Product Guide

McAfee Management for Optimized Virtual Environments AntiVirus 4.5.0

For use with McAfee ePolicy Orchestrator
COPYRIGHT
© 2016 Intel Corporation

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

LICENSE INFORMATION

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

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

1 Product overview 9
What is McAfee MOVE AntiVirus? ....................... 9
  Multi-Platform deployment .................................. 9
  Agentless deployment .................................. 10
Key features .................................... 10
Multi-Platform components .............................. 11
Agentless components .................................. 12
How it works ................................... 13
  The role of the McAfee MOVE AntiVirus SVM (Multi-Platform) ......... 13
  The role of the McAfee MOVE AntiVirus SVM (Agentless) ............... 13
  The role of the SVM Manager (Multi-Platform) ............................ 13
  The role of the security management platforms ........................... 13

2 Configuring McAfee MOVE AntiVirus 15
The importance of creating a security strategy .................. 15
McAfee ePO features leveraged by McAfee MOVE AntiVirus ................. 16
  About the McAfee ePO System Tree .............................. 17
  Using client tasks with McAfee MOVE AntiVirus ................... 18
Automated installation and deployment ......................... 19
Using policies in McAfee ePO .................................. 19
  Create a policy ................................ 20
  Assign a policy ................................ 20
  How the policies assignment works (Agentless) .................. 21
  Configuring policies ................................ 22
  Configuring permissions sets ................................ 22
  Using permission sets ................................ 22
  Configure permission sets ................................ 23
Configuring common settings for Multi-Platform ................. 23
  Protect McAfee MOVE AntiVirus resources .................................. 23
  Configure logging settings .................................. 24
  Configuring exclusions .................................. 24
Scanning for threats on client computers ....................... 26
  Types of scans ................................ 26
  How McAfee GTI works ................................ 26
  Excluding items from scans .................................. 26
  Configure common scan settings .................................. 27
  On-access scanning .................................. 28
  On-demand scanning .................................. 32
  Configure deferred scan settings (Multi-Platform only) .......... 39
version ................................... 76

7  Frequently asked questions ........................................... 77

Index ........................................................................ 85
Preface

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

Contents

- About this guide
- Find product documentation

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.
- **Users** — People who use the computer where the software is running and can access some or all of its features.

Conventions

This guide uses these typographical conventions and icons.

- *Italic* — Title of a book, chapter, or topic; a new term; emphasis
- **Bold** — Text that is emphasized
- **Monospace** — Commands and other text that the user types; a code sample; a displayed message
- **Narrow Bold** — Words from the product interface like options, menus, buttons, and dialog boxes
- Hypertext blue — A link to a topic or to an external website

**Note:** Extra information to emphasize a point, remind the reader of something, or provide an alternative method

**Tip:** Best practice information

**Caution:** Important advice to protect your computer system, software installation, network, business, or data

**Warning:** Critical advice to prevent bodily harm when using a hardware product
Find product documentation

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

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

Contents
- What is McAfee MOVE AntiVirus?
- Key features
- Multi-Platform components
- Agentless components
- How it works

What is McAfee MOVE AntiVirus?
McAfee MOVE AntiVirus provides anti-virus protection for virtual environments, without having to install anti-virus software on every virtual machine.

The software provides the protection and performance needed for your organization.

Once installed, McAfee MOVE AntiVirus immediately begins protecting your systems from malware.

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
The Multi-Platform is an agent-based deployment option. It 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.

The Multi-Platform deployment option:
- 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 take the required actions.
- Uses McAfee ePO to manage the McAfee MOVE AntiVirus configuration on client systems, McAfee MOVE AntiVirus SVM, and SVM Manager.
• Uses 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 the 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.

The Agentless deployment option:

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

• Relies on McAfee® VirusScan® Enterprise for Linux for 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.

Key features

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>McAfee Data Center 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>NA</td>
</tr>
</tbody>
</table>
## 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.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Multi-Platform</th>
<th>Agentless</th>
</tr>
</thead>
<tbody>
<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>NA</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>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>NA</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>NA</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>NA</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 as soon as the hypervisor is added to the cluster.</td>
<td>NA</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>NA</td>
<td>Yes</td>
</tr>
<tr>
<td>Endpoint Scan and Security reports</td>
<td>With the Cloud Workload Discovery software, quickly retrieve Endpoint Scan Report and Endpoint Security Report of all registered endpoints.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
**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 Common 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.

**McAfee MOVE AntiVirus extension** — The product extension that 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.

**Cloud Workload Discovery** — A Data Center discovery software that integrates the management and automation feature of McAfee ePO to discover and manage your guest VMs.

---

### 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. VirusScan Enterprise for Linux, 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.

How it 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.

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. VirusScan Enterprise for Linux, 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 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
- Automated installation and deployment
- Using policies in McAfee ePO
- Configuring permissions sets
- Configuring common settings for Multi-Platform
- 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.

Prevention — 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 and files, 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

- **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 these results to exclude them from being scanned.
Detection — 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 and initiate the on-demand scan on the target system.

Response — 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.

Tuning — 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

<table>
<thead>
<tr>
<th>McAfee ePO feature</th>
<th>McAfee MOVE AntiVirus</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queries and reports</td>
<td>Adds:</td>
</tr>
<tr>
<td></td>
<td>• Predefined queries to the Query list.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Predefined Result Types and Properties for creating and narrowing the scope of</td>
</tr>
<tr>
<td></td>
<td>custom queries.</td>
</tr>
<tr>
<td>Server tasks</td>
<td>Adds predefined server tasks to the Server Tasks list in Automation.</td>
</tr>
<tr>
<td>Threat Event Log</td>
<td>Adds McAfee MOVE AntiVirus events that you can filter and view.</td>
</tr>
</tbody>
</table>

### 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 4.5.0</td>
<td>Includes policy setting to prevent McAfee MOVE AntiVirus service and files, 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></td>
<td>MOVE AntiVirus 4.5.0</td>
</tr>
<tr>
<td></td>
<td>MOVE AntiVirus 4.5.0</td>
<td>Options</td>
</tr>
<tr>
<td></td>
<td>MOVE AntiVirus 4.5.0</td>
<td>On Access Scan</td>
</tr>
<tr>
<td></td>
<td>MOVE AntiVirus 4.5.0</td>
<td>On Demand Scan</td>
</tr>
<tr>
<td></td>
<td>MOVE AntiVirus 4.5.0</td>
<td>Shared Cloud Solutions (Multi-Platform only)</td>
</tr>
<tr>
<td></td>
<td>MOVE AntiVirus 4.5.0</td>
<td>SVM Manager Settings (Multi-Platform only)</td>
</tr>
<tr>
<td></td>
<td>MOVE AntiVirus 4.5.0</td>
<td>SVM Settings</td>
</tr>
<tr>
<td>Client Tasks</td>
<td>Restore from Quarantine</td>
<td>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.</td>
</tr>
<tr>
<td>(Multi-Platform)</td>
<td>Targeted On-Demand Scan</td>
<td>Optimizes file scanning for files where the previous scanning is timed out for reasons such as large file size, file structure, and file composition.</td>
</tr>
<tr>
<td>Function</td>
<td>Category</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Scan Diagnostics</strong></td>
<td><strong>Category</strong></td>
<td>Run the scan diagnostic task to easily find frequently scanned files, 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.</td>
</tr>
<tr>
<td><strong>Client Tasks</strong></td>
<td><strong>Scan Diagnostics</strong></td>
<td>Run the scan diagnostic task to easily find frequently scanned files, 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.</td>
</tr>
<tr>
<td><strong>Targeted ODS</strong></td>
<td><strong>Targeted On-Demand Scan</strong></td>
<td>Optimizes file scanning for files where the previous scanning is timed out for reasons such as large file size, file structure, and file composition.</td>
</tr>
</tbody>
</table>

### 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 scan diagnosis, 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.

