Best Practices Guide

# McAfee ePolicy Orchestrator 5.1.0 Software

## COPYRIGHT

## TRADEMARK ATTRIBUTIONS

## LICENSE INFORMATION

### License Agreement

# Contents

## Installing and configuring your McAfee ePO software

## Managing and reporting

## Scaling your managed network

## Maintaining and optimizing your McAfee ePO software

# Preface

This guide provides information about suggested best practices for using your McAfee® ePolicy Orchestrator® (McAfee ePO™) 5.1.0 software.

## 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.
- **Reviewers** — People who evaluate the product.

### Conventions

This guide uses these typographical conventions and icons.

| | |
|---|---|
| *Book title*, *term*, *emphasis* | Title of a book, chapter, or topic; a new term; emphasis. |
| **Bold** | Text that is strongly emphasized. |
| `User input, code, message` | Commands and other text that the user types; a code sample; a displayed message. |
| **Interface text** | Words from the product interface like options, menus, buttons, and dialog boxes. |
| Hypertext blue | A link to a topic or to an external website. |
| ℹ | **Note:** Additional information, like an alternate method of accessing an option. |
| 💡 | **Tip:** Suggestions and recommendations. |

| | |
|---|---|
| ❗ | **Important/Caution:** Valuable advice to protect your computer system, software installation, network, business, or data. |
| ⚠ | **Warning:** Critical advice to prevent bodily harm when using a hardware product. |

## What's in this guide

This guide outlines some core recommendations for implementing McAfee ePO software version 5.1.

This document is not meant to be a comprehensive guide for all implementations. Instead, use the information in this document during these four stages:

1. **Installing and configuring your McAfee ePO software** — Use these chapters:
   - Configuring your hardware on page 3
   - Installing and upgrading McAfee ePO software on page 3
   - Using the McAfee Agent and your System Tree on page 3
2. **Managing and reporting on your McAfee ePO environment** — Use these chapters:
   - Managing endpoint security with policies and packages on page 4
   - Using client and server tasks in your managed environment on page 4
   - Reporting with queries on page 4
3. **Scaling your McAfee ePO server managed network** — Use these chapters:
   - Using repositories on page 4
   - Using Agent Handlers on page 4
4. **Maintaining and optimizing your McAfee ePO software** — Use these chapters:
   - Maintaining your McAfee ePO server on page 5
   - Bandwidth usage on page 5
   - Automating and optimizing McAfee ePO workflow on page 5
   - Plan your disaster recovery on page 6

This document frequently references other documents in the McAfee ePO documentation set. The information contained in the other guides is not duplicated in this guide, but this guide points you to that information.

To fully understand the recommendations included in this guide, you must have a basic understanding of McAfee ePO software. If you don't have this level of experience, or you need more information about the software, consult one of the following documents:

- McAfee ePolicy Orchestrator Installation Guide
- McAfee ePolicy Orchestrator Product Guide
- McAfee ePolicy Orchestrator web API Scripting Guide
- McAfee ePolicy Orchestrator Log File Reference Guide

These guides are available from the McAfee Support Website.

## Find product documentation

After a product is released, information about the product is entered into the McAfee online Knowledge Center.

### Task

1. Go to the **Knowledge Center** tab of the McAfee ServicePortal at http://support.mcafee.com.
2. In the **Support Content** pane:
   - Click **Product Documentation** to find user documentation.
   - Click **Technical Articles** to find KnowledgeBase articles.
3. Select **Do not clear my filters**.
4. Enter a product, select a version, then click **Search** to display a list of documents.

1

# Introduction

The goal of this document is to increase your understanding of the McAfee ePO software so that you can easily and effectively protect your network.

**Contents**

## Using McAfee ePO software in your network

McAfee ePO software is a scalable, extensible management platform that enables centralized policy management and enforcement of your security products and the systems where they are installed.

It also provides comprehensive reporting and product deployment capabilities, all through a single point of control.

Using McAfee ePO software, you can perform these security tasks:

- Deploy security products and patches to the systems in your network.
- Manage the host and network security products deployed to your systems through the enforcement of security policies and the creation of tasks.
- Update the detection definition (DAT) files, anti-virus engines, and other security content required by your security software to ensure that your managed systems are secure.
- Use the built-in query system wizard to create reports that display informative user-configured charts and tables containing your network security data.
- Use a server task to run a query on a regular schedule, create a report, and email it to a list of users.

