection for VMs and communicates with the loadable kernel module on the hypervisor, McAfee ePO, and the McAfee GTI servers. The SVM is the only system directly managed by McAfee ePO. Endpoint Security for Linux Threat Prevention, McAfee Agent, and McAfee MOVE AntiVirus (Agentless) are pre-installed.

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

**McAfee GTI (Global Threat Intelligence)** — A comprehensive, real-time, cloud-based threat intelligence service that classifies suspicious files that are found on the file system. When the real-time malware defense detects a suspicious program, it sends a DNS request for analysis to a central database server hosted by McAfee Labs.

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

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

**vCloud Networking and Security Manager (vCNS)** — A centralized network management component that manages the vShield components for the SVM and VMware vShield Endpoint, and monitors the health of the SVM.

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

**Virtual Machines (VMs)** — Completely isolated guest operating system installations in a normal host operating system that support both virtual desktops and virtual servers.
The role of the McAfee MOVE AntiVirus SVM (Multi-Platform)
The Multi-Platform is an agent-based deployment option. It offloads all scanning to a dedicated Security Virtual Machine (SVM) that runs VirusScan Enterprise software. Guest VMs are no longer required to run anti-virus software locally, which improves performance for anti-virus scanning, and increases VM density per hypervisor.

The role of the McAfee MOVE AntiVirus SVM (Agentless)
McAfee MOVE AntiVirus SVM provides anti-virus protection for VMs and communicates with the loadable kernel module on the hypervisor, McAfee ePO, and the McAfee® Global Threat Intelligence™ (McAfee GTI) servers.
The SVM is the only system directly managed by McAfee ePO. Endpoint Security for Linux Threat Prevention, McAfee Agent, and McAfee MOVE AntiVirus are preinstalled.

The role of the SVM Manager (Multi-Platform)
The SVM Manager automatically assigns the McAfee MOVE AntiVirus SVM to McAfee MOVE AntiVirus clients based on configurable parameters like scan server load, McAfee ePO tags, and IP address ranges. The SVM Manager also assigns the McAfee MOVE AntiVirus SVM to McAfee MOVE AntiVirus clients that do not have tags and are not in IP address ranges.

The role of the security management platforms
This deployment provides virus protection for virtual machines on a hypervisor. You use the McAfee ePO console to deploy the McAfee MOVE AntiVirus SVM to hypervisors or to a whole vCenter.
(Agentless only) You can register the McAfee MOVE AntiVirus SVM with VMware NSX Manager and deploy it automatically to one or more clusters. This deployment automatically provides virus protection for virtual machines on a new hypervisor from the moment the hypervisor is added to the cluster.
Configuring McAfee MOVE AntiVirus

Configure McAfee MOVE AntiVirus settings to prevent malware access, keep your protection up to date, and scan for malware on client systems. McAfee MOVE AntiVirus provides two types of file scanning, on-access and on-demand. You can customize the scan settings based on your demands and requirements.

Contents
- The importance of creating a security strategy
- McAfee ePO features leveraged by McAfee MOVE AntiVirus
- Using policies in McAfee ePO
- Configuring permissions sets
- Scanning for threats on client computers
- Configure deferred scan settings (Multi-Platform only)
- Scan Diagnosis

The importance of creating a security strategy

Protecting your virtual systems from malware requires a well-planned strategy: define threat prevention and detection, response to threats, and ongoing analysis and tuning.

Prevent — Avoiding threats

Define your security requirements to make sure that your data sources are protected. Then, develop an effective scan strategy to stop intrusions before they gain access to your environment.

Configure these features to prevent intrusions:

- **Self-Protection** — (Multi-Platform only) One of the first things that malware tries to do during an attack is to disable your system security software. Configure **Self-Protection** for McAfee MOVE AntiVirus (Multi-Platform) to prevent McAfee MOVE AntiVirus service, files, and registries from being stopped or changed.

- **Common scan options** — Enable McAfee MOVE AntiVirus and configure options that apply to all scans, including:
  - (Multi-Platform) Quarantine location and the number of days to keep quarantined items before automatically deleting them
  - (Agentless) Quarantine network share where the quarantined files are stored

- **Scan Diagnostics** client task — Run the scan diagnostic tool or use McAfee ePO to calculate and display frequently scanned files, extensions, processes, and VMs. You can use the results to exclude the items from being scanned.
Detect — Finding threats
Develop an effective strategy to detect intrusions when they occur. Configure these features to detect threats:

• **On-Access Scan** — Scan for threats as files are read from or written to disk.

• **On-Demand Scan** — Run immediate and scheduled scans, including scanning for malware-related registry entries that weren't previously cleaned.

• **Targeted On-Demand Scan** — Select a system or a group of systems from the System Tree where to initiate the on-demand scan.

Respond — Handling threats
Use product log files, automatic actions, and other notification features to determine the best way to handle detections.

• **Actions** — Configure what happens in response to a detection.

• **Alerts** — Specify how McAfee MOVE AntiVirus notifies you when detections occur, including alerting options and logging.

Tune — Monitoring, analyzing, and fine-tuning your protection
Monitor and analyze your configuration to improve system and network performance, and enhance virus protection, if needed. Use these tools and features:

• **Queries, dashboards, and server tasks (McAfee ePO)** — Monitor scanning activity and detections.

• **Log files** — View a history of detected items. Analyzing this information might reveal that you must enhance your protection or change the configuration to improve system performance.

• **Scan policies** — Analyze log files or queries and change policies to increase performance or virus protection, if needed. For example, you can improve performance by configuring exclusions, high- and low-risk process scanning, and disabling scan on write.

• **Scan Diagnostics** reports — Run and view these scan diagnostic queries:
  • Top 10 Scanned File Extensions for each SVM
  • Top 10 Scanned Files for each SVM
  • Top 10 Scanned Virtual Machines for each SVM
  • (Multi-Platform only) Top 10 Scanned Processes for each SVM

**McAfee ePO features leveraged by McAfee MOVE AntiVirus**
McAfee MOVE AntiVirus leverages these features in the McAfee ePO environment.

<table>
<thead>
<tr>
<th>McAfee ePO feature</th>
<th>McAfee MOVE AntiVirus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies</td>
<td>Adds predefined policies to the Policy Catalog.</td>
</tr>
<tr>
<td>Client tasks</td>
<td>Adds predefined client tasks to the Client Task Catalog.</td>
</tr>
<tr>
<td>Dashboards and monitors</td>
<td>Adds predefined dashboards and monitors.</td>
</tr>
<tr>
<td>Permission sets</td>
<td>Adds a McAfee MOVE AntiVirus permission group to each permission set.</td>
</tr>
</tbody>
</table>
McAfee ePO feature | McAfee MOVE AntiVirus
---|---
Queries and reports | Adds:
• Predefined queries to the Query list.
  Query names include Multi-Platform, Agentless, and SVM name for easier filtering.
• **Predefined Result Types and Properties** for creating and narrowing the scope of custom queries.

Server tasks | Adds predefined server tasks to the Server Tasks list in Automation.

Threat Event Log | Adds McAfee MOVE AntiVirus events that you can filter and view.

**About the McAfee ePO System Tree**

The System Tree is a graphical representation of how your managed network is organized. McAfee ePO enables you to automate and customize system organization. The structure that you put in place affects how security policies are inherited and enforced throughout your environment.

You can perform these McAfee MOVE AntiVirus functions from the System Tree.

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies</td>
<td>MOVE AntiVirus Common 4.6.0</td>
<td>Includes policy setting to prevent McAfee MOVE AntiVirus service, files, and registries from being stopped or modified. You can also specify the settings required for events and logging for Multi-Platform.</td>
</tr>
<tr>
<td></td>
<td>MOVE AntiVirus 4.6.0</td>
<td>Options</td>
</tr>
<tr>
<td></td>
<td>MOVE AntiVirus 4.6.0</td>
<td>Options</td>
</tr>
<tr>
<td></td>
<td>MOVE AntiVirus 4.6.0</td>
<td>Options</td>
</tr>
<tr>
<td></td>
<td>MOVE AntiVirus 4.6.0</td>
<td>Options</td>
</tr>
<tr>
<td></td>
<td>MOVE AntiVirus 4.6.0</td>
<td>SVM Manager Settings</td>
</tr>
<tr>
<td></td>
<td>MOVE AntiVirus 4.6.0</td>
<td>SVM Settings</td>
</tr>
<tr>
<td>Client Tasks (Multi-Platform)</td>
<td>Restore from Quarantine</td>
<td>Performs actions on quarantined items. For example, you can restore a quarantined item after downloading a later version of the DAT that contains information that cleans the threat.</td>
</tr>
<tr>
<td></td>
<td>Targeted On-Demand Scan</td>
<td>Optimizes file scanning for files where the previous scan timed out for reasons such as large file size, file structure, and file composition.</td>
</tr>
<tr>
<td></td>
<td>Scan Diagnostics</td>
<td>Run the scan diagnostic task to easily find frequently scanned files, extensions, and VMs, then use the results to exclude these items from being scanned.</td>
</tr>
<tr>
<td></td>
<td>Check SVM Assignment</td>
<td>Checks whether an SVM is assigned to the client system to protect it.</td>
</tr>
</tbody>
</table>
### Function | Category | Description
--- | --- | ---
Check SVM Connectivity |  | Checks the connectivity status between an SVM and the client system.
Check SVM Manager Connectivity |  | Checks the connectivity status between the SVM Manager and the client system.
Perform EICAR Test |  | Performs an EICAR test on the client system.

### Client Tasks (Agentless) | Scan Diagnostics | Run the scan diagnostic task to easily find frequently scanned files, extensions, and VMs, then use the results to exclude these items from being scanned.

### Targeted ODS | Targeted On-Demand Scan | Optimizes file scanning for files where the previous scan timed out for reasons such as large file size, file structure, and file composition.

## Using client tasks with McAfee MOVE AntiVirus

Use client tasks to automate system management in your McAfee ePO environment. For example, you can configure a client task to deploy product updates, run a diagnostic scan, or run an on-demand scan.

Depending on your permissions, you can use predefined client tasks as is, edit them, or create custom client tasks.

McAfee MOVE AntiVirus adds these predefined client tasks to the Client Task Catalog.

### Function | Category | Description
--- | --- | ---
Client Tasks (Multi-Platform) | Restore from Quarantine | Performs actions on quarantined items. For example, you can restore an item after downloading a later version of the DAT that contains information that cleans the threat.
Targeted On-Demand Scan |  | Optimizes file scanning for files where the previous scanning is timed out for reasons such as large file size, file structure, and file composition.
Scan Diagnostics |  | Run the scan diagnostic task to easily find frequently scanned files, processes, extensions, and VMs, then use these results to exclude them from being scanned.
A good set of exclusions improves the performance of the virtual infrastructure.
Check SVM Assignment |  | Checks whether an SVM is assigned to the client system to protect it.
Check SVM Connectivity |  | Checks the connectivity status between an SVM and the client system.
Check SVM Manager Connectivity |  | Checks the connectivity status between the SVM Manager and the client system.
Perform EICAR Test |  | Performs an EICAR test on the client system.
Client Tasks (Agentless) | Scan Diagnostics | Run the scan diagnostic task to easily find frequently scanned files, extensions, and VMs, then use the results to exclude these items from being scanned.

For information about creating and using client tasks and the Client Task Catalog, see the McAfee ePO documentation.
Using policies in McAfee ePO

Policies enable you to configure managed products and apply the configuration to systems in your network, all from the McAfee ePO console.

Policies are collections of settings that you create, configure, and apply, then enforce. Most policy settings correspond to settings that you configure for the McAfee MOVE AntiVirus client systems. Other policy settings are the primary interface for configuring and deploying the McAfee MOVE AntiVirus SVM and its components.

McAfee MOVE AntiVirus adds these categories to the Policy Catalog.

**Table 2-1 McAfee MOVE AntiVirus categories**

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Options</td>
<td>Configures the Quarantine Manager options that apply to both on-access scanner and on-demand scanner. Also, specifies the SVM assignment details for Multi-Platform.</td>
</tr>
<tr>
<td>On Access Scan</td>
<td>Examines files on the computer as the user accesses them, and provides continuous, real-time detection of threats.</td>
</tr>
<tr>
<td>On Demand Scan</td>
<td>Configures the on-demand scan settings for the preconfigured scans that run on the SVM.</td>
</tr>
<tr>
<td>Share Cloud Solutions (Multi-Platform only)</td>
<td>Enables you to specify that files and certificates with specific reputations are allowed to perform certain scan actions, as specified by scan rules.</td>
</tr>
<tr>
<td>SVM Manager Settings (Multi-Platform only)</td>
<td>Configures the SVM Manager and autoscale settings required for SVM deployment and management.</td>
</tr>
<tr>
<td>SVM Settings</td>
<td>Specifies settings that apply to SVM configuration, scanning options, on-demand scan configurations required for SVM, and scan performance.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Options</td>
<td>Allows you to configure the settings to defend files, services, and registry keys on virtual machines and to log events and alerts.</td>
</tr>
</tbody>
</table>

In each category, these predefined policies are available:

**Table 2-3 McAfee MOVE AntiVirus predefined policies**

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee Default</td>
<td>Defines the default policy that takes effect if no other policy is applied. You can duplicate this policy, but you can't delete or modify it.</td>
</tr>
<tr>
<td>My Default</td>
<td>Specifies predefined settings for the category.</td>
</tr>
</tbody>
</table>

You can use predefined policies as is, edit the My Default policies, or create custom policies.

For information about creating and using policies and the Policy Catalog, see the McAfee ePO documentation.

**Create a policy**

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

**Before you begin**

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

By default, policies created in McAfee ePO are not assigned to any groups or systems. When you create a policy, you add a custom policy to the Policy Catalog. You can create policies before or after a product is deployed.
Task
1 Log on to McAfee ePO as an administrator.
2 Select Menu | Policy | Policy Catalog, then select MOVE AntiVirus 4.6.0 or MOVE AntiVirus Common 4.6.0 from the Product drop-down list.
3 Click New Policy.
4 On the Create a new policy dialog box, configure the options, as required, then click OK.
5 Click the new policy that is created, then configure the policy options, as required.
6 Click Save.

Assign a policy
You must assign a policy to the client systems for it to take effect.

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 In the System Tree, select the group containing the virtual machines where you want to apply the policy.
3 Select Menu | Systems | System Tree | Assigned Policies.
4 From the Product drop-down list, select MOVE AntiVirus 4.6.0 or MOVE AntiVirus Common 4.6.0.
5 In the Actions column of the McAfee Default policy, select Edit assignments.
6 In the Inherit from list on the Policy Assignments page, select Break inheritance and assign the policy and settings below.
7 In the Assigned Policy list, select the policy you created.
8 Click Save.
9 To apply the policy immediately, send wake-up agent call.

The policies are not modified on client systems until the next agent-server communication that includes a Collect and Send Properties operation. This can be initiated from the agent on the client, or by sending wake-up agent call from McAfee ePO.

How the policy assignment works (Agentless)
VM-based scan configuration is enabled by default. The McAfee ePO administrator can enforce unique scan policies with exclusion 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.

The on-access and on-demand scan policies can be applied to SVMs or to a specific virtual machine, or group. With VM-based scan configuration enabled by default, all VMs are protected by the on-access and on-demand scan policies, which are assigned to VM or group.

The on-access and on-demand scan policies can be assigned to the system using system-based assignment or rule-based assignment in McAfee ePO.
Update SVMs with scan policies (Agentless)
You can run the policy collector to update the target SVMs with the latest on-access and on-demand scan policies. The policies and updates are enforced to SVM in the default policy collection interval, which is 60 minutes.

Best practice: Specify the policy collection interval for your environment, as needed.

Task
1. Select Menu | Automation | MOVE AntiVirus Deployment | Configuration | Server Settings.
2. Click Run next to Run policy collector.
   The Policy collection completed successfully message appears when policies are successfully collected.
   You can change the policy enforcement interval by navigating to Menu | Automation | MOVE AntiVirus Deployment | Configuration | Server Settings | Edit. You can also view the task log for policy collection (MOVE AntiVirus:Policy collection task) by navigating to Menu | Automation | Server Task Log. The policy collection task log is updated in the default policy collection interval, which is 60 minutes.
3. Send wake-up agent call to the target SVMs.

Configuring policies
You can configure the McAfee MOVE AntiVirus client and SVM behavior with policy settings.