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client Tasks</strong></td>
<td><strong>Restore from Quarantine</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Targeted On-Demand Scan</strong></td>
<td><strong>Scan Diagnostics</strong></td>
<td>Optimizes file scanning for files where the previous scanning is timed out for reasons such as large file size, file structure, and file composition.</td>
</tr>
<tr>
<td><strong>Scan Diagnostics</strong></td>
<td><strong>Category</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Client Tasks</strong></td>
<td><strong>Scan Diagnostics</strong></td>
<td>Run the scan diagnostic task to easily find frequently scanned files, 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.</td>
</tr>
</tbody>
</table>

For information about creating and using client tasks and the Client Task Catalog, see the McAfee ePO documentation.
Automated installation and deployment

Having multiple installation and deployment methods ensures that you can select the level of automation or customization that best suits your environment.

- **Automated wizards** — Install and deploy the product with preconfigured, default settings and minimal interaction during installation.

- **McAfee MOVE AntiVirus SVM autoscaling** — The security administrator can define the number of backup SVMs that are ready to protect your client systems. Calculate the number of ready SVMs required for the maximum number of clients that need protection at any time of the day. The standby SVMs are automatically deployed based on the backup SVM value. For example, if you specify the backup SVM as 4, two standby SVMs are deployed automatically. Therefore, the McAfee MOVE AntiVirus SVMs automatically scale up and down depending on the number of endpoints connected.

- **SVM Manager** — Automatically assigns McAfee MOVE AntiVirus SVM to (Multi-Platform) clients based on configurable parameters like scan server load, McAfee ePO tags, and IP address ranges. This is applicable to Multi-Platform only.

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 |
|-----------------------------|---------------------------------------------|
| **Category**               | **Description**                             |
| Options                    | 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. |
| On Access Scan             | Examines files on the computer as the user accesses them, and provides continuous, real-time detection of threats. |
| On Demand Scan             | Configures the on-demand scan settings for the preconfigured scans that run on the SVM. |
| Share Cloud Solutions      | Enables you to specify that files and certificates with specific reputations are allowed to perform certain scan actions, as specified by scan rules. |
| (Multi-Platform only)      |                                             |
| SVM Manager Settings       | Configures the SVM Manager and autoscale settings required for SVM deployment and management. |
| (Multi-Platform only)      |                                             |
| SVM Settings               | Specifies settings that apply to SVM configuration, scanning options, on-demand scan configurations required for SVM, and scan performance. |

| Table 2-2  McAfee MOVE AntiVirus Common categories |
|-----------------------------|---------------------------------------------|
| **Category**               | **Description**                             |
| Options                    | Allows you to configure the settings to defend files, services, and registry keys on virtual machines and to log events and alerts. |
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**

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

1. Log on to McAfee ePO as an administrator.
2. Select **Menu | Policy | Policy Catalog**, then select **MOVE AntiVirus 4.5.0** or **MOVE AntiVirus Common 4.5.0** from the drop-down lists.
3. Select **Menu | Policy | Policy Catalog**, then click **New Policy**.
4. On the **New Policy** page, configure the policy settings, then click **OK**.
5. On the **General** tab of the **Policy Settings** page for the new policy, configure the settings to control basic behavior.
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**

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

1. Log on to McAfee ePO as an administrator.
2. In the System Tree, 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 4.5.0 or MOVE AntiVirus Common 4.5.0.

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 an agent wake-up 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 an agent wake-up call from McAfee ePO.

**How the policies assignment works (Agentless)**

VM-based scan configuration is enabled by default. With the VM-based scan configuration, 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.

**Run policy collector (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 within the default policy collection interval, which is 60 minutes.

![Best practice: We recommend that you specify the policy collection interval depending on your environment so that the policies and updates are not enforced to SVM in short period.]

**Task**

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

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 on successful collection of the policies.

   ![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 by navigating to Menu | Automation | Server Task Log.]

3 Send an agent wake-up 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 on 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 McAfee MOVE AntiVirus deployment option, because no permissions are granted by default.

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 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>
<tr>
<td>Server tasks</td>
<td>Server tasks</td>
</tr>
<tr>
<td>System Tree</td>
<td>Systems, System Tree access</td>
</tr>
<tr>
<td>Threat Event Log</td>
<td>Systems, System Tree access, Threat Event Log</td>
</tr>
</tbody>
</table>

**Configure permission sets**

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

**Task**

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

1. Log on to McAfee ePO as an administrator.
2. Select Menu | 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.
6. Click Save.

**Configuring common settings for Multi-Platform**

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

These settings include Self-Protection, logging, and events details for Multi-Platform.

**Protect McAfee MOVE AntiVirus resources**

One of the first things that malware attempts to do during an attack is to disable your system security software. Configure Self-Protection in the Options policy under MOVE AntiVirus Common 4.5.0 to prevent McAfee MOVE AntiVirus services and files, registries from being stopped or modified.
**Task**
For details about product features, usage, and best practices, click ? or Help.

1. Log on to McAfee ePO as an administrator.
2. Select Menu | Policy | Policy Catalog, then select MOVE AntiVirus Common 4.5.0 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 4.5.0 to retrieve the software deployment and configuration details.

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

1. Log on to McAfee ePO as an administrator.
2. Select Menu | Policy | Policy Catalog, then select MOVE AntiVirus Common 4.5.0 from the Product list.
3. From the Category list, select Options.
4. Click the name of an editable policy.
5. Configure Logging and Events settings on the page.
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.

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.

**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>
</table>
| ?                  | Question mark | Single character  
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 orWWWW. |
| *                  | Asterisk  | Multiple characters, except backslash (\).                                |
| **                 | Double asterisk | Zero or more of any characters, including backslash (\).  
This wildcard matches zero or more characters. For example: C: \ABC\**\XYZ matches C: \ABC\DEF\XYZ and C: \ABC\XYZ |

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

**Root-level exclusions**

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

**System variables**

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>
</tbody>
</table>
### Scanning for threats on client computers

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

#### Types of scans

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. Whenever 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 the next DAT release, when McAfee Labs publishes the update.

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 positive results. The McAfee GTI sensitivity level is set to **Medium** by default. Configure the sensitivity level for each scanner in the SVM Settings policy.

#### Excluding items from scans

McAfee MOVE AntiVirus scanners enable you to fine-tune the list of scanned items by specifying items to exclude.

For example, you might need to exclude some file types to prevent a scanner from locking a file used by a key application, database, or server. A locked file can cause the database or server to fail or generate errors.

---

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

### Configure common scan settings

To specify settings that apply to both on-access and on-demand scans, configure the MOVE AntiVirus 4.5.0 | Options policy settings.

The common scan setting under MOVE AntiVirus 4.5.0 | Options 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.