# Components

The architecture of the McAfee ePO software and its components is designed to help you successfully manage and protect your environment.

The McAfee ePO server provides these major functions:

- Manages and deploys products
- Enforces policies on your endpoints
- Collects events, product properties, and system properties from the managed endpoints and sends them back to McAfee ePO
- Distributes McAfee software, including new products, upgrades, and patches
- Reports on your endpoint security

This figure shows the major McAfee ePO components.

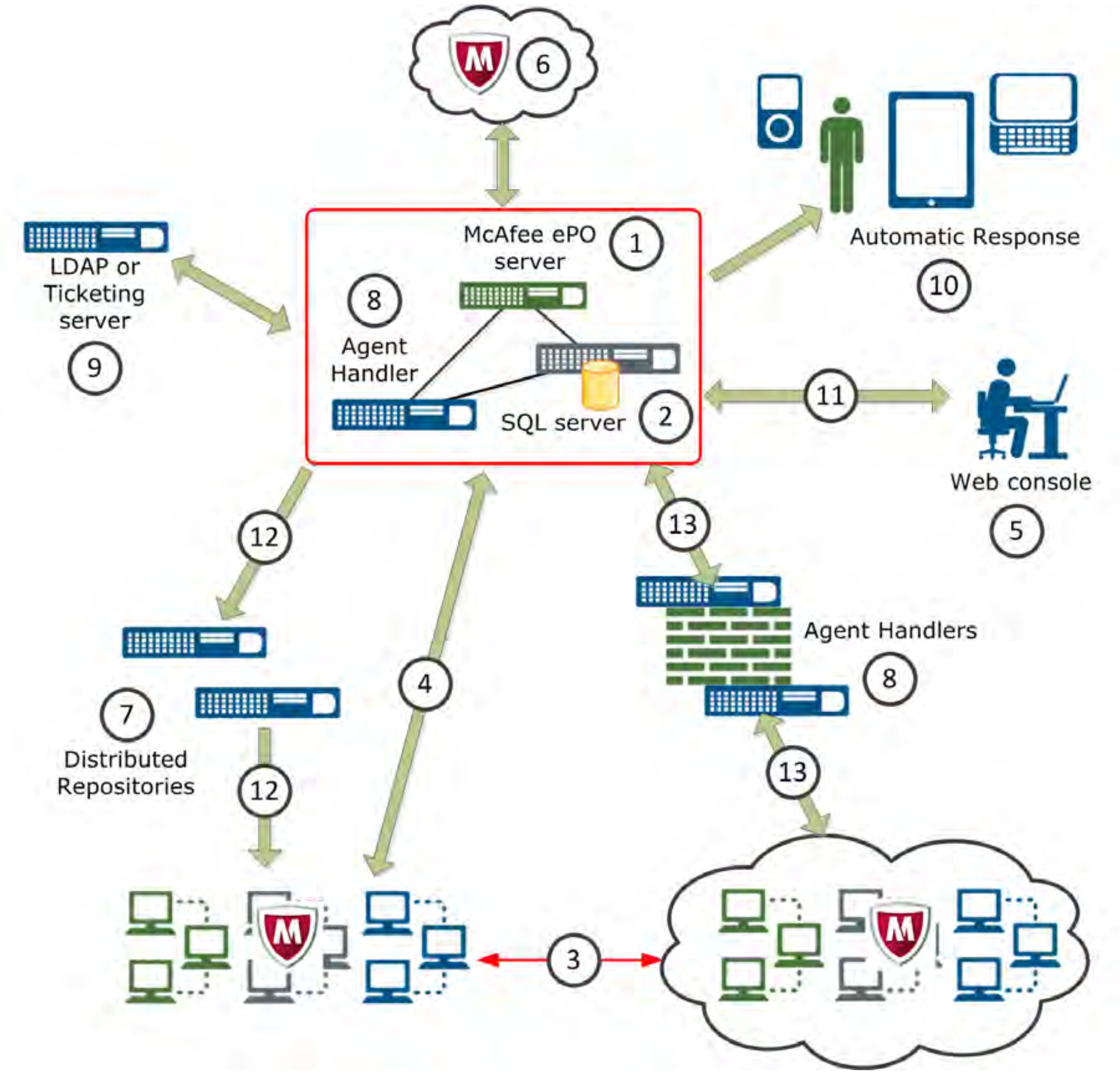


**Figure 1-1 Major McAfee ePO components**

The major McAfee ePO components are:

1 **McAfee ePO server** — Connects to the McAfee ePO update server to download the latest security content

2 **Microsoft SQL database** — Stores all data about your network managed systems, McAfee ePO, Agent Handlers, and repositories

3 **McAfee Agent installed on clients** — Provides these features:

- Policy enforcement
- Product deployments and updates
- Connections to send events, product, and system properties to the McAfee ePO server

4 **Agent-server secure communication (ASSC) connections** — Provides communications that occur at regular intervals between your systems and the server

> If remote Agent Handlers are installed in your network, agents communicate with the server through their assigned Agent Handlers.

5 **Web console** — Allows users to log on to the McAfee ePO console to perform security management tasks, such as running queries to report on security status or working with your managed software security policies

6 **McAfee web server** — Hosts the latest security content so that your McAfee ePO server can pull the content at scheduled intervals

7 **Distributed repositories** — Installed throughout your network to host your security content locally so that agents can receive updates more quickly

8 **Agent Handlers** — Reduces the workload of the server by off-loading event processing and McAfee Agent connectivity duties

> Agent Handlers are most effective when on the same network segment as the McAfee ePO database.

9 **LDAP or Ticketing system** — Connects your McAfee ePO server to your Lightweight Directory Access Protocol (LDAP) server or Simple Network Management Protocol (SNMP) ticketing server

10 **Automatic Responses** — Provides notifications to administrators and task automation when an event occurs

11 **Web Console** — Provides Hypertext Transfer Protocol Secure (HTTPS) connection between the McAfee ePO server and the web browser using default port 8443.

> McAfee recommends you not use the default port number for additional security. See McAfee ePolicy Orchestrator Product Guide to change console-to-application server communication port.

12 **Distributed Repositories** — Repository connections vary depending on the type of repository. For example, HTTP, FTP, or UDP connections.

13 **Agent Handlers** — Agent Handlers installed in the DMZ require specific port connections. See Ports used to communicate through a firewall on page 201.

# Installing and configuring your McAfee ePO software

Successfully installing and configuring McAfee ePO software on your server is the first step to protecting your network environment.

2

# Configuring your hardware

When you configure the McAfee ePO software, you must consider many factors, including the size of your network and the hardware you use.

**Contents**

## What affects McAfee ePO performance

To install and use the McAfee ePO server, it's important to know what factors affect the performance of your server and the attached SQL database.

For example, a McAfee ePO server and database can manage up to *200,000* client systems with only the *VirusScan Enterprise* product installed. But, as you add more software products and clients, that same server hardware can no longer provide the performance you expect.

Each of these factors affects your McAfee ePO server performance and must be considered as your managed network grows and your security needs change.

- **McAfee ePO server hardware** — See the Server hardware requirements on page 18 for server CPU, RAM, and hard drive recommendations.
- **SQL Server** — This server is the main workhorse behind the McAfee ePO server and affects the physical hardware and the ongoing maintenance of the SQL Server.
  - See Server hardware requirements on page 18 for SQL Server CPU, RAM, and hard drive recommendations.
  - See Maintaining your SQL database on page 151 for table data defragmentation and processes to purge client events.
- **Number of software products installed** — Each software product you install adds processing load on the McAfee ePO server and the SQL database.

- **Number of managed clients and their Agent Handlers** — These numbers are proportional to the McAfee ePO server and database performance.
  - See Server hardware requirements on page 18 for SQL Server CPU, RAM, and hard drive recommendations for the number of managed clients.
  - Each Agent Handler places these fixed loads on the database server:
    - Heartbeat updates every minute
    - Work queue checks (every 10 seconds)
    - Pool of database connections held open to the database (2 connections per CPU to the EventParser service and four connections per CPU to the Apache service)

## Server hardware requirements

You must determine the hardware requirements before you install the McAfee ePO software for the McAfee ePO server, SQL Server, and Agent Handlers, if needed.