<table>
<thead>
<tr>
<th>Policies for client</th>
<th>Policies for SVM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Which SVM a client uses.</td>
<td>Maximum size of the server cache.</td>
</tr>
<tr>
<td>When files are scanned.</td>
<td>The number of concurrent scans that an SVM policy can support.</td>
</tr>
<tr>
<td>Which files and programs to exclude from scanning.</td>
<td>Which port the SVM listens to for scan requests from clients.</td>
</tr>
<tr>
<td>Where to send alerts.</td>
<td>The number assigned to a log file and size.</td>
</tr>
<tr>
<td>What to do when a threat is found.</td>
<td>Which types of files to scan.</td>
</tr>
<tr>
<td>How to handle quarantined files.</td>
<td>McAfee GTI sensitivity level.</td>
</tr>
<tr>
<td>How the SVM operates.</td>
<td>On-demand and on-access scan settings.</td>
</tr>
</tbody>
</table>

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

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

For more information about permission sets, see the product documentation for your version of McAfee ePO.

McAfee MOVE AntiVirus permission set
The McAfee MOVE AntiVirus software adds sections to the permission sets including the MOVE AntiVirus SVM Manager role.
Global administrators must grant permissions to users for the MOVE AntiVirus Common, MOVE AntiVirus Deployment, MOVE AntiVirus General, and MOVE AntiVirus Policy Permission sections, because no permissions are granted by default.

<table>
<thead>
<tr>
<th>Permission section</th>
<th>Permission set</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOVE AntiVirus Common</td>
<td>View policy and task settings</td>
<td>User can view the policy and task settings that are available in the MOVE AntiVirus Common extension in McAfee ePO.</td>
</tr>
<tr>
<td></td>
<td>View and change policy and task settings</td>
<td>User can view and edit the policy and task settings that are available in the MOVE AntiVirus Common extension in McAfee ePO.</td>
</tr>
<tr>
<td>MOVE AntiVirus Deployment</td>
<td>View/Edit Deployment MOVE AntiVirus</td>
<td>User can view and edit the MOVE AntiVirus Deployment configuration details in McAfee ePO.</td>
</tr>
<tr>
<td></td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td>MOVE AntiVirus General</td>
<td>Run System Tag Info Command</td>
<td>This permission is used by the SVM Manager to fetch the system tag information, which is configured and assigned to the client systems.</td>
</tr>
<tr>
<td>MOVE AntiVirus Policy</td>
<td>View policy and task settings</td>
<td>User can view the policy and tasks settings that are available in the MOVE AntiVirus extension in McAfee ePO.</td>
</tr>
<tr>
<td>Permission</td>
<td>View and change policy and task settings</td>
<td>User can view and edit the policy and tasks settings that are available in the MOVE AntiVirus extension in McAfee ePO.</td>
</tr>
</tbody>
</table>

**Other required permissions**

The global administrator must give McAfee ePO permissions to handle other areas that work with McAfee MOVE AntiVirus including queries, dashboards, and the Threat Event Log.

<table>
<thead>
<tr>
<th>For these features...</th>
<th>These permissions sets are required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboards</td>
<td>Dashboards, Queries and Reports</td>
</tr>
<tr>
<td>Queries</td>
<td>Queries and Reports</td>
</tr>
<tr>
<td>Policies</td>
<td>System Tree access, Policy Assignment Rules</td>
</tr>
<tr>
<td>Events on virtual machines</td>
<td>Systems, System Tree access, Threat Event Log</td>
</tr>
</tbody>
</table>

**Using permission sets**

A permission set specifies all permissions that apply to one object and controls users' level of access to features.

McAfee MOVE AntiVirus adds a permission group MOVE AntiVirus SVM Manager to each permission set.

Permission groups define the access rights to the features. McAfee ePO grants all permissions for all products and features to global administrators. Administrators then assign user roles to existing permission sets or create permission sets.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Required permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic responses</td>
<td>Automatic Responses, Event Notifications, plus any feature-specific permissions</td>
</tr>
<tr>
<td></td>
<td>depending on the feature used (such as System Tree or queries).</td>
</tr>
<tr>
<td>Client tasks</td>
<td>• McAfee MOVE AntiVirus (Multi-Platform) Tasks</td>
</tr>
<tr>
<td></td>
<td>• McAfee MOVE AntiVirus (Agentless) Tasks</td>
</tr>
<tr>
<td>Dashboards and monitors</td>
<td>Dashboards</td>
</tr>
<tr>
<td>Policies</td>
<td>McAfee MOVE AntiVirus Policy</td>
</tr>
<tr>
<td>Queries</td>
<td>Queries and Reports</td>
</tr>
</tbody>
</table>
### Configure permission sets

Update the read/write permissions assigned to the user roles defined for your McAfee ePO environment.

**Task**
1. Log on to McAfee ePO as an administrator.
2. Select **Menu** | **User Management** | **Permission Sets**.
3. Select a user role from the **Permission Sets** list.
4. Next to any McAfee MOVE AntiVirus permission, click **Edit**.
5. Select the permission level, as needed.
6. Click **Save**.

### Configuring McAfee MOVE AntiVirus settings

Configure settings that apply to all components and features of McAfee MOVE AntiVirus in the **MOVE AntiVirus Common 4.6.0** and **MOVE AntiVirus 4.6.0** extensions.

#### Protect McAfee MOVE AntiVirus resources

One of the first things that malware tries to do during an attack is to disable your system security software. Configure Self-Protection in the **Options** policy under **MOVE AntiVirus Common 4.6.0** to prevent McAfee MOVE AntiVirus services, files, and registries from being stopped or modified.

**Task**
1. Log on to McAfee ePO as an administrator.
2. Select **Menu** | **Policy** | **Policy Catalog**, then select **MOVE AntiVirus Common 4.6.0** from the **Product** list.
3. From the **Category** list, select **Options**.
4. Click the name of an editable policy.
5. Under **Self-Protection**, enable these options.

<table>
<thead>
<tr>
<th>Select this...</th>
<th>For this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Self-Protection</td>
<td>To prevent McAfee MOVE AntiVirus services and files, registries from being stopped or modified.</td>
</tr>
<tr>
<td>Enable Self-Protection for MOVE CLI</td>
<td>To protect the command-line utility from being accessed by unauthorized users.</td>
</tr>
</tbody>
</table>

6. Click **Save**.
Configure logging settings

Configure McAfee MOVE AntiVirus logging in the Options policy under MOVE AntiVirus Common 4.6.0 to retrieve the software deployment and configuration details.

Task
1. Log on to McAfee ePO as an administrator.
2. Select Menu | Policy | Policy Catalog, then select MOVE AntiVirus Common 4.6.0 from the Product list.
3. From the Category list, select Options.
4. Click the name of an editable policy.
5. Configure these settings on the page.

<table>
<thead>
<tr>
<th>For this...</th>
<th>Do this...</th>
</tr>
</thead>
</table>
| Events | • Log events to Windows Application log — Select to display alerts in the local system's Windows Event Log.  
• Send events to McAfee ePO — Select to display alerts in the McAfee ePO Threat Event Log. |
| Logging | Rotate log file content when the file size reaches ____ MB — Type the maximum size for a log file to rotate it. Default size is 10 MB. |

6. Click Save.

Configuring exclusions

McAfee MOVE AntiVirus enables you to fine-tune your protection by specifying items to exclude from scanning. For example, you might need to exclude some file types to prevent a scanner from locking a file used by a database or server. A locked file can cause the database or server to fail or generate errors.

<table>
<thead>
<tr>
<th>For this scan type...</th>
<th>Specify items to exclude</th>
<th>Where to configure</th>
<th>Use wildcards?</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-access scan</td>
<td>Files, file types, folders, and process exclusions</td>
<td>On Access Scan policy</td>
<td>Yes</td>
</tr>
<tr>
<td>On-demand scan</td>
<td>Files, file types, and folders</td>
<td>On Demand Scan policy</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Every item in exclusion lists is mutually exclusive. Each exclusion is evaluated separately from the others in the list.

To exclude a folder on Windows systems, append a backslash (\) character to the path. To exclude a folder on Linux systems, append a forward slash (/) character to the path.

Path exclusions

The McAfee MOVE AntiVirus product allows you to fine-tune the list of file types scanned including individual files, folders, and disks. You might need these exclusions because the scanners might scan and lock a file when that file is being used by a database or server. This might cause the database or server to fail or generate errors.

When specifying the path exclusions, wildcards are supported.

(Windows system) All folder exclusion must append a backslash (\). For example, C:\temp\test\  
If you do not append a backslash (\) for the specified path, the file test is excluded.

(Linux system) All folder exclusion must append a forward slash (/). For example, /temp/test/  
If you do not append a forward slash (/) for the specified path, the file test is excluded.
Process exclusions

The McAfee MOVE AntiVirus product allows you to fine-tune the list of process types scanned including processes. You might need these exclusions because the scanners might scan and lock a process when that process is being used by a database or server. This might cause the database or server to fail or generate errors.

When specifying the process exclusions, wildcards are not supported.

Wildcards in exclusions

You can use wildcards to represent characters in exclusions for files, folders, and detection names.

Table 2-4 Valid wildcards

<table>
<thead>
<tr>
<th>Wildcard character</th>
<th>Name</th>
<th>Represents</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Question mark</td>
<td>Single character</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This wildcard applies only if the number of characters matches the length of the file or folder name. For example: The exclusion W?? excludes WWW, but doesn’t exclude WW or WWWW.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Windows) This wildcard matches one character. For example: ?:\ABC matches C:\ABC and D:\ABC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Linux) This wildcard matches one character. For example: /?DEF/ matches /CDEF/</td>
</tr>
<tr>
<td>*</td>
<td>Asterisk</td>
<td>Multiple characters, except backslash ().</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Windows) This wildcard matches zero or more characters. For example: C:\ABC*\XYZ matches C:\ABC\DEF\XYZ and C:\ABC\XYZ</td>
</tr>
<tr>
<td>**</td>
<td>Double asterisk</td>
<td>Zero or more of any characters, including backslash ().</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(Windows system) This wildcard matches zero or more characters. For example: C:\ABC**\XYZ matches C:\ABC\DEF\XYZ and C:\ABC\XYZ</td>
</tr>
</tbody>
</table>

(Windows) Wildcards can appear in front of a backslash (\) in a path. For example, C:\ABC\*\XYZ matches C:\ABC \DEF\XYZ.

(Linux) Wildcards can appear in front of a forward slash (/) in a path. For example, ?DEF matches /CDEF.

Root-level exclusions (Multi-Platform)

McAfee MOVE AntiVirus requires an absolute path for root-level exclusions. This means that you can’t use leading \ or ?:\ wildcard characters to match drive names at the root level.

Instead, you can use leading **\ wildcard characters in root-level exclusions to match drives and subfolders.

For example, **\test\ matches the following:

C:\test\  
D:\test\  
C:\temp\test\  
D:\foo\test\

Root-level exclusions (Agentless)

For Windows systems
McAfee MOVE AntiVirus requires an absolute path for root-level exclusions. You can use leading `?:` wildcard characters in root-level exclusions to match drives and subfolders.

For example, `?:\test\` matches the following:

- `C:\test\`
- `D:\test\`

### System variables (Multi-Platform)

These are the Windows system variables that are supported for Multi-Platform.

<table>
<thead>
<tr>
<th>System variable</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>%ALLUSERSPROFILE%</td>
<td>C:\ProgramData</td>
</tr>
<tr>
<td>%CommonProgramFiles%</td>
<td>C:\Program Files\Common Files</td>
</tr>
<tr>
<td>%CommonProgramFiles(x86)%</td>
<td>C:\Program Files (x86)\Common Files (only in 64-bit version)</td>
</tr>
<tr>
<td>%CommonProgramW6432%</td>
<td>C:\Program Files\Common Files (only in 64-bit version)</td>
</tr>
<tr>
<td>%ProgramData%</td>
<td>%SystemDrive%\ProgramData</td>
</tr>
<tr>
<td>%ProgramFiles%</td>
<td>%SystemDrive%\Program Files</td>
</tr>
<tr>
<td>%ProgramFiles(x86)%</td>
<td>%SystemDrive%\Program Files (x86) (only in 64-bit version)</td>
</tr>
<tr>
<td>%ProgramW6432%</td>
<td>%SystemDrive%\Program Files (only in 64-bit version)</td>
</tr>
<tr>
<td>%PUBLIC%</td>
<td>%SystemDrive%\Users\Public</td>
</tr>
<tr>
<td>%SystemDrive%</td>
<td>C:\</td>
</tr>
<tr>
<td>%SystemRoot%</td>
<td>%SystemDrive%\Windows</td>
</tr>
<tr>
<td>%windir%</td>
<td>%SystemDrive%\Windows</td>
</tr>
</tbody>
</table>

### Import path exclusions from Endpoint Security Threat Prevention scan policies

If you are using Endpoint Security Threat Prevention in your environment, you can import the list of path exclusions that are defined in the on-access scan and on-demand scan policies of Endpoint Security Threat Prevention to McAfee MOVE AntiVirus scan policies.

#### Before you begin
- You installed the McAfee MOVE AntiVirus extension on the McAfee ePO server.
- You installed the Endpoint Security Threat Prevention extension on the McAfee ePO server.
- You have path exclusions list ready in the on-access scan and on-demand scan policies of Endpoint Security Threat Prevention.

#### Task
1. Log on to McAfee ePO as an administrator.
2. Select **Menu | Policy | Policy Catalog**, then select **Endpoint Security Threat Prevention** from the **Product list**.
3. From the **Category** list, select **On Access Scan** or **On Demand Scan**.

   - From the on-demand scan policy, you can import only the exclusions that are defined on the **Full Scan** tab.
4. Next to the name of the policy where you want to import path exclusions, click **Export**.
   a. Next to the **Download file**, right-click the policy name and select **Save link as**....
   b. From the **Save As** window, browse to the location and click **Save** to save the xml file.

5. Select **Menu | Policy | Policy Catalog**, then select **McAfee MOVE AntiVirus 4.6.0** from the **Product list**.

6. From the **Category** list, select **On Access Scan** or **On Demand Scan**.

7. Click the name of an editable policy.

8. From **Path Exclusions** under the **Exclusions** option, click **Import**... to open the **Import Exclusion Path** dialog box.

9. Under **Select the file to add exclusion path**, click **Choose File**, then browse to the location, and select the xml file that is download from Endpoint Security Threat Prevention.
   
   ![Information](image)
   
   *If you want to clear the existing exclusions, select **Clear existing exclusions**.*

10. Click **OK** to import the exclusions list.

   You can now see that the exclusions list is imported.

11. Click **Save** to save the changes in the policy.

### Configuring client load per SVM (Multi-Platform)

Depending on your environment, you can configure the load type for each SVM, which specifies the workload and activities on clients. Configure the client load for each SVM in the **SVM Settings** policy.

The available options are:

- **Low (Higher number of clients)** — Less file activity on clients per SVM. When clients have less file activity, SVM can handle more clients. Default number of clients is 300.

- **Medium (Moderate number of clients)** — Medium file activity on clients per SVM. Default number of clients is 250.

- **High (Fewer number of clients)** — More file activity on clients per SVM. When clients have more file activity, SVM can handle fewer clients. Default number of clients is 150.

- **Custom** — Customize workload and activities for your clients.

   ![Tip](image)
   
   *We recommend **250**. Increasing this value might cause performance issues or scan delays, or both.*

### Alerts for number of client connections and scan time

You can configure alerts for the number of client connections and scan time per SVM. Configure the **Alert me** option for each SVM in the **SVM Settings** policy.

The available options are:
Scanning for threats on client computers

Contents
- Types of scans
  - How McAfee GTI works
  - Configure common scan settings
  - On-access scanning
  - On-demand scanning

Types of scans
Scanning files for threats when the user accesses them protects against intrusions when they occur. Periodically scanning areas of your system that are most susceptible to infection ensures complete protection.

McAfee MOVE AntiVirus provides two types of scans: on-access scans and on-demand scans.

- **On-access scan** — Configure on-access scans to run on managed endpoints. When you access files, folders, and programs, the on-access scanner checks the operation and scans the item, based on criteria defined by the administrator. On-access scanning provides continuous and real-time detection of threats.

  To configure and schedule on-access scans, use the on-access scan policy settings.

- **On-demand scan** — Configure and schedule on-demand scans to run on managed endpoints. This scan type examines all files on virtual machines for potential threats during the time specified. On-demand scans supplement the continuous protection of on-access scanning. You can also schedule regular scans at times that do not interfere with your work.