- **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

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

1. Log on to McAfee ePO as an administrator.
2. Select Menu | Policy | Policy Catalog, then select MOVE AntiVirus 4.5.0 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, 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, then the access is allowed.
3. If exclusion is not defined, the scanner checks whether the file is present in local cache in the client system. If it is present, then access is allowed.
4. If the file is not present in local cache in the client system, the scanner checks for publisher trust in the client system. If publisher trust matches, then 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, then 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.
   a. If the file is clean, the result is cached and the read, write, or rename operation is granted. McAfee MOVE AntiVirus cashes the result in the SVM and the client system.
   b. 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 thru 4 of *How on-access scanning works*.
2. If the publisher trust does not match:
   a. The client looks for the reputation in global cache in the SVM. If the reputation is available, then the access is allowed based on the Shared Cloud Solutions policy assigned to the system.
   b. If the reputation is not available in global cache in the SVM, the client sends the file hashes to the SVM for TIE lookup.
   c. 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.
   d. (With SVM is connected to TIE) If the file hash is not found in the SVM cache and TIE server does not have the reputation:
      a. (Advanced Threat Defense is present) If the policy on the endpoint determines that the file has to 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 meet:
         - Advanced Threat Defense (ATD) option is configured under Shared Cloud Solutions policy on the McAfee ePO server.
         - Size of the file is less than 10 MB
      b. The TIE server returns the file hash's reputation to the SVM once the data is received from Advanced Threat Defense after analysing the file.
3. The 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 scans 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

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

1. Log on to McAfee ePO as an administrator.
2. Select Menu | Policy | Policy Catalog, then select MOVE AntiVirus 4.5.0 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.
### For this... Do this...

<table>
<thead>
<tr>
<th>Scan</th>
<th>Select any combination of:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• When writing to disk</td>
<td></td>
</tr>
<tr>
<td>• When reading from disk</td>
<td></td>
</tr>
<tr>
<td>• On network drives</td>
<td></td>
</tr>
<tr>
<td>• Opened for backup (Multi-Platform only)</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>File types to scan</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>• All files — Select to scan all files.</td>
<td></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. By default, this option is selected.</td>
<td></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>
<td></td>
</tr>
</tbody>
</table>

![Archive and MIME-encoded files are not scanned by default. This behavior is changed by modifying the SVM Settings policy.]

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>Path Exclusions</th>
<th>Add them to the Path Exclusions and Process Exclusions lists.</th>
</tr>
</thead>
<tbody>
<tr>
<td>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:</td>
<td></td>
</tr>
<tr>
<td>• Wildcards are supported.</td>
<td></td>
</tr>
<tr>
<td>• (Multi-Platform only) Windows system variables are supported, see System variables for the list of supported system variables.</td>
<td></td>
</tr>
</tbody>
</table>

![)(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.

| Publisher Exclusions | 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. Here are the portable executable extensions that are excluded with this option: .cpl, .exe, .dll, .ocx, .sys, .scr, .drv, .efi, .fon | |

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

**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. Examine the file at the client system.

2. Checks if any exclusion is defined in the policy. If any exclusion is defined for the file, then the access is allowed.

3. If exclusion is not defined, the scanner checks whether the file is present in local cache in the client system. If it is present, then access is allowed.

4. If the file is not present in local cache in the client system, the scanner checks for publisher trust in the client system. If publisher trust matches, then 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, then 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 cashes 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 to clean the file, the scanner:

- Uses information in the currently loaded DAT files to clean the file.
- 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 thru 4 of *How on-demand scanning works*.

2 If the publisher trust does not match:
   a The client looks for the reputation in global cache in the SVM. If the reputation is available, then the access is allowed based on the **Shared Cloud Solutions** policy assigned to the system.
   b If the reputation is not available in global cache in the SVM, the client sends the file hashes to the SVM for TIE lookup.
   c 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.
   d (With SVM is connected to TIE) If the file hash is not found in the SVM cache and TIE server does not have the reputation:
      a (Advanced Threat Defense is present) If the policy on the endpoint determines that the file has to 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 meet:
         • **Advanced Threat Defense (ATD)** option is configured under **Shared Cloud Solutions** policy on the McAfee ePO server.
         • Size of the file is less than 10 MB
      b The TIE server returns the file hash's reputation to the SVM once the data is received from Advanced Threat Defense after analysing the file.

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

1. Log on to McAfee ePO as an administrator.
2. Select Menu | Policy | Policy Catalog, then from the Product list select MOVE AntiVirus 4.5.0.
3. From the Category list, select On Demand Scan.
4. Click the name of an editable policy.
5. Configure these settings, then click Save.
<table>
<thead>
<tr>
<th><strong>For this...</strong></th>
<th><strong>Do this...</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable On-demand Scan</td>
<td>Select Enable on-demand scan.</td>
</tr>
<tr>
<td>• Specify maximum time for each file scan ___ seconds</td>
<td>Enter the appropriate amount for your environment. We recommend 45.</td>
</tr>
<tr>
<td>• Run on-demand scan for every ___ days</td>
<td>Enter the appropriate amount for your environment. We recommend 7.</td>
</tr>
<tr>
<td>• On-demand scan will stop after ___ minutes</td>
<td>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)</td>
<td>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>

**File Types to Scan**

| **• All files** | Select to scan all files. By default, this option is selected. |
| **• 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. |
| **• 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. |

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 and Process Exclusions lists.

**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.

(Chapter 3: Configuring McAfee MOVE AntiVirus
Scanning for threats on client computers)
For this...  Do this...

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.

On-demand scan events and log details

McAfee MOVE AntiVirus generates various alerts around on-demand scan. You can view the ODS statuses and event logs in 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 know 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 scan. These alerts can be displayed in any of three 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>
</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>
</tbody>
</table>
**Targeted on-demand scan**

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

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 would start when one of the existing targeted on-demand scans completes.

**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 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 would start when one of the existing targeted on-demand scans completes.

**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**

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

1. Log on to McAfee ePO as an administrator.
2. Select **Menu | Policy | Policy Catalog**, then from the **Product list** select **MOVE AntiVirus 4.5.0**.
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>
</tbody>
</table>

The default value is 1 and increasing this value reduces the performance.

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 under the On Demand Scan policy.
- You configured Restrict number of targeted on-demand scans to____ per SVM under the SVM Settings policy.
- A new ODS does not start if an ODS is currently running on the targeted system.

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

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

2. Select Menu | 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, scheduling page is not available and targeted on-demand scan runs immediately on the targeted system.

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

5. On the Schedule page, schedule the task and 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 under the On Demand Scan policy.
- You configured Restrict number of targeted on-demand scans to____ per SVM under the SVM Settings policy.
- A new ODS does not start if an ODS is already running on the targeted system.
Task
For details about product features, usage, and best practices, click ? or Help.

1 Log on to the McAfee ePO server as an administrator.
2 Select Menu | Policy | Client Task Catalog.
3 From Client Task Types, select MOVE AntiVirus 4.5.0 | 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 scanning 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.

Whenever the previous on-access scanning timed out, the 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
For details about product features, usage, and best practices, click ? or Help.

1 Log on to McAfee ePO as an administrator.
2 Select Menu | Policy | Policy Catalog, select MOVE AntiVirus 4.5.0 from the Product drop-down menu, 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 &lt;=200 MB</td>
<td>480 seconds</td>
</tr>
<tr>
<td>&gt; 200 MB and &lt;=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 scan

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

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

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 scanning 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

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

1. Log on to McAfee ePO as an administrator.
2. Select Menu | Policy | Client Task Catalog.
3. From Client Task Types, select MOVE AntiVirus 4.5.0 | 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**.

<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>Diagnosis Time</td>
<td>Specifies the time period, in minutes, set for calculating the frequently scanned files. For example, 1–10 minutes.</td>
</tr>
</tbody>
</table>

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 4.5.0 [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 scanning 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 calculate the frequently scanned files, run the command:
   ```bash
   >cd /opt/McAfee/move/bin
   sudo ./scan_diagnostic or 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.

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

1. Log on to McAfee ePO as an administrator.
2. Select Menu | Policy | Client Task Catalog.
3. From MOVE AntiVirus 4.5.0 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 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 4.5.0 [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.
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.