Because the McAfee ePO server distributes software and content, you might think you need one McAfee ePO server for each major geographical region for efficient bandwidth utilization. You don't need more than one McAfee ePO server. Many McAfee ePO server users with large and small offices dispersed all over the world use only one McAfee ePO server. These users have repositories, which are simple file shares, at each office to handle the content distribution.

One McAfee ePO server has no technical limit on how many nodes it can manage. The key concept to remember about McAfee ePO servers is *less is better*. The fewer McAfee ePO servers you have, the easier it is to maintain your environment. Many users have one McAfee ePO server manage 200,000 or more nodes.

> The theoretical limit of McAfee ePO servers, in relationship to managed nodes, is even higher when you add Agent Handlers. But adding Agent Handlers directly impacts the performance of your McAfee ePO SQL database.

The SQL database, where the McAfee ePO server data is stored, determines the performance of your McAfee ePO server. This database is the main workhorse behind the McAfee ePO server. The three items that affect SQL performance are CPU, RAM, and disk performance. These three items control the responsiveness of the McAfee ePO server, from an SQL perspective. McAfee recommends that you exceed the minimum recommendations wherever possible.

The following table lists the hardware recommend for various sized organizations.

| Node count | McAfee ePO server | | | SQL Server | | | Agent Handler | | | Notes |
|---|---|---|---|---|---|---|---|---|---|---|
| | CPU cores* | RAM (GB) | Hard drive (GB) | CPU cores* | RAM (GB) | Hard drive (TB)** | CPU cores* | RAM (GB) | Hard drive (GB) | |
| < 10,000 | 4 | 8 | 300 | 4 | 8–16 | 0.5–1.0 | — | — | — | You can use a single server or VMs |
| 10,000–25,000 | 4 | 8–16 | 20–40 | 4 | 8–16 | 0.5–1.0 | 4 | 8 | 20–40 | See Planning your hard disk configuration on page 25 |
| 25,000–75,000 | 8 | 16–32 | 20–40 | 8 | 16–32 | 0.5–1.0 | 4 | 8 | 20–40 | |
| 75,000–150,000 | 8 | 32–64 | 40–80 | 16 | 32–128 | 1–2 | 4 | 8 | 40–80 | |

| Node count | McAfee ePO server | | | SQL Server | | | Agent Handler | | | Notes |
|---|---|---|---|---|---|---|---|---|---|---|
| | CPU cores* | RAM (GB) | Hard drive (GB) | CPU cores* | RAM (GB) | Hard drive (TB)** | CPU cores* | RAM (GB) | Hard drive (GB) | |
| 150,000 + | 16 | 64–128 | 40–80 | 32+ | 64–128 | 1–2 | 4 | 8 | 40–80 | |
| * These are physical Quad-core CPUs running at 2.2 GHz and 7.2 Gigatransfers per second (GT/s)<br>** Estimated event load for 6 months | | | | | | | | | | |

**Table Notes:**

- These estimates are for a McAfee ePO server running the EndPoint Suite of products.
- Basic RAM rule — Add 16 GB for every 25,000 nodes.

> You must use a 64-bit version operating system for the McAfee ePO server. You can use either a 32-bit or 64-bit version for the SQL database server operating system.

The following sections offer examples of environments that provide some guidelines for organization size and hardware requirements.

> These examples provide the minimum requirements for hardware. McAfee recommends that you exceed these requirements to improve performance and allow for growth, wherever possible.

## Example 1 — Fewer than 10,000 nodes

In an organization with fewer than 10,000 nodes, you can reduce hardware costs by installing the McAfee ePO server and SQL database on the same physical server. You can also have multiple McAfee products deployed in this environment, such as McAfee® VirusScan® Enterprise (VSE).

> Once you add the McAfee® Host Intrusion Prevention product, separate the McAfee ePO server and SQL database onto two physical servers.

This figure shows an organization with fewer than 10,000 nodes.