  To configure and schedule on-demand scans, use these client task settings:
  - **Targeted On Demand Scan** — Allows you to select a system or a group of systems from the System Tree to initiate the on-demand scan.
  - **Policy-based On-Demand Scan** — Schedules the predefined on-demand scans. Configure the behavior of these scans in the policy settings for on-demand scan.

  The **Options** policy includes settings that apply to all scan types.

How McAfee GTI works
If you enable McAfee GTI for the on-access or on-demand scanner, the scanner uses heuristics to check for suspicious files.

The scanner submits fingerprints of samples, or hashes, to a central database server hosted by McAfee Labs to determine if they are malware. By submitting hashes, detection might be made available sooner than when McAfee Labs publishes the next DAT release.

You can configure the sensitivity level that McAfee GTI uses when it determines if a detected sample is malware. The higher the sensitivity level, the higher the number of malware detections. However, allowing more detections can result in more false positives. The McAfee GTI sensitivity level is set to **Medium** by default.

Configure the sensitivity level for each scanner in the **SVM Settings** policy.
Configure common scan settings

To specify settings that apply to both on-access and on-demand scans, configure the MOVE AntiVirus 4.6.0 | Options policy settings.

The common scan settings in the policy apply to all scans:

- **Quarantine Manager** (Multi-Platform) — Specifies the quarantine location and the number of days to keep quarantined items before automatically deleting them.

- **Quarantine network share** (Agentless) — Specifies the specified network share where the quarantined files are stored. Make sure that you have write permission to the shared folder.
  
  McAfee MOVE AntiVirus supports only Windows share path for quarantine network share.

- **SVM Server Communication** (Multi-Platform) — Specifies the scan server port for communicating with the client system.

- **SVM Assignment** (Multi-Platform)
  
  - **Assign SVM using SVM Manager** — Specifies the IP address of the SVM manager for assigning the SVM using SVM Manager.
  
  - **Assign SVM manually** — Specifies the IP address of the SVM to assign the SVM manually.

**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 **Options**.

4. Click the name of an editable policy.

5. Configure settings on the page, as required, then click **Save**.
On-access scanning
The on-access scanner examines files on the computer as the user accesses them, and provides continuous, real-time detection of threats.

How on-access scanning works
The on-access scanner integrates with the system at the lowest levels (file system filter driver) and scans files where they first enter the system.

The on-access scanner delivers notifications to the System Service interface when detections occur.
When an attempt is made to access or modify a file, the scanner intercepts the operation and takes these actions.

1. Examines the file at the client system.
2. Checks if any exclusion is defined in the policy. If any exclusion is defined for the file, the access is allowed.
3. If an exclusion is not defined, the scanner checks whether the file is present in local cache in the client system. If it is present, access is allowed.
4. If the file is not present in local cache, the scanner checks for publisher trust in the client system. If it matches, the access is allowed.
5. If the publisher trust does not match, the scanner checks for the file in global cache in the SVM. If the file is present, the access is allowed.
6. If the file is not present in global cache, the scanner compares the information in the file to the known malware signatures in the currently loaded DAT files.
   - If the file is clean, the result is cached and the read, write, or rename operation is granted. McAfee MOVE AntiVirus caches the result in the SVM and client system.
   - If the file contains a threat, the scanner sends the file nature as malware to the client systems, where the configured action is taken.

**On-access scanning with TIE and ATD enabled**

1. On-access scanner goes through the steps 1 through 4 of *How on-access scanning works*.
2. If the publisher trust does not match:
   - The client looks for the reputation in global cache in the SVM. If the reputation is available, the access is allowed based on the **Shared Cloud Solutions** policy assigned to the system.
   - If the reputation is not available in global cache in the SVM, the client sends the file hashes to the SVM for TIE lookup.
   - The SVM checks the reputation cache for the file hash. If the file hash is found, the SVM gets the reputation data from the SVM cache and sends the reputation to the client and the action is taken.
   - (SVM is connected to TIE) If the file hash is not found in the SVM cache and TIE server does not have the reputation:
     - (Advanced Threat Defense is present) If the policy on the endpoint determines that the file must be sent to Advanced Threat Defense, the server sends the file for further analysis. To send the file to Advanced Threat Defense, these requirements must be met:
       - **Advanced Threat Defense (ATD)** option is configured in the **Shared Cloud Solutions** policy on the McAfee ePO server.
       - Size of the file is less than 10 MB
       - The TIE server returns the file hash's reputation to the SVM once the data is received from Advanced Threat Defense after analyzing the file.
3. McAfee MOVE AntiVirus takes action based on the **Shared Cloud Solutions** policy assigned to the system that is running the file.
4. The SVM sends threat details as threat events to McAfee ePO.

**Changing when files are scanned**

You can change the client policy to determine which files are scanned for threats and when.
By default, files are scanned when they are read from or written to disk, or when opened for backup. The McAfee Agent program files and the User Profile Manager process are excluded from scans.

When files are written to disk, the on-access scanner examines these files:

- Incoming files written to the local drive.
- Files (new, changed, or files copied or moved from one drive to another) created on the local drive or a mapped network drive (if enabled with Multi-Platform).

When files are read from disk, the scanner examines these files:

- Outgoing files read from the local drive or mapped network drives (if enabled with Multi-Platform).
- Files trying to execute a process on the local drive.
- Files opened on the local drive.

Depending on your environment, selecting On network drives can degrade network performance.

**Configure on-access scan policy settings**

These settings enable and configure on-access scanning, which includes specifying messages to send when a threat is detected and different settings based on process type.

**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 **On-Access Scan**.
4. Click the name of an editable policy.
5. Click **Show Advanced**.
6. Select **Enable On-Access Scan** to enable the on-access scanner and modify options.
7. Configure these settings to control which files are scanned.
<table>
<thead>
<tr>
<th>For this...</th>
<th>Select...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scan</strong></td>
<td>Any combination of:</td>
</tr>
<tr>
<td></td>
<td>• When writing to disk</td>
</tr>
<tr>
<td></td>
<td>• When reading from disk</td>
</tr>
<tr>
<td></td>
<td>• On network drives</td>
</tr>
<tr>
<td></td>
<td>• Opened for backup (Multi-Platform only)</td>
</tr>
<tr>
<td></td>
<td>Depending on your environment, selecting <strong>On network drives</strong> can degrade network performance.</td>
</tr>
</tbody>
</table>

The supported file systems for Linux client system are ext2, ext3, ext4, btrfs, cifs, vfat, ISO9660, xfs, and nfs.

<table>
<thead>
<tr>
<th><strong>File types to scan</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>All files</strong> — Select to scan all files.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Default + Additional files</strong> (Multi-Platform only) — Select to scan the default file types or any additional file types. You can add, edit, and remove additional file types, which are included for scanning. By default, this option is selected.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Following only</strong> — Select to specify a list of file extensions to scan. You can add, edit, and remove file extensions that are included for scanning. Wildcards are supported, and exact matches are required. Do not include the period when specifying extensions.</td>
<td></td>
</tr>
<tr>
<td>Archive and MIME-encoded files are not scanned by default. This behavior is changed by modifying the SVM Settings policy.</td>
<td></td>
</tr>
</tbody>
</table>

For more information about how to use wildcards when creating exclusions in VirusScan Enterprise or McAfee MOVE AntiVirus, see McAfee KnowledgeBase article **KB54812**.

<table>
<thead>
<tr>
<th><strong>Exclusions</strong></th>
<th><strong>Path Exclusions</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Add them to the <strong>Path Exclusions</strong> list.</td>
<td></td>
</tr>
</tbody>
</table>

The McAfee MOVE AntiVirus product allows you to fine-tune the list of file types scanned including individual files, folders, and disks. You might need these exclusions because the scanners might scan and lock a file when that file is being used by a database or server. This might cause the database or server to fail or generate errors.

When specifying the exclusions:

• Wildcards are supported for path exclusions.

• (Multi-Platform only) Windows system variables are supported, see **System variables** for the list of supported system variables.

   (Agentless only) System variables are not supported.

Using the **Import** option, you can browse to and select the exclusion rule file and add path exclusions.

   A path exclusion entry \*.log is available, so that the log files on the endpoints are not scanned. This improves the scanning performance of the client system.
### For this... Select...

<table>
<thead>
<tr>
<th><strong>Process Exclusions</strong></th>
<th><strong>Publisher Exclusions</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Add them to the Process Exclusions list.</td>
<td>You can choose to trust the authenticated and signed files from different publishers, so that the scanning performance improves by optimized use of resources at the SVM by sending fewer files for scanning from the endpoints.</td>
</tr>
<tr>
<td>The McAfee MOVE AntiVirus product allows you to fine-tune the list of process types scanned including processes. You might need these exclusions because the scanners might scan and lock a process when that process is being used by a database or server. This might cause the database or server to fail or generate errors.</td>
<td>Here are the portable executable extensions that are excluded with this option: .cpl, .exe, .dll, .ocx, .sys, .scr, .drv, .efi, .fon</td>
</tr>
<tr>
<td>Wildcards are not supported for process exclusions.</td>
<td>Certificate revocation check — This is used for the Windows Publisher Trust feature. You can configure the certificate revocation check with these options:</td>
</tr>
<tr>
<td></td>
<td>• none — McAfee MOVE AntiVirus does not do certificate revocation check.</td>
</tr>
<tr>
<td></td>
<td>• for end Certificate locally — McAfee MOVE AntiVirus checks whether the end certificate of the file is valid or has it being revoked. This is checked from the Windows CRL (local cache) that is maintained by Windows locally.</td>
</tr>
<tr>
<td></td>
<td>• for full certificate chain locally — McAfee MOVE AntiVirus checks the complete chain of certificate for a particular digitally signed file against the Windows CRL (local cache) that is maintained by Windows locally.</td>
</tr>
<tr>
<td></td>
<td>• for end certificate locally as well as by getting CRL from the issuing CA — McAfee MOVE AntiVirus checks against the Windows CRL (local cache) that is maintained by Windows locally and also checks against the issuing CA's (certificate authority) CRL that is done over network.</td>
</tr>
</tbody>
</table>

8 On the Actions tab, configure Threat detection primary response. Make sure that you select a primary action and a secondary action.

Available primary actions:
- **Delete files automatically and quarantine** — Once the threat is detected, it deletes and quarantines the threat to the specified location.

  (Agentless only) If no quarantine policy is configured, the Delete files automatically and quarantine action does not occur even if it is configured as the primary action.

- **Delete files automatically** — Once the threat is detected, it deletes the threat.
- **Deny access to files** — Prevents the user from accessing the file.

Available secondary action:
- **Deny access to files** — Prevents the user from accessing the file.

9 Click **Save** to store the policy.

See also
- Configuring exclusions on page 20
On-demand scanning
The on-demand scanner examines the client systems for potential threats at regular intervals or at convenient times.

Use on-demand scans to supplement the continuous protection of the on-access scanner, such as to scan latent and inactive processes. You can also schedule regular scans at times that do not interfere with your work.

How on-demand scanning works
The on-demand scanner searches files, folders, and registry for any malware that might have infected the computer.

You decide when and how often the on-demand scans occur. You can scan at a scheduled time or at startup.

The on-demand scanner intercepts the operation and takes these actions:

1. Examines the file at the client system.
2. Checks if any exclusion is defined in the policy. If any exclusion is defined for the file, the access is allowed.
3. If an exclusion is not defined, the scanner checks whether the file is present in local cache in the client system. If it is present, access is allowed.
4. If the file is not present in local cache, the scanner checks for publisher trust in the client system. If it matches, the access is allowed.
5. If the publisher trust does not match, the scanner checks for the file in global cache in the SVM. If the file is present, the access is allowed.
6. If the file is not present in global cache, the scanner compares the information in the file to the known malware signatures in the currently loaded DAT files.
   • If the file is clean, the result is cached and the read, write, or rename operation is granted. McAfee MOVE AntiVirus caches the result in the SVM and the client system.
   • If the file contains a threat, the scanner sends the file nature as malware to the client systems, where the configured action is taken.
     For example, if the action is configured to Deny files automatically and quarantine (the default setting), the scanner:
     • Deletes items that are detected as threats and saves copies in a non-executable format to the Quarantine folder.
     • Records the results in the activity log.
     • Notifies the user that it detected a threat in the file, and includes the item name and the action taken.
7. If the file doesn't meet the scanning requirements, the scanner doesn't check it. The scanner continues until all data is scanned.

The on-demand scan detection list is cleared when the next on-demand scan starts.

On-demand scanning with TIE and ATD enabled
1. On-demand scanner goes through the steps 1 through 4 of How on-demand scanning works.
2. If the publisher trust does not match:
   • The client looks for the reputation in global cache in the SVM. If the reputation is available, the access is allowed based on the Shared Cloud Solutions policy assigned to the system.
   • If the reputation is not available in global cache in the SVM, the client sends the file hashes to the SVM for TIE lookup.
• The SVM checks the reputation cache for the file hash. If the file hash is found, the SVM gets the reputation data from the SVM cache and sends the reputation to the client and the action is taken.

• (SVM is connected to TIE) If the file hash is not found in the SVM cache and TIE server does not have the reputation:
  • (Advanced Threat Defense is present) If the policy on the endpoint determines that the file must be sent to Advanced Threat Defense, the server sends the file for further analysis. To send the file to Advanced Threat Defense, these requirements must be met:
    • Advanced Threat Defense (ATD) option is configured in the Shared Cloud Solutions policy on the McAfee ePO server.
    • Size of the file is less than 10 MB
  • The TIE server returns the file hash’s reputation to the SVM once the data is received from Advanced Threat Defense after analyzing the file.

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

4 The SVM sends threat details as threat events to McAfee ePO.

Optimizing the scanning performance on systems
To minimize the impact that on-demand scans have on a system, specify performance options when configuring these scans.

Enable and configure on-demand scans
You can modify the on-demand scan policy to enable system on-demand scans, and to determine the schedule and frequency of scans.

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

By default, on-demand scans are not enabled. Other scan settings (for example, exclusions) are inherited from the client scan policy.

Task
1 Log on to McAfee ePO as an administrator.

2 Select Menu | Policy | Policy Catalog, then from the Product list select MOVE AntiVirus 4.6.0.

3 From the Category list, select On Demand Scan.

4 Click the name of an editable policy.

5 Configure these settings, then click Save.
For this... Select...

<table>
<thead>
<tr>
<th>Enable On-demand Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable on-demand scan.</td>
</tr>
<tr>
<td>• Specify maximum time for each file scan ___ seconds — Enter the appropriate amount for your environment. We recommend 45.</td>
</tr>
<tr>
<td>• Run on-demand scan for every ___ days — Enter the appropriate amount for your environment. We recommend 7.</td>
</tr>
<tr>
<td>• On-demand scan will stop after ___ minutes — The amount of time to wait for a scan to complete, in minutes. Defaults to 150 minutes. This is the duration for which a McAfee MOVE AntiVirus Agent waits for scan response of a file from the SVM. Typically, file scans are fast. However, file scans might take longer time due to large file size, file type, or heavy load on the SVM. In case, the file scan takes longer than the scan timeout limit, the file access is allowed and a scan timeout event is generated.</td>
</tr>
<tr>
<td>• Cache scan results for files smaller than ___ MB (Multi-Platform only) — Set the maximum file size (in MB) up to which scan results must be cached. Defaults to 40 MB. Files smaller than this threshold are copied completely to the SVM and scanned. If the file is found to be clean, its scan result is cached based on its SHA-1 checksum for faster future access. Files larger than this size threshold are transferred in chunks that are requested by the SVM and scanned.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>File Types to Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>• All files — Select to scan all files. By default, this option is selected.</td>
</tr>
<tr>
<td>• Default + Additional files (Multi-Platform only) — Select to scan the default file types or any additional file types. You can add, edit, and remove additional file types, which are included for scanning.</td>
</tr>
<tr>
<td>• Following only — Select to specify a list of file extensions to scan. You can add, edit, and remove file extensions that are included for scanning. Wildcards are supported, and exact matches are required. Do not include the period when specifying extensions.</td>
</tr>
<tr>
<td>Archive and MIME-encoded files are not scanned by default. This behavior is changed by modifying the SVM Settings policy.</td>
</tr>
</tbody>
</table>

For more information about how to use wildcards when creating exclusions in VirusScan Enterprise or McAfee MOVE AntiVirus, see McAfee KnowledgeBase article KB54812.

Path Exclusions

Add them to the Path Exclusions list.

Excluding scan items — The McAfee MOVE AntiVirus product allows you to fine-tune the list of file types scanned including individual files, folders, and disks. You might need these exclusions because the scanners might scan and lock a file when that file is being used by a database or server. This might cause the database or server to fail or generate errors.