```
C:\Users\Administrator>move_diagnose
Usage: Move_Diagnose /T:<time window in minutes> /O:<output file path>
Example: Move_Diagnose /T:5 /O:C:\MyFolderPath

C:\Users\Administrator>move_diagnose /T:1 /O:C:\results
Please wait while we collect and analyze the Frequently Scanned data...

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-D8414F97.pf
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%
text
50%
```

(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
- 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, the 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 clean automatically (the default setting), the resulting action depends on the cleaning instruction from the content file. For example, if the file can't be cleaned, the scanner might either delete the file or take the secondary action, depending on the content file instruction.

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 scan 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.
  To make scanning more efficient, 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.
  To make scanning more efficient, 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 cleans or 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
For details about product features, usage, and best practices, click ? or Help.

1 Log on to McAfee ePO as an administrator.

2 Select Menu | Policy | Policy Catalog, then select MOVE AntiVirus 4.5.0 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>
<tbody>
<tr>
<td>Multi-Platform</td>
<td>Quarantine Directory</td>
<td>Specify where quarantined items are stored by changing the quarantine directory. Mapped network drives and UNC network path names are not supported.</td>
</tr>
<tr>
<td>Agentless</td>
<td>Quarantine network share</td>
<td>Quarantined files are stored on the specified network share. The share is mounted as CIFS, so the remote share must support this protocol. Read and write permissions are required. 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.</td>
</tr>
<tr>
<td></td>
<td>Network domain name</td>
<td>The domain used to access the specified share.</td>
</tr>
<tr>
<td></td>
<td>Network user name</td>
<td>The user name used to access the specified share.</td>
</tr>
<tr>
<td></td>
<td>Network password</td>
<td>The password used to access the specified share.</td>
</tr>
</tbody>
</table>

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

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

2 Select Menu | Policy | Client Task Catalog.

3 From Client Task Types, select MOVE AntiVirus 4.5.0 | 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>
</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 this 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 attempted at the next policy enforcement.

A file is quarantined when:

- The **Quarantine network share** configuration, which is present under the **Options** policy, is mounted.
- A detection occurs.
- **Delete files automatically** 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 under 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.

**Configure the quarantine folder**

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

**Tasks**

- *Set permissions for shared folders on page 51*
  Setting permission for the quarantine folder allows you to specify who has access to the share.

**Set permissions for shared folders**

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

---

**Before you begin**

Create the following:

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

**Task**

1. Right-click the quarantine folder, then select *Properties*.
2. Select the *Sharing* tab, 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*.
5. Click *Add* to select an object type.
   - You can give permission only to administrators who require access to the quarantine folder.
   a. In *Select Users or Groups*, enter your Domain User account in the *object names* dialog box, then click *OK*.
   b. Select the user name you created earlier, select *Full Control*, then click *OK*.
6. Click *Add* to select an object type.
   a. In *Select Users or Groups*, enter your Domain Local Security Group in the *object names* dialog box, then click *OK*.
   b. With this group selected, select *Full Control*, then click *OK*. 

---
**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 necessary.
- Download `MOVE-AV-AL_RestoreTool.4.5.0.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.4.5.0.Zip`, start the quarantine restore tool.
   ```cmd
   quarantine_restore.cmd
   ```
   The Connect dialog box is automatically displayed.
2. Enter the location and credentials of the quarantine share, then click **OK**.
   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.
   **Information:** 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 two 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 in the `RestoreTool.log`. 
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></td>
<td>• HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\mvagtdrv</td>
</tr>
<tr>
<td></td>
<td>• HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\mvagtsvc</td>
</tr>
<tr>
<td></td>
<td>• HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\EventLog\Application\MOVE AV client</td>
</tr>
<tr>
<td>Service stop protection</td>
<td>The mvagtsvc service cannot be stopped.</td>
</tr>
</tbody>
</table>

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

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

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

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

mvadm config set IntegrityEnabled=3

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

mvadm config set IntegrityEnabled=5

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

mvadm config set IntegrityEnabled=0
When Service stop protection is enabled (by setting the highest bit to 1), the mvagtsvc service does not accept stop commands. File protection and registry protection require the agent driver be loaded, but service stop protection does not. Use these commands to load or unload the driver.

mvadm enable

mvadm disable

**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.

<table>
<thead>
<tr>
<th>Protection type</th>
<th>Protection effects</th>
</tr>
</thead>
</table>
| 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 to 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 helpful to:

- 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

McAfee® Threat Intelligence Exchange (TIE) provides context-aware adaptive security for your virtual environment. It quickly analyzes files and content from the SVM in your environment and makes
informed security decisions. These decisions are based on a file's security reputation and your own criteria set in the Shared Cloud Solutions policy of McAfee MOVE AntiVirus. The Multi-Platform deployment, with TIE and Advanced Threat Defense integration, becomes a multi-layered solution that involves various techniques to scan and detect the malware. It includes:

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

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

**How Threat Intelligence Exchange works**

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

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

**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 server management
- McAfee DXL client for McAfee ePO
- McAfee DXL client management

**How Advanced Threat Defense works**

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

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

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

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

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

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

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

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

### Scenarios for using Threat Intelligence Exchange

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

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

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

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

### How a reputation is determined

File and certificate reputation is determined when a file attempts to run on a managed system.

These steps occur in determining a file or certificate's reputation.

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

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

7 The SVM sends threat details as threat events to McAfee ePO.
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
- View visibility and health details of the SVM
- View default queries

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 McAfee MOVE AntiVirus 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 under 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.
View visibility and health details of the SVM

You can 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.

View default queries

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

**Task**
For details about product features, usage, and best practices, click ? or Help.
1. Log on to McAfee ePO as an administrator.
2. Select **Menu** | **Reporting** | **Queries & Reports**.