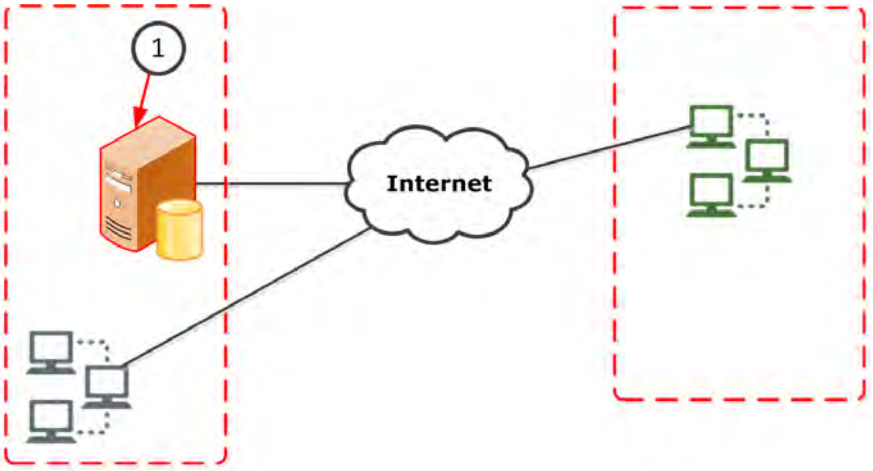


**Figure 2-1 Fewer than 10,000 node McAfee ePO network components**

In this figure, the McAfee ePO server has:

1 The McAfee ePO server and the Microsoft SQL database on the same server.

> Microsoft does not allow the SQL Express database to exceed 10 GB, and the memory available for the SQL Server Database Engine is limited to 1 GB.

The hardware used for McAfee ePO server and SQL database must be the most recent release of hardware with these minimum requirements:

- 4 Quad-core processor CPUs (for example, 16 core processors)
- 8 GB of RAM
- 300 GB of free hard drive space

## Example 2 — 10,000–25,000 nodes

You can use a single McAfee ePO server to manage an organization ranging from 10,000–25,000 nodes, with only the VirusScan Enterprise product installed.

As your node count approaches 10,000 nodes, McAfee recommends that you separate the McAfee ePO server and SQL servers onto their own physical servers.

This figure shows an organization configured for 25,000 nodes with the servers on different hardware.

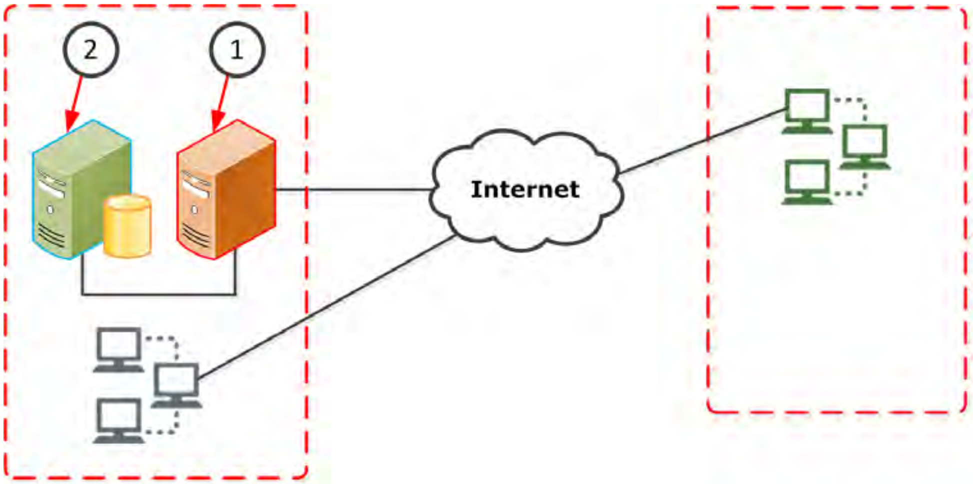


**Figure 2-2 McAfee ePO network components for 10,000–25,000 nodes**

In this figure, the 10,000–25,000 node organization example includes:

1 The McAfee ePO server

2 Separate SQL Server

10,000–25,000 node McAfee ePO server minimum hardware:

- 4 Quad-core processor CPU (for example, 16 core processors)
- 8–16 GB of RAM
- 20–40 GB of hard drive space

10,000–25,000 node SQL Server minimum hardware:

- 4 Quad-core processor CPUs (for example, 16 core processors)
- 8 to 16 GB of RAM
- 0.5 to 1.0 TB of hard drive space

## Example 3 — 25,000–75,000 nodes

You can manage an organization ranging from 25,000–75,000 nodes on a single McAfee ePO server, separate SQL Server, with only the VirusScan Enterprise product installed and properly placed repositories to update content and software to the agents.