When specifying the exclusions:

• Wildcards are supported.

• (Multi-Platform only) Windows system variables are supported, see System variables for the list of supported system variables.

(Agentless only) System variables are not supported.

Using the Import option, you can browse to and select the exclusion rule file and add path exclusions.

A path exclusion entry *.log is available, so that the log files on the endpoints are not scanned. This improves the scanning performance of the client system.

See also

Configuring exclusions on page 20
On-demand scan events and log details

McAfee MOVE AntiVirus generates alerts for on-demand scans. You can view the ODS statuses and event logs on McAfee ePO and client systems.

The log files for on-demand and on-access scans are available in the installation directory.

In the client log file, you can search for terms like ODS: start scan and ODS: scan complete to find the status on-demand scan.

(Multi-Platform only) You can also view the ODS status from the local system's Windows Event Log on the client system. (Event: On-Demand Scan Started on winvistax64mp.moveauto.com using engine version 5600.1067 and dat version 7203.0000)

McAfee MOVE AntiVirus generates alerts for on-demand scans. These alerts can be displayed in any of these locations:

- The local system’s Windows Event Log
- The McAfee ePO Threat Event Log
- The local system as a McAfee notification area pop-up menu

Table 2-5  Server on-demand scan events (Multi-Platform)

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event message</th>
</tr>
</thead>
<tbody>
<tr>
<td>36984</td>
<td>On-demand scan started.</td>
</tr>
<tr>
<td>36985</td>
<td>On-demand scan completed.</td>
</tr>
<tr>
<td>36986</td>
<td>On-demand scan terminated. Scan time limit reached.</td>
</tr>
<tr>
<td>36987</td>
<td>On-demand scan terminated. Scan disabled in policy.</td>
</tr>
<tr>
<td>36988</td>
<td>On-demand scan terminated. Exceeded maximum number of concurrent scans.</td>
</tr>
<tr>
<td>36989</td>
<td>High on-demand scan terminated. Scan failure on client.</td>
</tr>
<tr>
<td>36990</td>
<td>High on-demand scan terminated. Unexpected termination.</td>
</tr>
<tr>
<td>37009</td>
<td>Threat detected.</td>
</tr>
</tbody>
</table>

Table 2-6  Server on-demand scan events (Agentless)

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event message</th>
</tr>
</thead>
<tbody>
<tr>
<td>37055</td>
<td>On-demand scan started.</td>
</tr>
<tr>
<td>37056</td>
<td>On-demand scan completed.</td>
</tr>
<tr>
<td>37057</td>
<td>On-demand scan found malware.</td>
</tr>
<tr>
<td>37058</td>
<td>On-demand scan failed to start.</td>
</tr>
<tr>
<td>37059</td>
<td>On-demand scan terminated. Scan time limit reached.</td>
</tr>
<tr>
<td>37060</td>
<td>On-demand scan terminated. Scan target powered off.</td>
</tr>
<tr>
<td>37061</td>
<td>On-demand scan terminated. Scan disabled in policy.</td>
</tr>
<tr>
<td>37062</td>
<td>On-demand scan resumed.</td>
</tr>
<tr>
<td>37076</td>
<td>Malware detected and successfully deleted.</td>
</tr>
</tbody>
</table>
**Targeted on-demand scan**

The targeted on-demand scan feature allows the administrator to select a system or a group of systems where to initiate the on-demand scan.

When the admin initiates the targeted on-demand scan on the client system, McAfee Agent schedules the client task on the client system. The SVM picks the client task, then runs the scan on the client system, depending on the slot availability for the scan. McAfee Agent monitor shows the status such as TODSTask becomes active, TODSTask is successful, and TODSTask is finished, but this is not the actual on-demand scan status. You can view the on-demand scan status and event logs on McAfee ePO and client systems.

The SVM runs the specified maximum concurrent targeted on-demand scans per SVM defined by the administrator. When the SVM has reached the maximum number of targeted on-demand scans, the recently initiated on-demand scan runs later when the targeted on-demand scan slot is available.

**Example 1**

Consider a scenario where:

- Restrict number of on-demand scans to ___ per SVM is set as 2
- Restrict number of targeted on-demand scans to ___ per SVM is set as 2
- No on-demand scan is running currently
- Two targeted on-demand scans are running currently

With these assumptions, if you configure one more targeted on-demand scan, the newly scheduled targeted on-demand scan starts when one of the existing targeted on-demand scans finishes.

**Example 2**

Consider a scenario where:

- Restrict number of on-demand scans to ___ per SVM is set as 2
- Restrict number of targeted on-demand scans to ___ per SVM is set as 2
- One or two on-demand scans are running currently
- Two targeted on-demand scans are running currently

With these assumptions, if you configure one more targeted on-demand scan, the newly scheduled targeted on-demand scan starts when one of the existing targeted on-demand scans finishes.

**See also**

*On-demand scan events and log details on page 34*

**Configure targeted on-demand scans**

Change the SVM Settings policy to enable on-demand scanning, and to set the concurrent scan value as needed.

**Before you begin**

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

By default, on-demand scans are disabled. Other scan settings (for example, exclusions) are inherited from the client on-demand scan policy.

**Task**

1. Log on to McAfee ePO as an administrator.
2. Select **Menu | Policy | Policy Catalog**, then from the **Product** list select **MOVE AntiVirus 4.6.0**.
3 From the Category list, select SVM Settings.

4 Click the name of an editable policy.

5 Under Concurrent on-demand scans, configure these settings, then click Save.

<table>
<thead>
<tr>
<th>To do this...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restrict number of targeted on-demand scans to____per SVM</td>
<td>Enter the appropriate value for your environment.</td>
</tr>
<tr>
<td></td>
<td>The default value is 1. Increasing this value reduces the performance.</td>
</tr>
</tbody>
</table>

Create and run targeted on-demand scan
Select a system or a group of systems from the System Tree and initiate the targeted on-demand scan.

Before you begin
• You installed the McAfee MOVE AntiVirus extension on the McAfee ePO server.
• You enabled the Enable on-demand scan option in the On Demand Scan policy.
• You configured Restrict number of targeted on-demand scans to_____per SVM in the SVM Settings policy.
• A new ODS does not start if an ODS is currently running on the targeted system.

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

2 Select Menu | Systems | System Tree.

3 Select the VMs you want to run the targeted on-demand scan.

4 From Actions, select Targeted ODS [MOVE].

For McAfee ePO 5.1.3 version, the Schedule page is not available and targeted on-demand scan runs immediately on the targeted system.

(For Agentless) If any target VM is turned off, McAfee ePO sends the task once the VM is turned on, then SVM initiates the scan.

5 On the Schedule page, schedule the task, then click Next.

6 On the Summary page, review the task details and click Save to run the on-demand scan.

Create and run a targeted on-demand scan client task (Multi-Platform)
Select a system or a group of systems from the System Tree and assign a client task to initiate the targeted on-demand scan.

Before you begin
• You installed the McAfee MOVE AntiVirus extension on the McAfee ePO server.
• You enabled the Enable on-demand scan option in the On Demand Scan policy.
• You configured Restrict number of targeted on-demand scans to_____per SVM in the SVM Settings policy.
• A new on-demand scan does not start if the on-demand scan is already running on the targeted system.
**Task**

1. Log on to the McAfee ePO server as an administrator.
2. Select Menu | Policy | Client Task Catalog.
3. From Client Task Types, select MOVE AntiVirus 4.6.0 | Targeted On-Demand Scan [Multi-Platform].
4. Click the name of an existing client task or click New Task, then confirm the task type.
5. Configure Task Name and Description on each tab, then click Save.
6. Click Assign, specify the servers where you want to assign the task, then click OK.
7. Click 2 Schedule to schedule the task.

---

**Configure deferred scan settings (Multi-Platform only)**

The deferred scan feature optimizes file scanning for files where the previous scan timed out because of large file size, file structure, or file composition.

---

**Before you begin**

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

---

When the previous on-access scan timed out, scanning for a file starts again with an increased or new timeout, depending on the file size. You can configure this timeout value and the file size using the McAfee ePO server.

For an on-demand scan, the scanning for a file starts according to the timeout based on file size value specified in the deferred scan policy.

---

**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 On-Access Scan or On-Demand Scan 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 Scan Policy), then click OK.
5. Under Deferred Scan (Multi-Platform only), select Enable on-access deferred scan or Enable on-demand deferred scan and configure these file size ranges and scan timeout values, then click Save.

<table>
<thead>
<tr>
<th>File size range</th>
<th>Scan timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>&gt; 40 MB and ≤200 MB</td>
<td>480 seconds</td>
</tr>
<tr>
<td>&gt; 200 MB and ≤4096 MB</td>
<td>900 seconds</td>
</tr>
<tr>
<td>&gt; 4096 MB and greater</td>
<td>1800 seconds</td>
</tr>
</tbody>
</table>
Client notifications for deferred scans

If the deferred scanning is incomplete after reaching the maximum timeout, access to the file is allowed. These client notifications appear to the user on the client system for successful on-access scanning or scan timeouts:

- Deferred scan completed for file `<C:\Test\file name>`. File is safe to access.
- Deferred scan is in progress for file `<C:\Test\file name>`. (A thread in svchost.exe process took 45 seconds for scanning. Hence, access denied.)
- Deferred scan is timed out for file `<C:\Test\file name>`. Hence, access allowed.
- Deferred scan failed for file `<C:\Test\file name>` due to some internal error. Hence, access denied.
- Deferred scan failed for file `<C:\Test\file name>`. Hence, access denied.
- Access Denied: Deferred scan is in progress for file `<C:\Test\file name>`.
- Deferred scan completed for file `<C:\Test\file name>`. File is not accessible.
- Deferred scan completed for file `<C:\Test\file name>`. File is deleted.

The client notifications do not appear for on-demand scan.

Scan Diagnosis

Contents

- Identify frequently scanned items from McAfee ePO (Agentless)
- Identify frequently scanned items from command line (Agentless)
- Identify frequently scanned items from McAfee ePO (Multi-Platform)
- Identify frequently scanned items from command line (Multi-Platform)

Identify frequently scanned items from McAfee ePO (Agentless)

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

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 | Policy | Client Task Catalog.
3. From Client Task Types, select MOVE AntiVirus 4.6.0 | Scan Diagnostics [Agentless].
4. Click the name of an existing client task or click New Task and confirm the task type.
5 Configure these settings on each tab, then click **Save**.
   • **Task Name** — Specifies a unique name for the task.
   • **Description** — Specifies a description about the task.
   • **Diagnosis Time** — Specifies a description about the task.

6 Click **Assign**, specify the SVM where you want to assign the task, then click **OK**.

7 Click **Schedule** to schedule the task.
   At the end of specified minutes, the McAfee ePO completes the analysis and displays the results. The default allowed time limit is 10 minutes.

8 Select **Menu | Reporting | Queries & Reports**, then select **MOVE AntiVirus 4.6.0 [Agentless]** under **McAfee Groups** to view and run these scan diagnostic queries:
   • **MOVE AntiVirus: Top 10 Scanned File Extensions for each SVM** — Lists the top 10 file extensions scanned by the SVM.
   • **MOVE AntiVirus: Top 10 Scanned Files for each SVM** — Lists the top 10 files scanned by the SVM.
   • **MOVE AntiVirus: Top 10 Scanned Virtual Machines for each SVM** — Lists the top 10 virtual machines that are sending maximum scan and checksum requests.

**Identify frequently scanned items from command line (Agentless)**

Use the scan diagnostic command-line tool to calculate and display frequently scanned files, extensions, and VMs, on a system running the Agentless software. You can include these results in the path exclusion policies to exclude them from being scanned.

**Before you begin**
   • Make sure that the user is a root user, or has sudo permissions.
   • The name of the VM is resolved only when the vCenter is successfully registered in the SVM Settings policy using McAfee ePO. Otherwise, only the VM ID appears.

Access the command line interface (CLI) of the SVM to create and display this report.

This diagnostic tool captures these details:
   • Top 10 file scan requests.
   • Top 10 file extensions.
   • Top 10 virtual machines that are sending scan and checksum requests.
Task

1 To identify the frequently scanned files, run the command:

```bash
>cd /opt/McAfee/move/bin
sudo ./scan_diagnostic
```

or

```bash
sudo /opt/McAfee/move/bin/scan_diagnostic
```

These parameters are available:

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>--help</td>
<td>Shows how to use the command and its options.</td>
</tr>
<tr>
<td>--time arg</td>
<td>Specifies the time period, in seconds, set for calculating the frequently scanned files. For example, 60 seconds.</td>
</tr>
<tr>
<td>--elements arg</td>
<td>Specifies the number of entries to be captured and displayed in the result.</td>
</tr>
<tr>
<td>--path arg</td>
<td>Specifies the output folder path. The default path is /opt/McAfee/move/log.</td>
</tr>
</tbody>
</table>

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

```
svadmin@MOVE-SVR:~$ sudo /opt/McAfee/move/bin/scan_diagnostic --time 60

Profiling:
Top frequently scanned files

C:Users\Administrator\Desktop\out.txt 15.56%
C:Users\Administrator\Desktop\outLow.txt 8.61%
C:Users\Administrator\AppData\Roaming\Microsoft\Windows\Cookies\administrator\Ad
nx\111.txt 2.22%
C:Users\Administrator\AppData\Roaming\Microsoft\Windows\Cookies\administrator\Ad
nx\112.txt 2.22%
C:Users\Administrator\Application\AppData\Local\Low\Microsoft\Cryp
```

2 (Optional) Change the time limit by editing the `svaconfig.xml` file located at `/opt/McAfee/move/etc/`.

To stop the scan diagnostic tool while it is collecting the data, use the `Ctrl+C` keys.
Identify frequently scanned items from McAfee ePO (Multi-Platform)

Select one or a group of SVMs from the System Tree and assign a client task to calculate and display frequently scanned files, extensions, processes, and VMs. You can include these results in the path exclusion policies to exclude them from being scanned.

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 | Policy | Client Task Catalog.
3. From MOVE AntiVirus 4.6.0 under Client Task Types, select Scan Diagnostics [Multi-Platform].
4. Click the name of an existing client task or click New Task, then confirm the task type.
5. Configure these settings on each tab, then click Save.
   - Task Name — Specifies a unique user-friendly name for the task.
   - Description — Specifies some user-friendly description about the task.
   - Diagnosis Time — Specifies the time period, in minutes, set for calculating the frequently scanned files. For example 1-10 minutes.
6. Click Assign, select one SVM or a group of SVMs where you want to assign the task, then click OK.
7. Click Schedule to schedule the task.
   At the end of specified minutes, the McAfee ePO server completes the analysis and displays the results. The default allowed time limit is 10 minutes.
8. Select Menu | Reporting | Queries & Reports and select MOVE AntiVirus 4.6.0 [Multi-Platform] under McAfee Groups to view and run these scan diagnostic queries:
   - MOVE AntiVirus: Top 10 Scanned File Extensions for each SVM — Lists the top 10 file extensions scanned by the SVM.
   - MOVE AntiVirus: Top 10 Scanned Files for each SVM — Lists the top 10 files scanned by the SVM.
   - MOVE AntiVirus: Top 10 Scanned Processes for each SVM — Lists the top 10 processes scanned by the SVM.
   - MOVE AntiVirus: Top 10 Scanned Virtual Machines for each SVM — Lists the top 10 virtual machines that are sending maximum scan and checksum requests.

   This data is rolled over every 7 days.

Identify frequently scanned items from command line (Multi-Platform)

The scan diagnostic tool calculates and displays frequently scanned processes, files, extensions, and VMs. You can include these files in the path and process exclusion policies. These specified files are excluded from scans when they are written by a trusted process.

Before you begin
You must have administrator permissions to perform this task.

Access the SVM command line interface (CLI) on the SVM virtual machine to create and display this report.

This diagnostic tool captures these details:
- Top 10 file scan requests
- Top 10 file extensions
- Top 10 processes
- Top 10 virtual machines that are sending maximum scan and checksum requests.

**Task**

1. Open the SVM CLI: click **Start | Programs | McAfee | MOVE AV Server command prompt**.

   ![This command prompt has administrator rights.]

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

2. To calculate the frequently scanned files, run this command:

   ```
   move_diagnose /T: <Time Window> /O: <Output File>
   ```

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>The time period, in minutes, set for calculating the frequently scanned files. For example, 3 minutes.</td>
</tr>
<tr>
<td>O</td>
<td>Full path of the output file for storing the results.</td>
</tr>
</tbody>
</table>

   At the end of specified minutes, the tool completes the analysis and displays the results. The default allowed time limit is 10 minutes.