3. From the **McAfee Groups** pane, select **MOVE AntiVirus 4.5.0** 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>
<thead>
<tr>
<th>Query</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Protection Status</td>
<td>Displays the status of all McAfee MOVE AntiVirus clients managed by the server.</td>
</tr>
<tr>
<td>Clients connected with a given SVM</td>
<td>Displays the details of the client and SVM it is assigned.</td>
</tr>
<tr>
<td>DAT version</td>
<td>Displays the DAT version of all McAfee MOVE AntiVirus clients that are managed by the server.</td>
</tr>
<tr>
<td>Summary of Threats Detected in the Last 24 Hours</td>
<td>Displays threats detected in the last 24 hours.</td>
</tr>
<tr>
<td>Threats Detected in the Last 24 Hours</td>
<td>Displays the number of threats detected in the last 24 hours by hour.</td>
</tr>
<tr>
<td>Top 10 Computers with the Most Detections</td>
<td>Displays the top ten computers with the most threat detections in the last three months.</td>
</tr>
<tr>
<td>Top 10 Detected Threats</td>
<td>Displays the top ten detected threats in the last three months.</td>
</tr>
</tbody>
</table>
### 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 ten 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 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 they 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>Displays these scan time events of the SVM.</td>
</tr>
<tr>
<td>SVM Capacity Events</td>
<td>Specifies the maximum number of endpoints with the number of endpoints connected.</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 request.</td>
</tr>
</tbody>
</table>
Table 4-3  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 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 whenever an SVM is registered with SVM Manager.</td>
</tr>
<tr>
<td></td>
<td>• SVM_MANAGER_SVM_UNREGISTER — This event is reported whenever an SVM is unregistered from the SVM Manager because of issues like SVM shutdown, network interruptions.</td>
</tr>
<tr>
<td>SVM_MANAGER_STARTED</td>
<td>This event is reported when the SVM Manager starts.</td>
</tr>
<tr>
<td>SVM_MANAGER_STOPPED</td>
<td>This event is reported when the SVM Manager stops.</td>
</tr>
</tbody>
</table>

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 it is used to retrieve the SVM details. The script is available at `/opt/McAfee/movesvmmanger`.

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/movesvmmanager directory:

- `sudo ./msmclient.sh svmcount` — Displays the number of SVMs attached to the SVM Manager.
- `sudo ./msmclient.sh svminfo` — Displays some basic information about the SVMs attached to the SVM Manager.
- `sudo ./msmclient.sh svmdetails` — 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 Cloud Workload Discovery extension 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 in the licensed SVM.</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 three 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>Query</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------</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>
</tbody>
</table>
Client command-line interface reference

You can access the McAfee MOVE AntiVirus (Multi-Platform) client command-line interface (CLI) on the agent virtual machine to perform basic maintenance tasks.

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

Contents
- Accessing the CLI
- Password protected CLI

Accessing the CLI

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

- Open the Multi-Platform CLI: click Start | Programs | McAfee | MOVE AV Client 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 virtual machine.

config

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

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

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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AllowNetworkScan</td>
<td>0 (off) or 1 (on). Defaults to 0.</td>
<td>Enables or disables scanning of files residing on a network path.</td>
</tr>
<tr>
<td>ConnTimeout</td>
<td>A positive integer value. Defaults to 0 (no timeout).</td>
<td>Sets the connection timeout in milliseconds.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>EventSink</td>
<td>An integer between 0 (no notifications) and 14 (all notifications). Defaults to 14.</td>
<td>Determines where threat events are sent. The total combines the values for Windows Event Viewer log (2), McAfee ePO Threat Event Log (4), and McAfee system tray pop-up menu (8).</td>
</tr>
<tr>
<td>IntegrityEnabled</td>
<td>An integer between 0 (no self-protection) and 7 representing a binary value. Defaults to 7 (all self-protections).</td>
<td>Determines the active self-protections. The total combines the values for file (1), registry (2), and services (4).</td>
</tr>
<tr>
<td>LogFileNum</td>
<td>A positive integer value. Defaults to 4.</td>
<td>Limits the number of log files allowed before they are rotated.</td>
</tr>
<tr>
<td>LogFileSize</td>
<td>An integer greater than 1024. Defaults to 2048.</td>
<td>Limits the size (in KB) of an individual log file.</td>
</tr>
<tr>
<td>MaxFileSize</td>
<td>A positive integer value. Defaults to 40.</td>
<td>Limits the size (in MB) of files where scan results are cached. Files up to this size are transferred completely to the SVM for scanning.</td>
</tr>
<tr>
<td>QuarantineEnabled</td>
<td>0 (off) or 1 (on). Defaults to 1.</td>
<td>Enables or disables quarantine services.</td>
</tr>
<tr>
<td>QuarantineFolder</td>
<td>A valid file path. Defaults to C:\Quarantine.</td>
<td>Determines where quarantined files are stored. Cannot be a mapped network drive or UNC file path.</td>
</tr>
<tr>
<td>QuarantineDays</td>
<td>A positive integer. Defaults to 28.</td>
<td>Determines the number of days quarantined files are stored before being deleted. Submitting a 0 turns off quarantined file deletion.</td>
</tr>
<tr>
<td>RTEMode</td>
<td>0 (off) or 1 (on). Defaults to 0.</td>
<td>Indicates protection status on the virtual machine. This value cannot be changed through the config command.</td>
</tr>
<tr>
<td>OASStatus</td>
<td>0 (off) or 1 (on). Defaults to 0.</td>
<td>Indicates on-access scan status on the virtual machine. This value cannot be changed through the config command.</td>
</tr>
<tr>
<td>ODSStatus</td>
<td>0 (off) or 1 (on). Defaults to 0.</td>
<td>Indicates on-demand scan status on the virtual machine. This value cannot be changed through the config command.</td>
</tr>
<tr>
<td>ScanAllFileTypes</td>
<td>0 (specific extensions) or 1 (all files). Defaults to 1.</td>
<td>Determines whether to scan all files or only specific extensions.</td>
</tr>
<tr>
<td>ODSScanAllFileTypes</td>
<td>0 (specific extensions) or 1 (all files). Defaults to 1.</td>
<td>Determines whether to scan all files or only specific extensions.</td>
</tr>
<tr>
<td>ScanFlags</td>
<td>An integer between 0 (no operations scanned) and 7 representing a binary value. Defaults to 7 (all operations scanned).</td>
<td>Determines which operations trigger scanning. The total combines the values for Read (1), Write (2), and Backup (4).</td>
</tr>
<tr>
<td>ScanTimeout</td>
<td>A positive integer. Defaults to 45000.</td>
<td>Limits the time (in milliseconds) allowed for file scans after which the file can be accessed.</td>
</tr>
<tr>
<td>ODS ScanTimeout</td>
<td>A positive integer. Defaults to 45000.</td>
<td>Limits the time (in milliseconds) allowed for on-demand scan after which the file can be accessed.</td>
</tr>
<tr>
<td>ServerAddress1</td>
<td>An IPv4 address or FQDN. No default.</td>
<td>Specifies the IPv4 address or FQDN of the primary SVM used by the virtual machine.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Value</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ServerAddress2</td>
<td>An IPv4 address or FQDN. No default.</td>
<td>Specifies the IPv4 address or FQDN of the secondary SVM used by the virtual machine.</td>
</tr>
<tr>
<td>ServerPort1</td>
<td>Between 1024 and 65535. Defaults to 9053.</td>
<td>Specifies the port used to communicate with the primary SVM.</td>
</tr>
<tr>
<td>ServerPort2</td>
<td>Between 1024 and 65535. Defaults to 9053.</td>
<td>Specifies the port used to communicate with the secondary SVM.</td>
</tr>
<tr>
<td>ThreatAction1</td>
<td>0 (delete) or 1 (deny access). Defaults to 0.</td>
<td>Determines the primary action taken when a threat is detected.</td>
</tr>
<tr>
<td>ThreatAction2</td>
<td>0 (delete) or 1 (deny access). Defaults to 1.</td>
<td>Determines the secondary action taken when a threat is detected.</td>
</tr>
<tr>
<td>ODS ThreatAction1</td>
<td>0 (delete) or 1 (deny access). Defaults to 0.</td>
<td>Determines the primary action taken when a threat is detected during on-demand scan.</td>
</tr>
<tr>
<td>ODSThreatAction2</td>
<td>0 (delete) or 1 (deny access). Defaults to 1.</td>
<td>Determines the secondary action taken when a threat is detected during on-demand scan.</td>
</tr>
<tr>
<td>SVMManagerAddress</td>
<td>An IPv4 address or FQDN. No default.</td>
<td>Specifies the IPv4 address or FQDN of the SVM Manager.</td>
</tr>
<tr>
<td>SVMManagerPort</td>
<td>Between 1024 and 65535. Defaults to 8080.</td>
<td>Specifies the port used to communicate with SVM Manager.</td>
</tr>
</tbody>
</table>

**disable**

Use the `disable` command to disable the McAfee MOVE AntiVirus client on the virtual machine.