This figure shows an organization configured for 25,000–75,000 nodes with the servers on different hardware and a distributed repository.

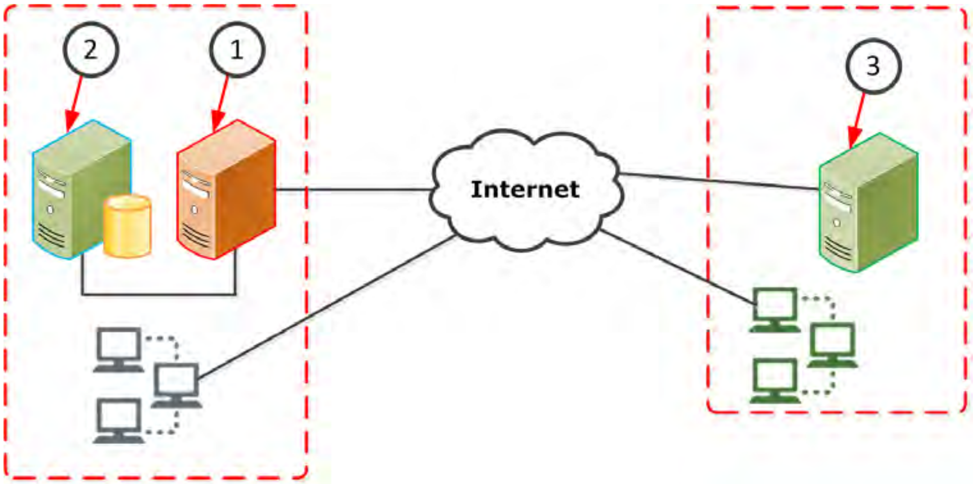


**Figure 2-3 McAfee ePO network components for 25,000–75,000 nodes**

In this figure, the 25,000–75,000 node organization example includes:

1. The McAfee ePO server
2. Separate SQL Server
3. Separate Distributed Repository to store and distribute important security content for your managed client systems.

25,000–75,000 node McAfee ePO server minimum hardware:

- 8 Quad-core processor CPU (for example, 32 core processors)
- 16–32 GB of RAM
- 20–40 GB of hard drive space

25,000 to 75,000 node SQL Server minimum hardware:

- 8 Quad-core processor CPUs (for example, 32 core processors)
- 16–32 GB of RAM
- 0.5–1.0 TB of hard drive space

## Example 4 — 75,000–150,000 nodes

You can manage an organization ranging from 75,000–150,000 nodes on a single McAfee ePO server, separate SQL Server, separate Agent Handler, and properly placed repositories to update content and software to the agents.