   ![Administrator: Command Prompt](image)

   **Top 10 Scanned Processes from 15:31 to 15:32**
   
   `notepad.exe 50%`
   `svchost.exe 50%`

   **Top 10 Scanned Files from 15:31 to 15:32**
   
   `\Device\HarddiskVolume2\Users\Administrator\Desktop\test.txt 50%`
   `\Device\HarddiskVolume2\Windows\Prefetch\NOTEPAD.EXE-B8414F97.pdf 50%`

   **Top 10 Scanned Virtual Machines from 15:31 to 15:32**
   
   `10.213.240.68 100%`

   **Top 10 Scanned File Extensions from 15:31 to 15:32**
   
   `pdf 50%`
   `txt 50%`
   `C:\Users\Administrator\`
3  (Optional) Change the time limit by configuring the registry settings in HKLM\System\CurrentControlSet\services\mvserver\Parameters\diagnostic\FrequentlyScanMaxTimeOutWindow.
Managing McAfee MOVE AntiVirus

Manage McAfee MOVE AntiVirus by responding to threat detections, managing quarantined items, and periodically analyzing your protection.

Contents
- Keeping your protection up to date
- Responding to detections
- Quarantined items
- How tagging works in an NSX environment (Agentless)
- Self-protection
- Events, responses, and McAfee MOVE AntiVirus
- Analyzing your protection
- Integrating TIE and Advanced Threat Defense

Keeping your protection up to date

McAfee MOVE AntiVirus depends on the engine and information in the content files to identify and act on threats. Every day, McAfee Labs releases new content files to address new threats.

To update systems managed by McAfee ePO, use the Master Repository. The Master Repository on the McAfee ePO server maintains the latest versions of the engine and content files.

For Agentless SVM, AutoUpdate for DAT files is disabled. Use McAfee ePO to create a client task and update to the latest versions of the engine and DAT files.

Responding to detections

When a threat occurs, the McAfee MOVE AntiVirus configuration determines the threat detection method and response.

If McAfee MOVE AntiVirus is configured to **Deny files automatically and quarantine** (the default setting), the scanner deletes items that are detected as threats and saves copies in a non-executable format to the Quarantine folder. If the file can't be deleted, the scanner denies access to the file.

**Unwanted program detection**

The on-access and on-demand scanners detect unwanted programs using policy settings that you configured and DAT files.

When a detection occurs, the scanner that detected the unwanted program applies the action that you configured for that scanner.
Review the information in the log file, then decide whether to take any of these additional actions:

- Fine-tune the settings for the scanner to make your scans more efficient.
- Exclude unwanted program and files from detection.
  If a legitimate program was detected (false positive), configure it as an exclusion.

### On-access scan detections

When a threat is detected, the on-access scanner responds according to the settings in the On-Access Scan policy.

Review the information in the activity log to decide whether to take more actions:

- Fine-tune the settings for scan to make your scans more efficient.
  For example, exclude legitimate files and delete known threats from the quarantine.
- Configure the scanner to:
  - **Deny files automatically and quarantine** — Deletes and quarantines the item that contains the threat.
  - **Delete files automatically** — Deletes the item that contains the threat.
  - **Deny access to files** — Prevents the user from accessing files with detected threats.
- Configure the scanner to display a message to users when a threat is detected.

### On-demand scan detections

When an on-demand detection occurs, the scanner response depends on the type of on-demand scan.

For targeted on-demand scans, the scanner uses **Targeted On-Demand Scan** client task settings. For policy-based on-demand scans, the scanner uses On-Demand Scan policy settings.

Review the information in the log file to decide whether to take more actions:

- Fine-tune the settings for the scan to make your scans more efficient.
  For example, exclude legitimate files and delete known threats from the quarantine.
- Configure the scanner to prompt for action.
- Configure the scanner to:
  - **Deny files automatically and quarantine** — Deletes and quarantines the item that contains the threat.
  - **Delete files automatically** — Deletes the item that contains the threat.
  - **Notify only** — Notifies when accessed an item that contains the threat.

### Quarantined items

McAfee MOVE AntiVirus deletes items that are detected as threats and saves copies in a non-executable format to the Quarantine folder.

You can restore a quarantined item.
Configure the settings for quarantine

Configure Quarantine Manager settings in the Options policy, including the location of quarantined items and how long to keep them.

**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 Options.

4. Click the name of an editable policy.

5. Configure the Quarantine Manager settings, then click Save.

<table>
<thead>
<tr>
<th>For...</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Multi-Platform  | Quarantine Directory    | Specify where quarantined items are stored by changing the quarantine directory.  
  Mapped network drives and UNC network path names are not supported. |
| Agentless       | Quarantine network share| Quarantined files are stored on the specified network share. The share is mounted as CIFS, so the remote share must support this protocol. Read  
  and write permissions are required. McAfee MOVE AntiVirus supports only Windows share path for  
  quarantine network share. Linux share path is not supported for quarantine network share.  
  Enter the IP address or FQDN so that it can be resolved by the SVM. How this is entered depends  
  on the environment and how the SVM is configured. |
| Network domain name | The domain used to access the specified share. |
| Network user name     | The user name used to access the specified share. |
| Network password     | The password used to access the specified share. |

**Restore quarantined items (Multi-Platform)**

McAfee MOVE AntiVirus deletes any items that are detected as threats, converts a copy of the item to a non-executable format, and saves it in the Quarantine folder.

**Before you begin**

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

You can restore a quarantined item.

**Task**

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

2. Select Menu | Policy | Client Task Catalog.

3. From Client Task Types, select MOVE AntiVirus 4.6.0 | Restore from Quarantine (Multi-Platform).

4. Click the name of an existing client task or click New Task, then confirm the task type.
5 Configure these settings on each tab, then click **Save**.

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task Name</td>
<td>Specifies a unique name for the task.</td>
</tr>
<tr>
<td>Description</td>
<td>Specifies a description about the task.</td>
</tr>
<tr>
<td>Detection name</td>
<td>Specifies the exact detection name of the item to restore from quarantine. You can find the Threat Name under Menu</td>
</tr>
<tr>
<td></td>
<td>If TIE is disabled, the detection name of the item might be Artemis!EB51D377817C,RDN/Generic.dx!dqq</td>
</tr>
<tr>
<td></td>
<td>If TIE is enabled, the detection name of the item might be TIE! 4414f6c4303c2ce9a23261a880b3ee6b3ef4f378. The detection name of the item is prefixed with TIE! and suffixed with the SHA-1 reputation value of the item.</td>
</tr>
</tbody>
</table>

6 Click **Assign**, specify the servers where you want to assign the task, then click **OK**.

7 Click **Schedule** to schedule the task.

You can also use the `mvadm` command on the client system to restore the quarantined items:
```
mvadm q restore <Detection_Name>
```

---

### How quarantine works (Agentless)

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

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

A file is quarantined when:

- **The Quarantine network share** configuration, which is present in the **Options** policy, is mounted.
- A detection occurs.
- **Delete files automatically and quarantine** is the primary action. Quarantined files are automatically deleted after 28 days.

If no quarantine policy is configured, the **Delete files automatically and quarantine** action does not occur even if it is configured as the primary action in the scan policies.
The restore tool at-a-glance
This diagram provides an overview of how the quarantine restore tool works.

The restore tool requires Java Runtime Environment (JRE) 1.8.

- Modify quarantine_restore.cmd by adding `-Djava.net.preferIPv4Stack=true` to the JVMARGS variable.

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

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

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

Task
1. Right-click the quarantine folder, then select Properties.
2. Select the Sharing tab, then click Advanced Sharing.
3. In the Advanced Sharing dialog box, select Share this folder.
4. Click Permissions, select the default user name Everyone, click Remove, then click Apply.
Click Add to select an object type.

You can give permission only to administrators who need access to the quarantine folder.

a In Select Users or Groups, enter your Domain User account in the object names dialog box, then click OK.

b Select the user name you created earlier, select Full Control, then click OK.

Click Add to select an object type.

a In Select Users or Groups, enter your Domain Local Security Group in the object names dialog box, then click OK.

b With this group selected, select Full Control, then click OK.

### Restore a file

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

**Before you begin**

- Update the DATs on the SVM and the system where you run the restore, when needed.
- Download MOVE-AV-AL_RestoreTool.4.5.1.Zip from the McAfee download site and extract the contents.
- Make sure that the TCP port 445 is open on the guest VM’s firewall.

**Task**

1. From the folder where you extracted MOVE-AV-AL_RestoreTool.4.5.1.Zip, start the quarantine restore tool.

   `quarantine_restore.cmd`

   The Connect dialog box is automatically displayed.

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

   McAfee MOVE AntiVirus supports only Windows share path for quarantine network share.

   If you need to connect to a different share, click Connect.

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

   If a file is listed multiple times, it has been quarantined multiple times and the contents of the file are different.

4. Choose one of these options:

   - Save the file to your local system.
     1. Select Save File.
     2. Browse to the location, enter a file name, and click OK.

       The file is saved to the specified location. The quarantined file remains on the share.

   - Restore the file to selected VMs.
     1. Select the VMs where you want to restore the file, then click Restore.
     2. Enter valid credentials to restore the file to all selected VMs.
The same file can be restored to multiple VMs by multi-selecting the VM hosts before you click Restore. The same credentials must be valid for all selected VMs for this method to work.

The file is restored to each selected VM. The quarantined file is removed from the share after it is successfully restored. When the restore is completed, the list of quarantined files and VMs are updated to reflect the current state.

Errors are logged on the RestoreTool.log.

How tagging works in an NSX environment (Agentless)

When malware is detected on a VM where you configured NSX tagging, the affected VM is tagged with the NSX tag (ANTI_VIRUS.VirusFound.threat=high).

- In the On Access Scan policy, if the primary action is configured to Delete files automatically or Delete files automatically and quarantine, and when malware is detected and deleted on a client system, the NSX tagging and untagging happens at the same time. The malware detection details can be viewed in McAfee ePO Orion logs.

- In the On Access Scan policy, if the primary action is configured to Deny access to files and when malware is detected and deleted on a client system, the client system is tagged with ANTI_VIRUS.VirusFound.threat=high. The tag is removed on the next successful completion of an on-demand scan.

- In the On Access Scan policy, if the primary action is configured to Delete files automatically and quarantine and the quarantine details are not configured, and when malware is detected and deleted on the client system, the client system is tagged with the NSX tag ANTI_VIRUS.VirusFound.threat=high. The tag is removed on the next successful completion of an on-demand scan.

- When you run on-demand scan and malware is detected on a VM, the NSX tag is removed for the VM only if the primary action is configured to Delete files automatically or Delete files automatically and quarantine.

Self-protection

The self-protection feature defends files, services, and registry keys on virtual machines. Use the VirusScan Enterprise access protection rules for protecting the components of the SVM.

McAfee MOVE AntiVirus (Multi-Platform) Client

The self-protection feature prevents malicious attacks on McAfee MOVE AntiVirus (Multi-Platform) client components. This keeps your virus protection active and stable.

<table>
<thead>
<tr>
<th>Protection type</th>
<th>Protection effects</th>
</tr>
</thead>
<tbody>
<tr>
<td>File protection</td>
<td>Files inside the installed directory and driver file (mvagtdrv.sys) are protected from being deleted or renamed.</td>
</tr>
<tr>
<td>Registry protection</td>
<td>These registry keys, all subkeys, and all values under them are protected.</td>
</tr>
<tr>
<td>Service stop protection</td>
<td>The mvagtsvc service cannot be stopped.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protection type</th>
<th>Protection effects</th>
</tr>
</thead>
<tbody>
<tr>
<td>File protection</td>
<td>Files inside the installed directory and driver file (mvagtdrv.sys) are protected from being deleted or renamed.</td>
</tr>
<tr>
<td>Registry protection</td>
<td>These registry keys, all subkeys, and all values under them are protected.</td>
</tr>
<tr>
<td>Service stop protection</td>
<td>The mvagtsvc service cannot be stopped.</td>
</tr>
</tbody>
</table>
The self-protection feature is controlled by the IntegrityEnabled configuration parameter. By default, the parameter is set to 0x7, and all components of the feature are enabled.

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

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

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

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

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

```bash
mvadm config set IntegrityEnabled=5
```

To disable the self-protection feature, set the parameter to 0 with this command:

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

When Service stop protection is enabled (by setting the highest bit to 1), the mvagtsvc service does not accept stop commands. File protection and registry protection require the agent driver be loaded, but service stop protection does not.

**McAfee MOVE AntiVirus (Multi-Platform) SVM**

Use the following VirusScan Enterprise access protection rules for protecting the components of the SVM. These must be configured manually after installation.
Protection type | Protection effects
--- | ---
File protection (via VirusScan Enterprise access protection) | Use the user defined rules of VirusScan Enterprise to protect MOVE files. Create a **File/Folder Access Protection Rule** that excludes the `mvserver.exe` process, and blocks the `C:\Program Files (x86)\McAfee\MOVE AV Server\** folder.

For **File actions to prevent**, select these options:

- Write access to files
- New files being created
- Files being deleted

See *McAfee VirusScan Enterprise Product Guide* for details.

Registry protection (via VirusScan Enterprise access protection) | Use the user defined rules of VirusScan Enterprise to protect registry keys.

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

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mvserver`
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mvserver\Parameters`
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mvserver\Parameters\ODS`

**Events, responses, and McAfee MOVE AntiVirus**

Configure Automatic Responses to respond to threat events.

The Threat Event Log is a log file of all threat events that McAfee ePO receives from managed systems.

In McAfee ePO, you can define which events are forwarded to the McAfee ePO server. To display the complete list of events in McAfee ePO, select **Menu | Configuration | Server Setting**, select **Event Filtering**, then click **Edit**.

Set up a Purge Threat Event Log server task to purge the Threat Event Log periodically.

For information about Automatic Responses and working with the Threat Event Log, see the McAfee ePO documentation.

**Analyzing your protection**

The ongoing process of analyzing your system protection enables you to improve the protection and performance of your system.

Analyzing your protection helps you determine:

- Which threats you are facing
- What malware was used in the attack
- Where the threats are coming from
- Where and when the attacks occurred
- How often threats are found
- Which systems are being targeted
- How the attack affected the system

Protection analysis is also helps you:

- Create reports for IT and managers.
- Capture information used to create scripts and queries.
Dashboards and queries

Use McAfee ePO queries to view events, run default queries, and create reports.

- View events in the Threat Event Log.
- Run default queries that show important client information.
- Create reports using data sent by the McAfee Agent to the McAfee ePO database.

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

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

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

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

VMs running Agentless do not have the McAfee Agent installed. Only the SVM appears in the McAfee ePO console, which means you don't see each VM. vShield Manager provides a report that validates the protection status of each VM.

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.

How Threat Intelligence Exchange works

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

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

Threat Intelligence Exchange includes these components.

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

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

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

**How Advanced Threat Defense works**

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

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

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

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

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

**Advanced Threat Defense components**

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

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

- A local blacklist to quickly detect known malware.
- McAfee GTI for cloud lookups to detect malware that has already been identified by organizations throughout the globe.
- Embedded McAfee Gateway Anti-Malware Engine in for emulation capability.
- Embedded McAfee Anti-Malware Engine embedded in for signature-based detection.
- A virtual sandbox environment for dynamic file analysis.
Scenarios for using Threat Intelligence Exchange

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

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

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

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

How a reputation is determined

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

1. A user or system tries to run a file.
2. McAfee MOVE AntiVirus compares and inspects the file with local cache and can't determine its validity and reputation.
3. The client looks for the reputation in global cache in the SVM and can't find the reputation, then sends the file hashes to the SVM for TIE lookup based on the **Shared Cloud Solutions** policy assigned to the system.
4. The SVM checks the reputation cache for the file hash. If the file hash is found, the SVM gets the reputation data from the SVM cache and sends the reputation to the client and action is taken.
5. If the file hash is not found in the SVM cache and TIE server does not have the reputation:
   • (Advanced Threat Defense is present) If the policy on the endpoint determines that the file has to be sent to Advanced Threat Defense, the TIE server sends the file for further analysis. To send the file to Advanced Threat Defense, these requirements must meet:
     • **Advanced Threat Defense (ATD)** option is configured in the **Shared Cloud Solutions** policy on the McAfee ePO server.
     • Size of the file is less than 10 MB.
     • The TIE server returns the file hash's reputation to the SVM once the data is received from Advanced Threat Defense after analyzing the file.
6. McAfee MOVE AntiVirus responds based on the **Shared Cloud Solutions** policy assigned to the system that is running the file.
7. The SVM sends threat details as threat events to McAfee ePO.