```
mvadm disable
```

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

⚠️ This command removes virus protection from the virtual machine leaving it vulnerable to threats.

**enable**

Use the `enable` command to enable the McAfee MOVE AntiVirus client on the virtual machine.

```
mvadm enable
```

<table>
<thead>
<tr>
<th>Arguments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Enables the McAfee MOVE AntiVirus client. This restores virus protection to the virtual machine.</td>
</tr>
</tbody>
</table>
**ftypes**

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

```
mvadm ftypes add oas extn
mvadm ftypes remove oas extn
mvadm ftypes list oas
mvadm ftypes add oas exe pdf zip
mvadm ftypes add ods exe pdf zip
```

Wildcards are not supported by the `ftypes` command, and extensions must be an exact match. Issuing an `mvadm ftypes add doc` command does not cause `.DOCX` files to be scanned.

<table>
<thead>
<tr>
<th>Arguments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>add oas extn</code></td>
<td>Causes the files with extension <code>extn</code> to be included for anti-virus scanning.</td>
</tr>
<tr>
<td><code>remove oas extn</code></td>
<td>Removes the files with extension <code>extn</code> from the list of files to be included for anti-virus scanning.</td>
</tr>
<tr>
<td><code>list oas</code></td>
<td>Lists the file extensions to be included for on-access scan.</td>
</tr>
<tr>
<td><code>add ods exe pdf zip</code></td>
<td>Adds the files with extensions <code>exe pdf zip</code> to be included for on-access scan.</td>
</tr>
<tr>
<td><code>add ods exe pdf zip</code></td>
<td>Adds the files with extensions <code>exe pdf zip</code> to be included for on-demand scan.</td>
</tr>
</tbody>
</table>

**help**

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

```
mvadm help
mvadm help command
```

<table>
<thead>
<tr>
<th>Arguments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>default</code></td>
<td>Lists the summary description for the McAfee MOVE AntiVirus client CLI commands.</td>
</tr>
<tr>
<td><code>command</code></td>
<td>Lists the detailed help for the provided command.</td>
</tr>
</tbody>
</table>

**loglevel**

Use the `loglevel` command to view and edit the log level of the McAfee MOVE AntiVirus client.

```
mvadm loglevel
mvadm loglevel enable {MODULE_NAME | ALL} {TYPES... | ALL}
mvadm loglevel disable {MODULE_NAME | ALL} {TYPES... | ALL}
```
**Arguments** | **Description**
---|---
default | Lists the current log level of each module that is part of the McAfee MOVE AntiVirus client. Use this form to get a full list of modules for use with other forms of the loglevel command.

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

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

These are the supported log level types:

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

**pp**

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

Process passthrup rule supports these path format:

- Just the process name, for example: `xyz.exe`
- Partial path, for example: `abc\xyz.exe`
- Complete path, for example: `C:\abc\xyz.exe`
- Windows path, for example: `%windir%\abc\xyz.exe`

Note these points while using the `pp` command to specify trusted processes:

- If `%abc%` does not resolve, skip it from the list.
- This format is only valid from McAfee ePO.
- This resolves the path with respect to the system user.

```
mvadm pp list oas
mvadm pp list ods
mvadm pp add oas <process path>
mvadm pp remove oas <process path>
mvadm pp set <process path>
mvadm pp add oas <file path>
```
### Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
</table>
| **add oas** `<process image path>` | Adds the specified process (or processes) as a trusted process. As an example:  
  mvadm pp add userprofilemanager.exe  
  All files acted upon by the userprofilemanager.exe file are excluded from the scan. |
| **remove oas** `<process image path>` | Removes the specified process (or processes) as a trusted process.                                                                                                      |
| **set** `<process image path>` | Removes all existing trusted processes and adds the specified process (or processes) as trusted processes.                                             |
| **add oas** `<file path>` | Adds specified file path as a trusted file path for on-access scan. For example:  
  mvadm pp add oas c:\windows\system32\notepad.exe  
  All file paths acted upon by the c:\windows\system32\notepad.exe file path are excluded from on-access scan. |

### exp

Use the `exp` command to specify path exclusion. All paths acted upon by a trusted process are excluded from on-access scan.

- `mvadm exp add oas <file path>
- `mvadm exp list oas`

### Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
</table>
| **add oas** `<file path>` | Excludes specified file path from trusted file path during on-access scan. For example:  
  mvadm exp add oas "3|11|c:\folder1\*.txt"  
  3 | 11 — This scans the specified directory only.  
  3 | 15 — This scans the specified directory and subdirectories.  
  All file paths acted upon by the 3|11|c:\folder1\*.txt file path are excluded during on-access scan. |
| **list oas** | Lists excluded file paths from on-access scan. |

### q

Use the `q` command to change McAfee MOVE AntiVirus (Multi-Platform) quarantine behavior.

- `mvadm q list`
- `mvadm q restore <detected as>`
- `mvadm q remove <detected as>`
### Arguments

**list**

Lists the currently quarantined files and their detection type.

**restore <detected as>**

Restores all .VIR files from the currently configured quarantine folder with the specified `<detected as>` category.

**remove <detected as>**

Deletes all .VIR files from the currently configured quarantine folder with the specified `<detected as>` category.

---

### status

Use the `status` command to display the current state of the McAfee MOVE AntiVirus client in terms of operational mode (enabled or disabled) and its McAfee MOVE AntiVirus Multi-Platform SVM details.

```
mvadm status
```

### Arguments

**default**

Lists the current McAfee MOVE AntiVirus client status.

**OASStatus**

Displays the current status of the on-access scan.

**ODSStatus**

Displays the current status of the on-demand scan.

**ODSScanAllFiletypes**

Lists the all file types of on-demand scan.

---

### Example

```
C:\Program Files\McAfee\MOVE AV client>mvadm status
Scan Configuration: Enabled
On Access Scan: Enabled
On Demand Scan: Disabled
Driver Status: Driver is loaded
Primary Server: 10.216.19.210:9053 [Active]
Secondary Server: NONE:9053 [Not Configured]
SVM Manager: 10.216.19.154:8080 [Configured]
Protection Status: Enabled
```

### version

Use the `version` command to display the version of the McAfee MOVE AntiVirus client installed on the virtual machine.