This figure shows an organization configured for 75,000–150,000 nodes

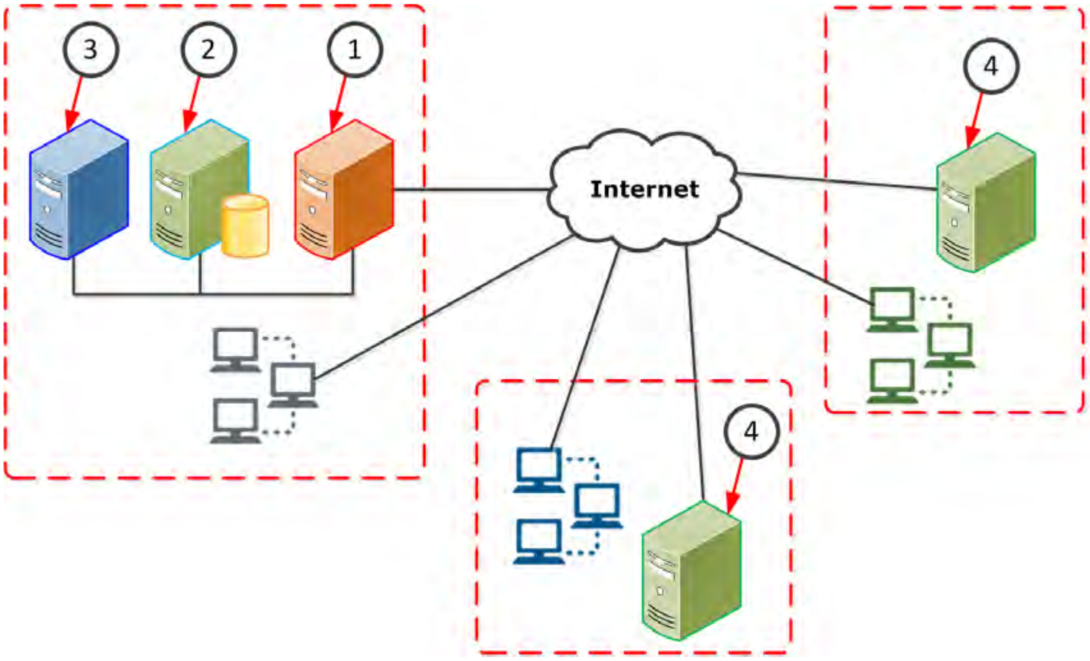


**Figure 2-4 75,000 –150,000 node McAfee ePO network components**

In this figure, the 75,000–150,000 node organization example includes:

1. The McAfee ePO server
2. Separate SQL Server
3. Separate McAfee ePO Agent Handlers to coordinate McAfee Agent requests between themselves and the McAfee ePO server. Agent Handlers require constant communication back to the SQL database. They check the McAfee ePO server database work queue approximately every ten seconds to find what tasks they need to perform. Agent Handlers need a relatively high speed, low latency connection to the database. Agent Handlers reduce the workload on the McAfee ePO server by approximately 50 percent. We recommend one Agent Handler for each 50,000 nodes.

   > For organizations with 75,000 to 150,000 nodes, McAfee recommends that you install an Agent Handler close to the McAfee ePO server, for redundancy. This leaves the McAfee ePO server to manage agent-server communications if the Agent Handler fails.

4. Separate McAfee ePO Distributed Repositories to store and distribute important security content for your managed client systems.

75,000–150,000 node McAfee ePO server minimum hardware:

- 8 Quad-core processor CPUs (for example, 32 core processors)
- 32–64 GB of RAM
- 40–80 GB of hard drive space

75,000–150,000 node SQL Server minimum hardware:

- 16 Quad-core processor CPUs (for example, 64 core processors)
- 32–128 GB of RAM
- 1.0–2.0 TB of hard drive space

75,000–150,000 node Agent Handler minimum hardware:

- 4 Quad-core processor CPUs (for example, 16 core processors)
- 8 GB of RAM
- 40–80 GB of hard drive space

## Example 5 — 150,000+ nodes

You can manage an organization of more than 150,000 nodes with a single McAfee ePO server, separate SQL Server, separate Agent Handler, and properly placed repositories to update content and software to the agents.

For an organization of this size, use the highest performance hardware you can afford for your McAfee ePO SQL Server.

150,000+ node McAfee ePO server minimum hardware:

- 16 Quad-core processor CPUs (for example, 64 core processors)
- 64–128 GB of RAM
- 40–80 GB of hard drive space

150,000+ node SQL Server minimum hardware:

- 32+ Quad-core processor CPUs (for example, 128 core processors)
- 64–128 GB of RAM
- 1.0–2.0 TB of hard drive space

150,000+ node Agent Handler minimum hardware:

- 4 Quad-core processor CPUs (for example, 16 core processors)
- 8 GB of RAM
- 40–80 GB of hard drive space

> For an organization with more than 150,000 nodes, you must have at least one Agent Handler, installed at a remote site.

These are not upper limits for hardware. If you have the budget for additional hardware resources, McAfee recommends that you exceed these recommendations.

**See also**
*What repositories do* on page 107
*Planning your hard disk configuration* on page 25
*Using a SAN with your SQL database* on page 28
*Sharing the SQL database hardware* on page 25
*Server hardware requirements* on page 18

# Planning your hardware configuration

The physical hardware configuration you use for the McAfee ePO server and SQL Server determines the number of nodes these servers manage.

Previous versions of McAfee ePO easily managed up to 200,000 nodes using one McAfee ePO server with a separate SQL Server. But the latest versions of McAfee ePO have many more features and are much more robust, which affects the number of nodes they can manage efficiently. Now McAfee ePO can manage up to 50,000 nodes with basic server hardware and reasonable planning. Once you exceed 50,000 nodes, the way you configure your McAfee ePO server hardware becomes much more important to achieve the best possible performance.