How a reputation is determined with TIE 2.0.0

When the SVM sends a signed file for certificate lookup and this certificate has a file that has administrator overridden file reputation, the file hash is sent for file reputation lookup again. Then the overridden file reputation is considered for the file, ignoring certificate reputation value.

For example, let us consider a scenario where:
• The file has a certificate value as **Known trusted**
• The file reputation of any files associated with the same certificate is overridden by the administrator to **Known malicious**

With these assumptions, when an SVM sends a file for TIE lookup, TIE notifies that it has a file reputation overridden for the certificate. Then the SVM sends for file reputation again and responds based on the file reputation.
Monitoring activity in your environment

An important step in a protection strategy is using tools to monitor the malware events that occur on your systems.

Contents

- Monitoring activity with McAfee ePO
- McAfee MOVE AntiVirus dashboard
- Check visibility and health details of the SVM
- Check predefined queries
- McAfee MOVE AntiVirus server tasks

Monitoring activity with McAfee ePO

Use McAfee ePO to monitor activity on your managed systems and determine what to do when issues occur. Dashboards are collections of monitors that track activity in your McAfee ePO environment.

McAfee MOVE AntiVirus provides predefined dashboards and monitors. Depending on your permissions, you can use them as is, modify them to add or remove monitors, or create custom dashboards.

McAfee MOVE AntiVirus dashboard

The McAfee MOVE AntiVirus dashboard is added to your McAfee ePO server when you install the software. The dashboard displays a collection of monitors based on the results of the default McAfee MOVE AntiVirus software queries.

The default monitors that appear on the McAfee MOVE AntiVirus dashboard are:

- **SVM Load: Number of Connected Endpoints** — Displays the number of managed endpoints with load category of the SVM.
  - **Capacity Full** — Indicates that the SVM limit is reached when the number of endpoints is equal to what can be assigned.
  - **Capacity Above Threshold** — Appears when capacity of an SVM is more than its threshold value.
  - **Capacity Below Threshold** — Appears when capacity of an SVM is less than its threshold value.
- **SVM with Higher Average Scan Time in last 7 days** — Specifies the top 10 SVMs, which have reached average scan time threshold and they are in this state for the longest time in the past 7 days.

See the chapter on dashboards in the *McAfee ePolicy Orchestrator Product Guide* for information about managing dashboards.
Check visibility and health details of the SVM

You can view and check the product properties of McAfee MOVE AntiVirus and the product component SVM using McAfee ePO.

Task
1. Log on to McAfee ePO as an administrator.
2. Select Menu | Systems | System Tree | Systems tab.
3. Click an SVM system to open the System Information page.
4. Click Product tab and select the product as MOVE AntiVirus.

You can now see the product properties, which can be used to determine the health details of the SVM.

Check predefined queries

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

Task
1. Log on to McAfee ePO as an administrator.
2. Select Menu | Reporting | Queries & Reports.
3. From the McAfee Groups pane, select MOVE AntiVirus 4.6.0 to display the queries for the selected group.
4. From the Queries list, select a query, then click Run.
5. On the query results page, click any item in the results to drill down further.
6. Click Close when finished.

Predefined Multi-Platform queries

The McAfee MOVE AntiVirus (Multi-Platform) deployment option adds several queries to your McAfee ePO environment.

| Table 4-1 Multi-Platform queries |
|-----------------|---------------------------------|
| **Query**       | **Description**                 |
| Client Protection Status | Displays the status of all McAfee MOVE AntiVirus clients managed by the server. |
| Clients connected with a given SVM | Displays the details of the client and the SVM that is assigned to it. |
| DAT version | Displays the DAT version of all McAfee MOVE AntiVirus clients that are managed by the server. |
| Summary of Threats Detected in the Last 24 Hours | Displays threats detected in the last 24 hours. |
| Threats Detected in the Last 24 Hours | Displays the number of threats detected in the last 24 hours by hour. |
| Top 10 Computers with the Most Detections | Displays the top 10 computers with the most threat detections in the last three months. |
| Top 10 Detected Threats | Displays the top 10 detected threats in the last three months. |
### Table 4-1 Multi-Platform queries (continued)

<table>
<thead>
<tr>
<th>Query</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 10 Users with the Most Detections</td>
<td>Displays the top 10 users with the most threat detections in the last three months.</td>
</tr>
<tr>
<td>TIE/ATD Metrics for each MP SVM</td>
<td>Lists all TIE or Advanced Threat Defense related metrics such as Total File reputation requests to TIE, Total Certificate reputation requests to TIE, and Total number of Advanced Threat Defense candidates for each McAfee MOVE AntiVirus SVM.</td>
</tr>
</tbody>
</table>

### Table 4-2 Client queries and events

<table>
<thead>
<tr>
<th>Query</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MP Connectivity Details</td>
<td>Displays the connectivity status details between an SVM and SVM manager, and a client and SVM Manager such as Success, Failed, and Unassigned.</td>
</tr>
</tbody>
</table>

Before running this report, make sure that you run these client tasks:
- Check SVM Assignment
- Check SVM Connectivity
- Check SVM Manager Connectivity

### Table 4-3 SVM queries and events

<table>
<thead>
<tr>
<th>Query</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVM Load: Number of Connected Endpoints</td>
<td>Categorizes the SVMs into Capacity full, Capacity Above Threshold, and Capacity Below Threshold based on the number of connected endpoints.</td>
</tr>
<tr>
<td>SVM with Higher Average Scan Time in last 7 days</td>
<td>Specifies the top 10 SVMs, which have reached the average scan time threshold and are in this state for the longest time in the past 7 days.</td>
</tr>
<tr>
<td>SVM with SVM Manager details</td>
<td>Lists all SVMs with SVM Manager details.</td>
</tr>
<tr>
<td>SVM: Average Scan Time Events</td>
<td>Lists the SVM Average Scan Time, SVM Average Scan Time Threshold, and SVM Average Scan Time Sampling Interval details. This report is generated from SVM average Scan Time Threshold hit and SVM Average Scan Time Threshold Restored events. The average scan time threshold for each SVM can be modified in the Alert me option in the SVM Settings policy.</td>
</tr>
<tr>
<td>SVM Capacity Events</td>
<td>Lists the SVM Capacity Full, SVM Capacity Restored, and SVM Capacity Threshold hit details. This report is generated from SVM Capacity Threshold hit, SVM Capacity Full, and SVM Capacity Threshold Restored event. The threshold limit of client connections for each SVM can be modified in the Alert me option in the SVM Settings policy.</td>
</tr>
<tr>
<td>Top 10 Scanned File Extensions for each SVM</td>
<td>Lists the top 10 file extensions scanned by the SVM.</td>
</tr>
<tr>
<td>Top 10 Scanned Files for each SVM</td>
<td>Lists the top 10 files scanned by the SVM.</td>
</tr>
<tr>
<td>Top 10 Scanned Processes for each SVM</td>
<td>Lists the top 10 processes scanned by the SVM.</td>
</tr>
<tr>
<td>Top 10 Scanned Virtual Machines for each SVM</td>
<td>Lists the top 10 virtual machines that are sending maximum scan and checksum requests.</td>
</tr>
<tr>
<td>MP Error Codes Data</td>
<td>Displays the error code details that occurred while managing McAfee MOVE AntiVirus.</td>
</tr>
</tbody>
</table>
Table 4-4  SVM Manager queries and events

<table>
<thead>
<tr>
<th>Query</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVM Assignment Failed</td>
<td>Specifies the details and reasons of SVM assignment by the SVM Manager. This event is reported on the McAfee ePO server.</td>
</tr>
<tr>
<td></td>
<td>• SVM_MANAGER_SVM_ASSIGNMENT_FAILED — This event is reported when an SVM assignment request is sent from a client to the SVM Manager and it is unable to complete the client request, because no registered SVM is reported with full capacity.</td>
</tr>
<tr>
<td>SVM Capacity Events</td>
<td>Specifies the maximum number of endpoints with the number of endpoints connected. These events are reported on the McAfee ePO server.</td>
</tr>
<tr>
<td></td>
<td>• SVM_MANAGER_SVM_THRESHOLD_CAPACITY_HIT — This event is reported when an SVM assignment request is sent from a client to the SVM Manager and cumulative capacity of all SVMs eligible to serve that client has reached the threshold value, which is set in the advanced options of the SVM Manager policy.</td>
</tr>
<tr>
<td></td>
<td>• SVM_MANAGER_SVM_CAPACITY_FULL — This event is reported when an SVM assignment request is sent from a client to the SVM Manager and all SVM eligible to serve that client have reached their full capacity.</td>
</tr>
<tr>
<td>SVM Registration Events</td>
<td>Displays the SVM registration events raised by the SVM Manager. These events are reported on the McAfee ePO server.</td>
</tr>
<tr>
<td></td>
<td>• SVM_MANAGER_SVM_REGISTER — This event is reported when an SVM is registered with SVM Manager.</td>
</tr>
<tr>
<td></td>
<td>• SVM_MANAGER_SVM_UNREGISTER — This event is reported when an SVM is unregistered from the SVM Manager because of issues like SVM shutdown, network interruptions.</td>
</tr>
</tbody>
</table>

SVM_MANAGER_STARTED This event is reported when the SVM Manager starts.

SVM_MANAGER_STOPPED This event is reported when the SVM Manager stops.

You can add these queries to dashboards to more efficiently track your environment by displaying several queries at once.

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

The McAfee ePO Threat Event Log contains information about detections, scan failure, and on-demand scan events.

SVM information

A shell script, msmclient.sh, is available with SVM Manager and is used to retrieve the SVM details. The script is available at /opt/McAfee/movesvamanager.

For these commands to work and retrieve the results, the SVM Manager application must be running.

Run these commands with root rights from the /opt/McAfee/movesvamanager directory:

• sudo ./msmclient.sh osscount — Displays the number of SVMs attached to the SVM Manager.

• sudo ./msmclient.sh ossinfo — Displays some basic information about the SVMs attached to the SVM Manager.

• sudo ./msmclient.sh ossdetails — Displays some advanced information about the SVM: current SVM load, SVM GUID, and last heartbeat time.
Predefined Agentless queries

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

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

The Agentless deployment option provides these predefined queries:

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

Contents
- (Multi-Platform) MOVE AntiVirus : Generate Certificates
- (Agentless) MOVE AntiVirus: Compute licensing information

(Multi-Platform) MOVE AntiVirus : Generate Certificates
If there is a connectivity issue with the SVM Manager, you must generate the certificates for McAfee MOVE AntiVirus, so that the McAfee MOVE AntiVirus SVM and SVM Manager communicate and authenticate each other properly. For details, see the McAfee MOVE AntiVirus 4.6.0 Installation Guide

(Agentless) MOVE AntiVirus: Compute licensing information
From Menu | Automation | Server Tasks, you can run MOVE AntiVirus: Compute licensing information server task to list the number of VMs being managed by the licensed SVM. You can find the output of this server task from MOVE AntiVirus: Licensing information Queries & Reports.
Troubleshooting

Use this information to resolve problems while running McAfee MOVE AntiVirus and using its deployment modes.

Contents
- Error codes
- Frequently asked questions

Error codes

Here are steps to troubleshoot some of the errors that you might see while deploying and managing the McAfee MOVE AntiVirus product. You might see these errors on the McAfee ePO pages or in the log files.

Product Area: McAfee MOVE AntiVirus extension

You might see these errors on the McAfee ePO pages or in the log files while deploying and managing the McAfee MOVE AntiVirus product using McAfee MOVE AntiVirus extension.

MOVE_ERROR_30001

<table>
<thead>
<tr>
<th>Error string:</th>
<th>[MOVE_ERROR_30001] Critical error. Downloading ePO init files failed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cause:</td>
<td></td>
</tr>
<tr>
<td>For Static IP Pool</td>
<td>The provided IP Pool details might be wrong.</td>
</tr>
<tr>
<td>For DHCP</td>
<td>The DNS might not be able to ping FQDN or host name of the McAfee ePO server.</td>
</tr>
<tr>
<td>Workaround:</td>
<td></td>
</tr>
<tr>
<td>For Static IP Pool</td>
<td>1 FQDN is resolved from McAfee ePO and the client and vice versa.</td>
</tr>
<tr>
<td></td>
<td>2 Verify that the provided IP Pool details are correct.</td>
</tr>
<tr>
<td>For DHCP</td>
<td>1 FQDN is resolved from McAfee ePO and the client and vice versa.</td>
</tr>
<tr>
<td></td>
<td>2 Verify that the DNS that you got through DHCP can ping FQDN or host name of the McAfee ePO server.</td>
</tr>
</tbody>
</table>
**MOVE_ERROR_30002**

**Error string:** [MOVE_ERROR_30002] Compatibility checking failed

**Cause:** MOVEALCompatMatrix.xml might not be compatible with the versions of vCenter, ESXi, vShield Manager, vShield Endpoint, and VM Tools.

**Workaround:** This error can be ignored because it does not impact while deploying and managing the McAfee MOVE AntiVirus product.

---

**MOVE_ERROR_30003**

**Error string:** [MOVE_ERROR_30003] For some VM's either VMTools is not running or VM's are not part of the AD, hence, vShield driver installation will fail on them

**Cause:** VM Tools are not running on some of the VMs or the VMs are not part of the Active Directory server.

**Workaround:**
1. Verify that VMware Tools are running properly on all VMs.
2. Verify that the VMs are part of the Active Directory server.
3. Verify that you configured and registered all LDAP servers, which are managing the client systems to be protected.

---

**MOVE_ERROR_30004**

**Error string:** [MOVE_ERROR_30004] All VM's in the Hypervisor are not part of the AD, vShield driver installation will fail on them

**Cause:** The VMs are not part of the Active Directory server.

**Workaround:**
1. Verify that the VMs are part of the Active Directory server.
2. Verify that you configured and registered all LDAP servers, which are managing the client systems to be protected.

---

**MOVE_ERROR_30005**

**Error string:** [MOVE_ERROR_30005] VMTools in some VM's are not running, vShield driver installation might fail on them

**Cause:** VMware Tools is not running on some of the VMs.

**Workaround:**
1. Verify that the VMs are part of the Active Directory server.
2. Verify that you have configured and registered all LDAP servers, which are managing the client systems to be protected.
**MOVE_ERROR_30007**

**Error string:** [MOVE_ERROR_30007] Rest api call failed with exception

**Cause:**
- **For vCNS environment:** vShield Manager details are not configured properly in McAfee ePO.
- or
- **For NSX environment:** NSX Manager details are not configured properly in McAfee ePO.

**Workaround:**
- **For vCNS environment**
  1. Verify that you configured the vShield Manager details in the MOVE AntiVirus Deployment wizard properly in McAfee ePO.
  2. From the McAfee ePO system, open SQL Server and verify the details in the `DC_AL_VSM_DETAILS` table.
- **For NSX environment**
  1. Verify that you configured the NSX Manager details properly in the MOVE AntiVirus Deployment wizard in McAfee ePO.
  2. From McAfee ePO system, open SQL Server and verify the details in the `DC_AL_NSX_MANAGER_DETAILS` table.

**MOVE_ERROR_30008**

**Error string:** [MOVE_ERROR_30008] Getting vsm heartbeat details : `<APPLIANCE_URL>` failed using : `<CLIENT_DETAILS>`

**Cause:** The vShield Manager might not be running.

**Workaround:**
Verify that the vShield Manager is up and running.

**MOVE_ERROR_30009**

**Error string:** [MOVE_ERROR_30009] Error occurred while executing service setup task. Continuing with next setup

**Cause:** VMs might not be synchronized properly from the vCeter account in McAfee ePO.

**Workaround:**
Synchronize the vCeter account on the Registered Cloud Account page in McAfee ePO.

**MOVE_ERROR_30010**

**Error string:** [MOVE_ERROR_30010] NSX Manager is already registered with different McAfee ePO.

**Cause:** NSX Manager is registered with another McAfee ePO.

**Workaround:**
1. Verify that the vCenter account is registered with another McAfee ePO.
2. Verify that the NSX Manager is registered with another McAfee ePO in the MOVE AntiVirus Deployment wizard.
3. Unregister the MOVE service from the Service Registration page in the MOVE AntiVirus Deployment wizard in McAfee ePO.
**MOVE_ERROR_30011**

**Error string:** [MOVE_ERROR_30011] Error occurred while communicating with NSX Manager.

**Cause:** NSX certificate details are not valid.

**Workaround:**
1. Reconfigure and validate the NSX Manager details on the **Edit NSX Manager Details** page in the MOVE AntiVirus Deployment wizard.
2. Verify that the validation is successful.