```
mvadm version
```

### Arguments

**default**

Displays the version of the McAfee MOVE AntiVirus client installed on the virtual machine. This is most useful for verifying that an upgrade operation is complete, or checking if an upgrade is needed.
Password protected CLI

Set the password protection through the client policy to prevent users from changing the anti-virus settings, or disabling the AV protection.

After setting the password, type the password to execute any of these commands on the `mvadm` command-line of the clients.

- config
- disable
- enable
- filetypes
- procpassthru
- loglevel

Set password for client CLI

Specify the password on the McAfee ePO server to prevent users from changing the AV settings, or disabling the AV protection on the client.

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

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

1. Log on to McAfee ePO as an administrator
2. Select Menu | Policy | Policy Catalog, then select MOVE AntiVirus Common 4.5.0 from the Product list.
3. From the Category list, select Options.
4. Click the name of an editable policy.
5. Enable Enable Self-Protection for MOVE CLI and type the password, then retype it in Confirm Password.
6. Click Save to modify the policy.

You can now verify that the commands on the client system are password-protected.
You can access the command-line interface (CLI) on the SVM virtual machine to perform basic maintenance tasks.

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

## Access the CLI

A shortcut to the command-line interface (CLI) for the SVM is added to the Windows Start menu during installation.

### Task

- Open the McAfee MOVE AntiVirus 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.

### cache

Use the `cache` command to perform operations on the SVM’s scan cache.

- `mvadm cache save cfilename`
- `mvadm cache load cfilename`
- `mvadm cache list`
- `mvadm cache flush`
- `mvadm cache info`

### Arguments

<table>
<thead>
<tr>
<th>Arguments</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>save cfilename</td>
<td>Save the current set of checksums from the trusted checksum cache to the file <code>cfilename</code>.</td>
</tr>
<tr>
<td>load cfilename</td>
<td>Load the checksums from file <code>cfilename</code> to the trusted checksum cache.</td>
</tr>
<tr>
<td>list</td>
<td>List the checksums available in the trusted checksum cache.</td>
</tr>
</tbody>
</table>
### Arguments | Description
---|---
flush | Remove all checksums from the trusted checksum cache.
info | Print details of the trusted checksum cache.

**config**

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

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

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

### Parameters | Value | Description
---|---|---
ComputeChecksum | 0 (server) or 1 (client). Defaults to 1. | Determines whether to use the server-computed checksum of the file or the checksum sent by the McAfee MOVE AntiVirus client.
ConnTimeout | A positive integer value. Defaults to 0 (no timeout). | Sets the connection timeout in milliseconds.
GTILevel | Between 0 (disabled) and 5 (Very High). Defaults to 1 (Very Low). | Sets the Global Threat Intelligence level.
IntegrityEnabled | 0 (off) or 1 (on). Defaults to 1. | Enables or disables the self-protection feature.
LogFileNum | A positive integer value. Defaults to 4. | Limits the number of log files allowed before they are rotated.
LogFileSize | An integer greater than 1024. Defaults to 2048. | Limits the size (in KB) of an individual log file.
MaxCacheItems | A positive integer value. Defaults to 1,000,000. | Limits the number of items that can exist in the cache.
NumThreads | Between 0 and 500. Defaults to 300. | Limits the number of available scan request threads.
ScanArchiveFiles | 0 (off) or 1 (on). Defaults to 0. | Enables or disables scanning inside archive files.
ScanPUPS | 0 (off) or 1 (on). Defaults to 0. | Enables or disables checking for potentially unwanted programs (PUPs). Scan behavior is determined by VirusScan Enterprise settings.
ServerPort1 | Between 1024 and 65535. Defaults to 9053. | Determines the port on which the server listens for client requests.
SVMManagerAddress | An IPv4 address or FQDN. No default. | Specifies the IPv4 address or FQDN of the SVM Manager.
SVMManagerPort | Between 1024 and 65535. Defaults to 8080. | Specifies the port used to communicate with SVM Manager.
RAMDiskEnabled | 1 (0x1) | Enables or disables the RAM disk option.
### Parameters

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaxNumClients</td>
<td>250 (0xf4240)</td>
<td>Maximum number of clients, which can be connected to the OSS.</td>
</tr>
<tr>
<td>OSSGUID</td>
<td>&lt;GUID&gt;</td>
<td>Unique GUID required to register it to SVM Manager.</td>
</tr>
</tbody>
</table>

### help

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

```bash
mvadm help
```

```bash
mvadm help command
```

### Arguments

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default Lists the summary description for the McAfee MOVE AntiVirus SVM CLI commands.</td>
</tr>
<tr>
<td>command Lists the detailed help for command command.</td>
</tr>
</tbody>
</table>

### loglevel

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

```bash
mvadm loglevel
```

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

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

### Arguments

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default Lists the current log level of each module in the McAfee MOVE AntiVirus SVM. Use this form to get a full list of modules for use with the other forms of the loglevel command.</td>
</tr>
<tr>
<td>enable {MODULE_NAME</td>
</tr>
<tr>
<td>disable {MODULE_NAME</td>
</tr>
</tbody>
</table>

These are the supported log level types:

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

### stats

Use the `stats` command to display the current statistics of the McAfee MOVE AntiVirus SVM.

```bash
mvadm stats
```
Arguments Description

default Displays current usage and performance statistics for the McAfee MOVE AntiVirus SVM. The statistics are collected in real time, and the displayed data is a snapshot of the information at the time the command was invoked. The full list of reported statistics is shown in the example output.

Example output

```
C:\>mvadm stats
Total number of checksum req:                        13125
Total number of file transfer req:                11825
Total number of smart file req:                      14
Total number of scans on RAM disk:                                                    11825
Checksum cache hit:                                   1300
Total av scan req:                                11825
Total av scan failure:                                0
Data recv failure:                                    0
Resp send failure:                                    0
Total scan threads:                                 300
Total heartbeat threads:                             0
Total idle threads:                                 300
Number of requests in queue:                          0
Number of items in cache:                             0
Avg request process time:                      0.045183 sec
Avg request wait time:                             0.000000 sec
Number of frequently modified files scanned:         848
Data saved for frequently modified files:            98%
Maximum entries for frequently modified files:        25
Total Tie Requests:                               95486
Total Tie File Reputation Requests:                 90622
Total Tie Cert Reputation Requests:                  36
Total ATD candidates:                               851
Total ATD successful submissions:                    76
Total Tie Cache Hits:                               4712
Total Tie Certificate Cache Hits:                   116
Total Tie File Reputation change events:            140
Total Tie Certificate reputation change events:       0
Total Tie Certificate hashes in Global cache:        46827
Tie Avg Response Time per Request:             0.370643 sec
```

version

Use the `version` command to display the version of the McAfee MOVE AntiVirus SVM application installed on the server virtual machine.

```
mvadm version
```

Arguments Description

default Displays the version number of the McAfee MOVE AntiVirus SVM. This is most useful for verifying that an update has completed successfully, or checking if an update is needed.
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?**

You must convert the .vmdk file format to .vhd file to deploy the SVM Manager to Microsoft Hyper-V. You must 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 .vhdx format image, run this command: `ConvertTo-VirtualHardDisk -SourceLiteralPath "C:\VMDKs\SVM_Manager_3.x-disk1.vmdk"`

5. For .vhd 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 have converted 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 one by one on 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**
You need to 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 under General tab.
9. Click Save to save the changes, then click apply the policy to the clients.

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

If you require the Multi-Platform Threat Event pop-up alerts through the Remote Desktop Protocol (RDP) session, you can 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 Cloud Workload Discovery VM with Agentless?**

Perform these steps to create an on-demand scan task for the Cloud Workload Discovery VM with Agentless systems.

1. Check in the Cloud Workload Discovery 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 the 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 4.5.0.
   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 do an agent wake-up 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 an expected behavior. This informational message can be ignored.

In some environments, you might see these warning messages in mvagent.log, which is the scan log generated by the McAfee MOVE AntiVirus (Multi-Platform) client on protected systems:

- **WARNING**: utl_rt.c : 109: Process info is NULL for proc handle 0x4
- **WARNING**: fsh_winnt.c : 216: Failed to get for process info of (System)

The message does not upload as an event to McAfee ePO.

**How can I manually check the DAT version installed on the McAfee MOVE AntiVirus SVM in an Agentless environment?**

You can check what 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 the valid credentials.
4. Run this command to change the directory: `cd /opt/McAfee/move/bin`
5. Run this command to display the SVM details: `./svm-config -v`

   **For example:**
   
   McAfee MOVE AntiVirus Agentless 4.5.0.317
   McAfeeVSEForLinux 2.0.3.29216-29216-x86_64
   Virus definition files 8212.0000
   Virus scanning engine 5800.7501
   Virus scanning engine API 5800.7501
   Apache 1.3.42 (Unix)
   OpenSSL 1.0.1t 3 May 2016
   sqlite 2.8.17

**Method 2**

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

   The required details appear in the command window.
**Why is 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 FDQN 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 hostname.

**An error occurred while communicating with NSX after trying to upgrade to McAfee MOVE AntiVirus. How do I fix this?**

Edit the SQL database to edit the McAfee ePO server table entries and run the Data Migration task before trying to upgrade to McAfee MOVE AntiVirus.

1. Open the SQL database and delete the row from the `DC_AL_NSX_MANAGER_DETAILS` table corresponding to the vCenter account.
2. Select *Menu* | *Automation* | *MOVE AntiVirus Deployment* | *Configuration* | *Server Settings*.
3. Click Run next to Run NSX Data Migration.
4. Navigate to the MOVE AntiVirus Deployment page and complete the upgrade process.

**What do I do if an upgrade attempt to McAfee MOVE AntiVirus 4.5.0 fails?**

Perform these steps to successfully upgrade from McAfee MOVE AntiVirus (Agentless) 4.0.0 to McAfee MOVE AntiVirus 4.5.0.

1. Install the McAfee MOVE AntiVirus 4.5.0 extension on the McAfee ePO server.
2. Check in the SVM 4.5.0.
3. Use the Migration Assistant utility and run the data migration. For information, see *McAfee MOVE AntiVirus Migration Guide*.
4. Upgrade the McAfee MOVE AntiVirus Service.

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


**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 Intel Security download site, then do a fresh deployment.
Perform these steps only if the SVM shows as **Unmanaged** in McAfee ePO System Tree:

1. Delete the system.
   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. Proceed 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 the **Registered Cloud Accounts**, then the vCenter will appear 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 may 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 the **Registered Cloud Accounts**.

1. Log on to McAfee ePO as an administrator.

2. Select **Menu** | **configuration** | **Registered Cloud Accounts** to open **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 will now create a task that will synchronize the vCenter according to the above configuration.

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

**Method 1**

Perform these steps to disable and re-enable the MOVE driver.

1. Log on to the system as an administrator.

2. Click **Start** | **Run**.
3 Run these commands one by one:
   • mvadm disable
   • mvadm enable

4 Close the command prompt window.

Method 2
Perform these steps to restart Multi-Platform client service.

1 Log on to the system as an administrator.

2 Click Start | Run.

3 Run these commands one by one:
   • sc stop mvagtdrv
   • sc start mvagtdrv

4 Close the command prompt window.

What do I do if there is 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:

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

What do I do when 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 may 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.</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 NSX environment. Where do I find the original name of the hostname where the infection occurred instead on IP of McAfee MOVE AntiVirus SVM?

The Threat Event Log displays the hostname of the system where infection has occurred.

Make sure that you configured SVM Configuration details and tested connection settings under SVM Settings policy on the McAfee ePO server.

1. Log on to McAfee ePO as an administrator.
2. Select Menu | Reporting | Threat Event Log.
# Index

## A
- about
  - McAfee MOVE AntiVirus 9
- about this guide 7
- Agentless
  - components 12
  - features 10

## C
- client command-line reference
  - accessing client 65
  - config command 65
  - disable command 67
  - enable command 67
  - ftypes command 68
  - help command 68
  - loglevel command 68
  - pp command 69
  - q command 70
  - status command 71
  - version command 71
- client notification
  - deferred scan 40
- client task 18
  - quarantine 49
  - scan diagnosis 40, 43
  - targeted ODS 38
- command line
  - password protected 72
- common settings
  - configuring 23
- components
  - defined 11, 12
  - overview 11, 12
- config command
  - client 65
  - SVM 74
- configuration
  - deferred scan 39
  - exclusions 24
  - on-access scan 30
  - on-demand 32
  - permission sets 23

## D
- configuration (continued)
  - quarantine manager 48
  - quarantine settings 50
  - targeted on-demand scan 37
- conventions and icons used in this guide 7
- dashboard
  - McAfee MOVE AntiVirus 59
  - MOVE AntiVirus queries 60
- default queries, displaying 60
- deferred scan
  - client notification 40
  - configuring 39
- deployment
  - agentless 10, 13
  - method 13
  - methods 9, 10, 13
  - multi-platform 9, 13
- details
  - protection 55
- detection
  - finding threats 15
  - on-access scan 48
  - on-demand scan 48
  - responding 47
  - unwanted program 47
- diagnostic tool
  - running 41
- disable command 67
- documentation
  - audience for this guide 7
  - product-specific, finding 8
  - typographical conventions and icons 7

## E
- enable command 67
- events
  - MOVE AntiVirus 54
- exclusions
  - configuring 24
  - scan items 26
Index

F
features
  McAfee MOVE AntiVirus (Agentless) 10
  McAfee MOVE AntiVirus (Multi-Platform) 10
file protection 53

H
help command
  client 68
  SVM 75

I
installation
  automated 19
  wizard 19
integration
  TIE 55
introduction
  McAfee MOVE AntiVirus 9

L
logging
  McAfee MOVE AntiVirus 24
logging and events
  on-demand scan 36
loglevel command
  client 68
  SVM 75

M
management
  diagnostic tool 41
  quarantine 50
managing
  McAfee MOVE AntiVirus 47
McAfee GTI
  about 26
McAfee MOVE AntiVirus
  about 9
  client tasks 18
  configuring 15
  features 10
  managing 47
  self-protection 53
McAfee ServicePortal, accessing 8
Multi-Platform
  components 11
  features 10
mvadm
  cache command 73
  config command 65, 74
  disable command 67
  enable command 67

mvadm (continued)
  ftypes command 68
  help command 68, 75
  loglevel command 68, 75
  pp command 69
  q command 70
  stats command 75
  status command 71
  version command 71, 76

O
on-access scan
  configuring 30
  scan type 26
  scanning 13, 15, 26, 28, 30, 48
on-demand scan
  configuring 32
  logging and events 36
  scan type 26, 32
  scanning 13, 15, 26, 48
  targeted 37
  working 32

P
permission sets 22
  configuring 23
policies
  applying 20
  create new 20
  options summary 20
  using 19
  VM-based scan 21
protection
  analyzing 55

Q
quarantine
  command-line access 70
  configuring quarantine manager 48
  folder, configuring 51
  overview 50
  restore a file 52
  restore tool 50
  restoring 49
queries
  default, viewing 60
  list 60
  MOVE AntiVirus queries 60
  pie charts 60
  viewing default queries 60
queries, MOVE AntiVirus Agentless
  predefined 63
R
registry protection 53
reports
  supplied queries 60
response
  handling threats 15
MOVE AntiVirus 54

S
scan diagnosis 40
  configuring 40, 43
scan items
  excluding 24, 26
scan type
  on-access 28
scanning
  on-access 15, 26, 28, 30, 48
  on-demand 15, 26, 48
scanning option
  configuring 27
  on-access 13
  on-demand 13
scanning, deferred 39
security, strategy 15
self-protection
  McAfee MOVE AntiVirus 23
server command-line reference
  accessing SVM 73
  cache command 73
  config command 74
  help command 75
  loglevel command 75
  stats command 75
  version command 76
SVM
  configuring 13
  self-protection 53
  view details 60
SVM CLI
  cache command 73
  config command 74
  help command 75
  loglevel command 75
  stats command 75
  version command 76
SVM Manager
  about 13

T
targeted on-demand scan
  Agentless 38
    configuring 37
    Multi-Platform 38
technical support, finding product information 8
threat prevention
  scanning 15
TIE
  integrating 55

V
virtual machines
  protecting 13
VM-based scan
  policies 21

W
wizard
  installation 19