**MOVE_ERROR_30012**

**Error string:** [MOVE_ERROR_30012] MOVE Service cannot be unregistered or upgraded because it is used in NSX Manager Security Policy.

**Cause:** The Security Policy is being used in NSX Manager.

**Workaround:**
2. Click **Edit** on each security policy.
3. From the **Guest Introspection Services** page, delete the security policy.
4. Verify that **Guest Introspection Services** is showing as 0 for all listed policies on the **Security Policy** page.
5. Delete McAfee MOVE Service deployment from the **Service Deployments** page.

**MOVE_ERROR_30013**

**Error string:** [MOVE_ERROR_30013] MOVE Service cannot be unregistered because it is deployed on cluster(s).

**Cause:** SVM is deployed on the cluster(s).

**Workaround:**
2. Click **Edit** on each security policy.
3. From the **Guest Introspection Services** page, delete the security policy.
4. Verify that **Guest Introspection Services** is showing as 0 for all listed policies on the **Security Policy** page.
5. Delete McAfee MOVE Service deployment from the **Service Deployments** page.

**Product Area: McAfee MOVE AntiVirus client (Multi-Platform)**

You might see these errors on the Queries & Reports (**MOVE AntiVirus: Error Code Details** or **MOVE AntiVirus: Multi-Platform Connectivity Status**) in McAfee ePO or in the log files.

**Error code: 12002**

**Error reason string:** SVM Registration with SVM Manager failed

**Cause:** Communication issue between client and the SVM Manager or SVM and the SVM Manager.

**Workaround:**
1. Verify that the SVM Manager IP details are configured in the **Options** policy in McAfee ePO.
2. Verify that the **Options** policy is assigned to the client and SVM.
### Error code: 12029

<table>
<thead>
<tr>
<th>Error reason string:</th>
<th>SVM Registration with SVM Manager failed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cause:</td>
<td>Communication issue between client and the SVM Manager or SVM and the SVM Manager.</td>
</tr>
</tbody>
</table>
| Workaround:          | 1 Verify that the SVM Manager IP details are configured in the Options policy in McAfee ePO.  
                        | 2 Verify that the Options policy is assigned to the client and SVM. |

### Error code: 40001

<table>
<thead>
<tr>
<th>Error string:</th>
<th>SVM Registration with SVM Manager failed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cause:</td>
<td>SVM is not available with SVM Manager to assign it to the client.</td>
</tr>
</tbody>
</table>
| Workaround:         | 1 Deploy the McAfee MOVE AntiVirus SVM to a virtual machine.  
                        | 2 Verify that the SVM Manager IP details are configured in the Options policy in McAfee ePO.  
                        | 3 Assign the Options policy to the newly deployed SVM system. |

### Product Area: McAfee MOVE AntiVirus SVM (Multi-Platform)

You might see these errors on the Queries & Reports (MOVE AntiVirus: Error Code Details or MOVE AntiVirus: Multi-Platform Connectivity Status) in McAfee ePO or in the log files.

### Error code: 15

<table>
<thead>
<tr>
<th>Error string:</th>
<th>Failed to send request to the TIE server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cause:</td>
<td>McAfee DXL client and DXL broker might not be compatible.</td>
</tr>
<tr>
<td>Workaround:</td>
<td>Verify that the McAfee DXL client and DXL broker version is compatible.</td>
</tr>
</tbody>
</table>

### Error code: 16

<table>
<thead>
<tr>
<th>Error string:</th>
<th>Failed to send request to the TIE server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cause:</td>
<td>McAfee DXL client service might be stopped / MOVE service might not be recognized the McAfee DXL client.</td>
</tr>
</tbody>
</table>
| Workaround:         | 1 Log on to the McAfee MOVE AntiVirus SVM system.  
                        | 2 Open Task Manager and verify that the McAfee DXL client service appears.  
                        | 3 From system tray, click and select About... to open McAfee About... window.  
                        | 4 Under McAfee Data Exchange Layer, verify that the DXL Connected Status is Connected.  
                        | 5 Restart the MOVE service. |
**Error code: 201**

<table>
<thead>
<tr>
<th>Error string:</th>
<th>Failed to send request to the TIE server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cause:</td>
<td>DXL fabric might not be connected.</td>
</tr>
<tr>
<td>Workaround:</td>
<td>1 In the System Tree, click the TIE server name, then click <strong>Products</strong>. Verify that the following components are listed with the corresponding version for the installation process.</td>
</tr>
<tr>
<td></td>
<td>• McAfee DXL Broker</td>
</tr>
<tr>
<td></td>
<td>• McAfee DXL Client</td>
</tr>
<tr>
<td></td>
<td>• McAfee Threat Intelligence Exchange Server</td>
</tr>
<tr>
<td></td>
<td>2 In the System Tree, verify that the TIESERVER and DXLBROKER tags were applied to the system.</td>
</tr>
<tr>
<td></td>
<td>3 Select **Menu</td>
</tr>
<tr>
<td></td>
<td>4 In the System Tree, select the TIE server, then from the <strong>Actions</strong> menu, select **DXL</td>
</tr>
<tr>
<td></td>
<td>5 Verify that the <strong>Connection State</strong> is <strong>Connected</strong>.</td>
</tr>
<tr>
<td></td>
<td>6 Log on to the McAfee MOVE AntiVirus SVM system.</td>
</tr>
<tr>
<td></td>
<td>7 From system tray, click ![System Tray Icon] and select <strong>About</strong>... to open McAfee <strong>About</strong>... window.</td>
</tr>
<tr>
<td></td>
<td>8 Under <strong>McAfee Data Exchange Layer</strong>, verify that the <strong>DXL Connected Status</strong> is <strong>Connected</strong>.</td>
</tr>
</tbody>
</table>

**Error code: 202**

<table>
<thead>
<tr>
<th>Error string:</th>
<th>Failed to send request to the TIE server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cause:</td>
<td>DXL fabric might be trying to connect continuously.</td>
</tr>
<tr>
<td>Workaround:</td>
<td>1 In the System Tree, click the TIE server name, then click <strong>Products</strong>. Verify that the following components are listed with the corresponding version for the installation process.</td>
</tr>
<tr>
<td></td>
<td>• McAfee DXL Broker</td>
</tr>
<tr>
<td></td>
<td>• McAfee DXL Client</td>
</tr>
<tr>
<td></td>
<td>• McAfee Threat Intelligence Exchange Server</td>
</tr>
<tr>
<td></td>
<td>2 In the System Tree, verify that the TIESERVER and DXLBROKER tags were applied to the system.</td>
</tr>
<tr>
<td></td>
<td>3 Select **Menu</td>
</tr>
<tr>
<td></td>
<td>4 In the System Tree, select the TIE server, then from the <strong>Actions</strong> menu, select **DXL</td>
</tr>
<tr>
<td></td>
<td>5 Verify that the <strong>Connection State</strong> is <strong>Connected</strong>.</td>
</tr>
<tr>
<td></td>
<td>6 Log on to the McAfee MOVE AntiVirus SVM system.</td>
</tr>
<tr>
<td></td>
<td>7 From system tray, click ![System Tray Icon] and select <strong>About</strong>... to open McAfee <strong>About</strong>... window.</td>
</tr>
<tr>
<td></td>
<td>8 Under <strong>McAfee Data Exchange Layer</strong>, verify that the <strong>DXL Connected Status</strong> is <strong>Connected</strong>.</td>
</tr>
</tbody>
</table>
## Error code: 11

**Error string:** Failed to send request to the TIE server  
**Cause:** TIE server might not be running.  
**Workaround:**  
1. Log on to the TIE server as a root user.  
2. Run this command: `service tieserver status`  
3. Verify that the PostgreSQL for McAfee TIE Server and ties server and McAfee TIE Server status appears running.  
4. If these are not running, perform these actions.  
   a. Run this command: `service tieserver start`  
   b. Verify that the PostgreSQL for McAfee TIE Server and ties server and McAfee TIE Server started running.

## Error code: 1

**Error string:** SVM is shutting down  
**Cause:** MOVE AV Server service might not be running or SVM might not be functional.  
**Workaround:**  
1. Make sure that the McAfee MOVE AntiVirus SVM system is turned on.  
2. Log on to the McAfee MOVE AntiVirus SVM system.  
3. Make sure that the MOVE AV Server service is running.

## Error code: 2

**Error string:** SVM is max client threshold reached  
**Cause:** The number of clients connected to the SVM is more than its threshold value.  
**Workaround:**  
1. Log on to the McAfee ePO server as an administrator.  
2. Deploy the McAfee MOVE AntiVirus SVM to your virtual machine(s).

## Error code: 3

**Error string:** SVM to client heartbeat break  
**Cause:** SVM might be turned off or SVM might be over loaded or SVM and client version is not compatible.  
**Workaround:**  
1. Make sure that the McAfee MOVE AntiVirus SVM system is turned on.  
2. Verify that the SVM is not over loaded.  
3. Verify that the SVM and client version is compatible.
### Error code: 4

<table>
<thead>
<tr>
<th><strong>Error string:</strong></th>
<th>Client to SVM connection failed</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cause:</strong></td>
<td>SVM might be turned on or MOVE AV Server service might not be running.</td>
</tr>
</tbody>
</table>
| **Workaround:**   | 1 Verify that the McAfee MOVE AntiVirus SVM is running.  
2 Make sure that the MOVE AV Server service is running. |

### Error code: 12002

<table>
<thead>
<tr>
<th><strong>Error string:</strong></th>
<th>Failed to submit file to ATD server</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cause:</strong></td>
<td>ATD might not be integrated properly.</td>
</tr>
</tbody>
</table>
| **Workaround:**   | 1 Log on to the McAfee ePO as an administrator.  
2 Select Menu | Policy | Policy Catalog, then select McAfee Threat Intelligence Exchange Server Management from the Product list.  
3 Click the TIE Server Settings policy that is applied to the SVM.  
4 Under Advanced Threat Defense tab, make sure that Username, Password, and Server details are configured.  
5 On the McAfee MOVE AntiVirus SVM system, run this command: mvadm stats  
6 Verify that Total ATD candidates and Total ATD successful submissions values appear. |

### Error code: 12029

<table>
<thead>
<tr>
<th><strong>Error string:</strong></th>
<th>Failed to submit file to ATD server</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cause:</strong></td>
<td>ATD might not be integrated properly.</td>
</tr>
</tbody>
</table>
| **Workaround:**   | 1 Log on to the McAfee ePO as an administrator.  
2 Select Menu | Policy | Policy Catalog, then select McAfee Threat Intelligence Exchange Server Management from the Product list.  
3 Click the TIE Server Settings policy that is applied to the SVM.  
4 Under Advanced Threat Defense tab, make sure that Username, Password, and Server details are configured.  
5 On the McAfee MOVE AntiVirus SVM system, run this command: mvadm stats  
6 Verify that Total ATD candidates and Total ATD successful submissions values appear. |
Product Area: McAfee MOVE AntiVirus SVM (Agentless)

You might see these errors on the McAfee ePO pages or in the log files while deploying and managing the McAfee MOVE AntiVirus SVM (Agentless).

**MOVE_ERROR_20001**

<table>
<thead>
<tr>
<th>Error string:</th>
<th>[MOVE_ERROR_20001] Failed to create quarantine mount event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cause:</td>
<td>Quarantine details might not be configured properly.</td>
</tr>
<tr>
<td>Workaround:</td>
<td>1 Verify that quarantine details are configured in the Options policy in McAfee ePO.</td>
</tr>
<tr>
<td></td>
<td>2 Run the policy collector and send an wake-up agent call to the target SVM.</td>
</tr>
<tr>
<td></td>
<td>3 From the SVM, open /opt/McAfee/move/etc/optpolicy.xml and verify that the quarantine details are updated.</td>
</tr>
<tr>
<td></td>
<td>4 Verify that the quarantine path is resolved from the McAfee ePO server and the McAfee MOVE AntiVirus SVM.</td>
</tr>
<tr>
<td></td>
<td>5 Make sure that the user has administrator rights to quarantine the share folder.</td>
</tr>
</tbody>
</table>

**MOVE_ERROR_20002**

<table>
<thead>
<tr>
<th>Error string:</th>
<th>[MOVE_ERROR_20002] Mounting &lt;name of the network mount&gt; failed, error(&lt;system error code&gt;): &lt;system error message&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cause:</td>
<td>Quarantine details might not be configured properly.</td>
</tr>
<tr>
<td>Workaround:</td>
<td>1 Verify that quarantine details are configured in the Options policy in McAfee ePO.</td>
</tr>
<tr>
<td></td>
<td>2 Run the policy collector and send an wake-up agent call to the target SVM.</td>
</tr>
<tr>
<td></td>
<td>3 From the SVM, open /opt/McAfee/move/etc/optpolicy.xml and verify that the quarantine details are updated.</td>
</tr>
<tr>
<td></td>
<td>4 Verify that the quarantine path is resolved from the McAfee ePO server and the McAfee MOVE AntiVirus SVM.</td>
</tr>
<tr>
<td></td>
<td>5 Make sure that the user has administrator rights to quarantine the share folder.</td>
</tr>
</tbody>
</table>

**MOVE_ERROR_20003**

<table>
<thead>
<tr>
<th>Error string:</th>
<th>[MOVE_ERROR_20003] Mounting [name of the local storage mode] failed, error((&lt;system error code&gt;)): &lt;system error message&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cause:</td>
<td>Quarantine details might not be configured properly.</td>
</tr>
<tr>
<td>Workaround:</td>
<td>1 Verify that quarantine details are configured in the Options policy in McAfee ePO.</td>
</tr>
<tr>
<td></td>
<td>2 Run the policy collector and send an wake-up agent call to the target SVM.</td>
</tr>
<tr>
<td></td>
<td>3 From the SVM, open /opt/McAfee/move/etc/optpolicy.xml and verify that the quarantine details are updated.</td>
</tr>
<tr>
<td></td>
<td>4 Verify that the quarantine path is resolved from the McAfee ePO server and the McAfee MOVE AntiVirus SVM.</td>
</tr>
<tr>
<td></td>
<td>5 Make sure that the user has administrator rights to quarantine the share folder.</td>
</tr>
</tbody>
</table>
MOVE_ERROR_20004

Error string: [MOVE_ERROR_20004] Detected malware <name of the malware>, quarantaine failed hence file is not deleted, file has been DENIED ACCESS, VMID: <ID of the VM> filename: <name of the file>

Cause: Quarantine details might not be configured properly.

Workaround:
1. Verify that quarantine details are configured in the Options policy in McAfee ePO.
2. Run the policy collector and send an wake-up agent call to the target SVM.
3. From the SVM, open /opt/McAfee/move/etc/optpolicy.xml and verify that the quarantine details are updated.
4. Verify that the quarantine path is resolved from the McAfee ePO server and the McAfee MOVE AntiVirus SVM.
5. Make sure that the user has administrator rights to quarantine the share folder.

MOVE_ERROR_20005

Error string:
[MOVE_ERROR_20005] hyper_register unable to contact the hypervisor <name of the exception> Please verify the hypervisor information supplied in the SVA policy on ePO or
[MOVE_ERROR_20005] hyper_register unable to contact the hypervisor <name of the exception> due to invalid credentials. Please verify the hypervisor information supplied in the SVA policy on ePO or
[MOVE_ERROR_20005] hyper_register unable to contact the hypervisor <name of the exception> due to invalid hypervisor URL. Please verify the hypervisor information supplied in the SVA policy on ePO

Cause: vCenter or hypervisor details might not be configured properly.

Workaround:
1. Verify that the vCenter or hypervisor details are configured in the SVM Settings policy in McAfee ePO.
2. Run the policy collector and send an wake-up agent call to the target SVM.
3. From the SVM, open /opt/McAfee/move/etc/svapolicy.xml and verify that the vCenter or hypervisor details are updated.

MOVE_ERROR_20006

Error string: [MOVE_ERROR_20006] hyper_register unable to contact the hypervisor due to timeout <name of the exception> Please verify the hypervisor information supplied in the SVA policy on ePO and retry

Cause: vCenter or hypervisor details might not be configured properly.

Workaround:
1. Verify that the vCenter or hypervisor details are configured in the SVM Settings policy in McAfee ePO.
2. Run the policy collector and send an wake-up agent call to the target SVM.
3. From the SVM, open /opt/McAfee/move/etc/svapolicy.xml and verify that the vCenter or hypervisor details are updated.
4. Verify that you are able to log on to the vCenter or hypervisor.
5. Verify that the vCenter or hypervisor is up and running.
Frequently asked questions

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

How can I convert the SVM Manager format to Microsoft Hyper-V format?

Convert the .vmdk file format to .vhdx file to deploy the SVM Manager to Microsoft Hyper-V. Attach the converted file as a hard disk to create a new virtual machine.

1. Download and install Microsoft Virtual Machine Converter 3.0 (MVMC 3.0).

   The SVM Manager can only be converted using the Microsoft Virtual Machine Converter 3.0 command line Windows PowerShell scripts.

2. Click Start | All Programs | Accessories, right-click Windows PowerShell, then click Run as administrator.

3. In the PowerShell console, run this command:
   
   ```
   Import-Module "C:\Program Files\Microsoft Virtual Machine Converter\MvmcCmdlet.psd1"
   ```

4. For .vhd format image, run this command:

   ```
   ConvertTo-VirtualHardDisk -SourceLiteralPath "C:\VMDKs\SVM_Manager_3.x-disk1.vmdk"
   ```

5. For .vhdx format image, run this command:

   ```
   ConvertTo-VirtualHardDisk -SourceLiteralPath "C:\VMDKs\SVM_Manager_3.x-disk1.vmdk" -DestinationLiteralPath "C:\VHDs" -VhdType FixedHardDisk -VhdFormat Vhd
   ```

6. After you convert the file format to .vhd or .vhdx, mount the disk image to the Microsoft Server 2012 R2 Hyper-V system:

   a. On the Server 2012 R2 Hyper-V Manager, click New | Virtual Machine, then click Next.

      Specify these VM details in the wizard, then click Next.

      | Option       | Definition                          |
      |--------------|-------------------------------------|
      | VM Name      | Specify the VM name of the instance. |
      | Memory Size  | Set the memory size of the VM.       |
      | Network Interface | Specify the details about the network interface associated to the instance. |

   b. Select Use and existing virtual hard disk, specify the path to the .vhdx or .vhd file, then click Next.

   c. Click Finish, then turn on the SVM manager.

The McAfee MOVE AntiVirus detection pop-up message does not appear on the Windows desktop. How do I fix this?

Method 1:

Enable the McAfee Agent policy option, Show the McAfee system tray icon (Windows only), to display McAfee MOVE AntiVirus detection pop-up message on the Windows desktop.

1. Log on to McAfee ePO as an administrator.

2. Select Menu | Policy | Policy Catalog.

3. From the Product drop-down list, select McAfee Agent.

4. From the Category drop-down list, select General.

5. Click New Policy.
6 On the New Policy page, configure the policy settings, then click OK.

7 Open the newly created policy.

8 Enable Show the McAfee system tray icon (Windows only) from General Options on the General tab.

9 Click Save, then apply the policy to the clients.

**Method 2 (Multi-Platform only):**

If you need the Multi-Platform Threat Event pop-up alerts through the Remote Desktop Protocol (RDP) session, run UPDATERUI.EXE manually.

Perform these steps inside your remote session.

1 Click Start | Run.

2 Run this command: "C:\Program Files\McAfee\Common Framework\CmdAgent.exe" /s

   The McAfee Agent icon now appears in the toolbar, and the OAS Statistics can be viewed in the remote session.

**How can I create an on-demand scan task for a vSphere VM with Agentless?**

1 Check in the McAfee MOVE AntiVirus Meta Package extension to McAfee ePO and create a Registered Cloud Account for vSphere.

2 Click System Tree. You see the vSphere group that was previously added and all client computers under that vSphere group entry.

3 Select an unmanaged computer where you want to trigger the on-demand scan:
   a Click Actions | Agent | Modify Policies on a Single System.
   b From the Product drop-down list, select MOVE AntiVirus 4.6.0.
   c From the Category drop-down list, select On Demand Scan.
   d Click New Policy.
   e On the New Policy page, configure the policy settings, then click OK.
   f Open the newly created policy, select Enable on-demand scan, then click Save.

4 Select the SVM that is managing that client VM and issue wake-up agent call.

   The on-demand scan starts at the next available slot.

   The Policy Collector task collects the unmanaged system policies and adds them to the SVM policy for the next policy enforcement.

**What can I do if I see the warning message "Failed to get process info of (system)", which is recorded in the Multi-Platform client mvagent.log?**

This is expected behavior. This informational message can be ignored.

In some environments, you might see these warning messages in the mvagent.log, which is the scan log generated by the McAfee MOVE AntiVirus (Multi-Platform) client on protected systems:
How can I manually check the DAT version installed on the McAfee MOVE AntiVirus SVM in an Agentless environment?

Check which DAT version is installed on the McAfee MOVE AntiVirus SVM using the Linux command line interface (CLI).

**Method 1:**

1. Log on to the McAfee MOVE AntiVirus SVM.
2. At the command prompt, run this command: `sudo`
3. When prompted, provide valid credentials.
4. Run this command to display the SVM details: `/opt/isec/ens/threatprevention/bin/isecav -v`
   
   **For example:**
   
   McAfee Endpoint Security for Linux Threat Prevention Version : 10.2.0.717
   
   HF Version : 1177340
   
   License : Full
   
   DAT Version : 8479.0
   
   Engine Version : 5900.7806

**Method 2:**

1. Log on to the McAfee MOVE AntiVirus SVM.
2. At the command prompt, run this command: `sudo /opt/McAfee/move/bin/sva-config -v`
3. When prompted, provide valid credentials.

   **The required details appear in the command window.**

Why is the DNS suffix missing on the SVM after successful deployment using a Static IP Pool configured with a DNS suffix?

If you are using Static IP Pool address, make sure that the NSX Manager has the ePO IP or FQDN details.

1. Log on to vCenter as an administrator.
2. Click **Networking and security** | **Service definition**.
3. Double-click **McAfee MOVE AV**.
4. On the **Manage** tab, click **Deployment**.

   **Under OVF URL, make sure that the ePO IP or FQDN have been provided and not just the McAfee ePO server host name.**
What do I do if an upgrade to McAfee MOVE AntiVirus (Agentless) 4.6.0 fails?

Perform these steps to successfully upgrade from McAfee MOVE AntiVirus (Agentless) 4.5.1 to McAfee MOVE AntiVirus 4.6.0.

1. Install the McAfee MOVE AntiVirus 4.6.0 Meta Package extension on the McAfee ePO server.
2. Check in the SVM 4.5.1.
3. Upgrade the McAfee MOVE AntiVirus Service.

How can I fix any filesystem error that appears after deploying Agentless?

2. Deploy the Agentless OVF template. For details, see Agentless installation and configuration in the McAfee MOVE AntiVirus 4.6.0 Installation Guide.

What do I do if Agentless SVM shows as unmanaged when registering with the McAfee ePO server?

Make sure that the copy of the Agentless OVF package is from a known good source, preferably the McAfee download site, then do a fresh deployment.

Perform these steps only if the SVM shows as Unmanaged in the McAfee ePO System Tree.

1. Delete the system from McAfee ePO.
   When prompted, do not choose to remove the McAfee Agent.
2. For the existing SVM, from the local command line interface, run the registration script with this command: sudo /opt/McAfee/move/bin/svm-config
3. When prompted, click Yes to unregister with the vShield Manager.
4. Complete the procedure to unregister the product.
5. Turn off the SVM and delete it from the disk.
6. Continue with the new deployment.

Agentless configuration fails and displays failed status on the McAfee ePO for the vCenter account. How do I fix this?

There are two causes for the status to show Configuration Failed:

- If the vShield Manager is not registered with vCenter under Registered Cloud Accounts, then the vCenter appears as Not Configured on the McAfee ePO console under McAfee MOVE AntiVirus (Agentless).
- If the vShield Manager was first successfully registered with vCenter, but later removed from the Registered Cloud Accounts, it might can not synchronize the vCenter account successfully, resulting in Not Configured being displayed on the McAfee ePO console under McAfee MOVE AntiVirus (Agentless).

Register or reregister the vCenter account under Registered Cloud Accounts.

1. Log on to McAfee ePO as an administrator.
2. Select Menu | configuration | Registered Cloud Accounts to open the Registered Cloud Account page.
3. Select the vCenter Account and click Delete.
4. Restart the ePO Event Parser Service.
5 Select Menu | Registered Cloud Accounts, and confirm that the specific vCenter account is now deleted.

6 On the Registered Cloud Account page, click Actions, then select Add Cloud Account.

7 Type the vCenter Account Details on the Registered Cloud Accounts page, then click Test Connection.

8 If Test Connection is successful, click Next, then accept the certificate.

9 Click Finish, then click OK.

10 Check the configuration status of the vCenter Account, and now it shows as Configured.

The McAfee ePO server now creates a task that will synchronizes the vCenter according to the above configuration.

**How do I keep disabled Windows Defender on Windows 10 system after installing Multi-Platform?**

1 Log on to the system as an administrator.

2 Click Start | Run.

3 Run these commands one after the other:
   - `sc stop mvagtsvc`
   - `sc start mvagtsvc`

4 Close the command prompt window.

**How do I avoid loss of network connectivity on virtual machines that use VMXNet3 NICs when deploying Agentless through McAfee ePO?**

**Method 1:**

Make sure that the version of VMware Tools installed on the virtual machine is the exact same build as the VMware Tools version supplied by the host. When the script is invoked and the builds match, only the needed Guest Introspect (vShield components) are installed.

**Method 2:**

Make sure that the virtual machines also have their e1000 NICs installed, to maintain network functionality when the script is invoked remotely.

**How do I delete the IP pool when an IP address is already in use?**

Run this SQL query to remove the IP Pool details from the McAfee ePO database:

```sql
DELETE FROM [DC_AL_CONFIG_IPPOOL] WHERE IPPOOL_NAME='<POOL_NAME>'
```

**What do I do when the error “Critical error. Downloading ePO init files failed” appears when deploying SVM through McAfee ePO using an IP Pool?**

When you deploy the SVM through McAfee ePO using an IP Pool on the VMware ESX host, you might can see these errors in the SVM console session:

- ERROR [MOVEAL:pool-1-thread-1] svm.SvmEpoRegistrationTaskImpl - ePO Registration failed for SVM with vm name: and for the Hypervisor: HyperVisor_Name
When you see these errors, make sure that the prefix length is correct for the IP Pool according to the characteristics of the destination network.

**What is the error return code description for McAfee MOVE AntiVirus (Agentless) SVM registration with the vShield Manager?**

When McAfee MOVE AntiVirus (Agentless) SVM registration fails, vShield Manager provides a **Return Code** error.

<table>
<thead>
<tr>
<th>Return Code</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>OK operation successful.</td>
</tr>
<tr>
<td>201</td>
<td>Created: Entity successfully altered.</td>
</tr>
<tr>
<td>400</td>
<td>Bad Request: Internal error codes. Please refer to the Error Schema for more details.</td>
</tr>
<tr>
<td>401</td>
<td>Unauthorized: Incorrect user name or password.</td>
</tr>
<tr>
<td>600</td>
<td>Unrecognized vendor ID.</td>
</tr>
<tr>
<td>601</td>
<td>Vendor is already registered.</td>
</tr>
<tr>
<td>602</td>
<td>Unrecognized altitude.</td>
</tr>
<tr>
<td>603</td>
<td>Solution is already registered.</td>
</tr>
<tr>
<td>604</td>
<td>Invalid IPv4 address.</td>
</tr>
<tr>
<td>605</td>
<td>Invalid port.</td>
</tr>
<tr>
<td>606</td>
<td>Port out of range.</td>
</tr>
<tr>
<td>607</td>
<td>Unrecognized moid (Managed Object Reference ID).</td>
</tr>
<tr>
<td>608</td>
<td>Location information is already set.</td>
</tr>
<tr>
<td>609</td>
<td>Location not set.</td>
</tr>
<tr>
<td>610</td>
<td>Insufficient rights.</td>
</tr>
<tr>
<td>612</td>
<td>Solutions still registered.</td>
</tr>
<tr>
<td>613</td>
<td>Solution location information still set.</td>
</tr>
<tr>
<td>614</td>
<td>Solution still activated.</td>
</tr>
<tr>
<td>615</td>
<td>Solution not activated.</td>
</tr>
<tr>
<td>616</td>
<td>Solution is already activated.</td>
</tr>
<tr>
<td>617</td>
<td>IP: Port already in use.</td>
</tr>
<tr>
<td>618</td>
<td>Bad solution ID.</td>
</tr>
<tr>
<td>619</td>
<td>vShield Endpoint is not licensed.</td>
</tr>
<tr>
<td>620</td>
<td>Internal error.</td>
</tr>
</tbody>
</table>

**I am using McAfee MOVE AntiVirus (Agentless) in an NSX environment. Where do I find the original name of the host name where the infection occurred instead of IP of McAfee MOVE AntiVirus SVM?**

The Threat Event Log displays the host name of the system where the infection occurred.

1. Log on to McAfee ePO as an administrator.
2. Select **Menu | Reporting | Threat Event Log**.
I am using McAfee MOVE AntiVirus (Agentless) in an NSX environment. For some reason, McAfee MOVE AntiVirus SVM is doing nothing. How do I redeploy the McAfee MOVE AntiVirus SVM?

1. Turn off the McAfee MOVE AntiVirus SVM.
2. Delete the McAfee MOVE AntiVirus SVM.
   The NSX Manager now redeploys the McAfee MOVE AntiVirus SVM.

What do I do when error "Internal error on the server" appears when trying to delete a Registered Cloud Account?

This error occurs if you select Delete Tags, and one or more systems that do not belong to that cloud account erroneously have the same tag assigned.

**Method 1:**
1. From the Delete Account dialog box, deselect Delete Tags, and then click OK to delete the registered cloud account.

**Method 2:**
1. Identify one or more systems that do not belong to the registered cloud account but have the same tag assigned.
2. Remove the tag from the systems you identified.
3. Delete the registered cloud account.
Index

A
about
  McAfee MOVE AntiVirus 5
Agentless
  components 8
error codes 65
  features 6
troubleshooting 65

C
client notification
  deferred scan 38
client task 14
  quarantine 47
  scan diagnosis 38, 41
  targeted ODS 36
components
  defined 7, 8
  overview 7, 8
configuration
  deferred scan 37
  exclusions 20
  on-access scan 28
  on-demand 31
  permission sets 19
  quarantine manager 47
  quarantine settings 48
  targeted on-demand scan 35

D
dashboard
  McAfee MOVE AntiVirus 59
  MOVE AntiVirus queries 60
default queries, displaying 60
defferred scan
  client notification 38
  configuring 37
deployment
  agentless 5, 7, 9
  method 9
  methods 5, 7
  multi-platform 5, 7
details
  protection 53
detection
  finding threats 11
  on-access scan 46
  on-demand scan 46
  responding 45
  unwanted program 45
diagnostic tool
  running 39

E
error codes
  Agentless 65
  Multi-Platform 65
  troubleshooting 65
events
  MOVE AntiVirus 53
  exclusions
    configuring 20

F
features
  McAfee MOVE AntiVirus (Agentless) 6
  McAfee MOVE AntiVirus (Multi-Platform) 6
file protection 51

I
integration
  TIE 54

L
logging
  McAfee MOVE AntiVirus 20
  logging and events
    on-demand scan 34
management
  diagnostic tool 39
  quarantine 48
queries (continued)
  MOVE AntiVirus queries 60
  pie charts 60
  viewing default queries 60
  queries, MOVE AntiVirus Agentless predefined 63

R
  registry protection 51
  reports
    supplied queries 60
  response
    handling threats 11
    MOVE AntiVirus 53

S
  scan diagnosis
    configuring 38, 41
  scan items
    excluding 20
  scan type
    on-access 26
  scanning
    on-access 11, 24, 26, 28, 46
    on-demand 11, 24, 46
  scanning option
    configuring 25
    on-access 7
    on-demand 7
  scanning, deferred 37
  security, strategy 11
  self-protection
    McAfee MOVE AntiVirus 19
  service protection 51
  status, displaying 60
  SVM
    configuring 9
    self-protection 51
    view details 60
  SVM Manager
    about 9

T
  targeted on-demand scan
    Agentless 36
    configuring 35
    Multi-Platform 36
  threat prevention
    scanning 11
  TIE
    integrating 54
  troubleshooting
    Agentless 65
troubleshooting (continued)
  error codes 65
  Multi-Platform 65

V

virtual machines
  protecting 9

VM-based scan
  policies 16, 17