Initially your managed node count determines your McAfee ePO server platform and the recommended hardware specifications. The node count helps you answer these questions:

- Can I install the McAfee ePO server and SQL Server on the same physical hardware?
- Can I use a virtual machine for McAfee ePO or the SQL Servers?
- Can McAfee ePO use an existing SQL Server running other databases for McAfee ePO?
- How do I partition my hard disk drives for the McAfee ePO server and SQL Server?

## Using one server

You must determine the number of nodes you want the McAfee ePO server and SQL Server to manage before you know if both servers can be installed on the same physical server.

Environments, with 5,000 or 10,000 nodes can have the McAfee ePO server and SQL Server installed on one physical server to save hardware, IT, and energy costs. This works if you do the following:

- Optimize your storage by using multiple dedicated drives for each application as your node count increases.
- Manage only the basic McAfee products, such as VirusScan Enterprise or Host Intrusion Prevention, not both.

If in the future you plan to manage more McAfee products and add many more nodes, split the one server into two physical servers:

- One for the McAfee ePO server
- One for the SQL Server

**See also**

*Planning your hard disk configuration* on page 25

## Installing your server in a virtual environment

You can run the McAfee ePO server on multiple versions of virtual environments, but if your node count gets too high you might experience slower disk performance.

To install the McAfee ePO server on a VM and solve this disk performance problem, you must:

- Dedicate physical disks to the McAfee ePO server in the VM.
- Assign priority for the CPUs to the McAfee ePO server.

With fewer than 10,000 nodes, you can also use an SQL Server database installed on a VM for the McAfee ePO server. If node count exceeds 10,000 nodes, the same disk performance bottleneck occurs.

## Sharing the SQL database hardware

You can install the McAfee ePO server SQL database on a shared SQL Server, unless you are managing a high number of nodes.

However, it is important to remember that the McAfee ePO server SQL database performs thousands of disk reads and writes every few seconds, which can negatively impact performance on an overutilized SQL Server.

You can share your existing fully clustered, redundant, and centrally managed SQL environment if:

- The shared SQL Server is not already overutilized.
- Your McAfee ePO server manages fewer than 25,000 nodes.
- Other SQL database functions do not cause spikes that could slow the McAfee ePO server SQL database reads and writes.

| Node count | McAfee ePO and SQL on one server | Use VM server | McAfee ePO DB on shared SQL Server |
|---|---|---|---|
| 100–5,000 | OK | Optional | Optional |
| 5,000–25,000 | Optional | Optional | Optional |
| 25,000–75,000 | Not recommended | Not recommended | Not recommended |
| 75,000 or more | No | No | No |

See What affects McAfee ePO performance on page 17 for specific examples of how the number of products installed, the number of nodes managed, and bandwidth affect your McAfee ePO server and SQL database hardware requirements.

# Planning your hard disk configuration

When configuring your McAfee ePO server hardware, the hard disk configuration is one of the most important factors for larger McAfee ePO environments.

Your McAfee ePO server processes thousands of events from multiple products, which must be written to the SQL database. When you use the McAfee ePO server to administer your network and to execute queries, McAfee ePO software accesses the SQL Server database for millions of events and thousands of nodes. These functions make disk configuration one of the most important factors for larger McAfee ePO server implementations.

The primary limiting factor when choosing your configuration is the cost of storage. Depending on your hardware budget, choose the best configuration to prepare for future growth, even though you might have only 5,000 nodes to manage currently with the McAfee ePO server. Choose the best and fastest configuration that you can afford.

### Example 1 — Fewer than 5,000 nodes

If you have fewer than 5,000 nodes to manage with the McAfee ePO server, disk configuration is rarely an issue. Use your normal procedure for configuring the disks on the servers. Typically assign individual disks to the:

- Operating system
- McAfee ePO software
- SQL database

If you are using RAID for redundancy, use RAID 1. The following example shows a typical disk configuration using one server.

McAfee does not recommend RAID 5 for redundancy. Our tests show that a RAID 10 server processes 27 percent more events per second and 19 percent more agent-server communications per second than the RAID 5 server when using the same hardware.

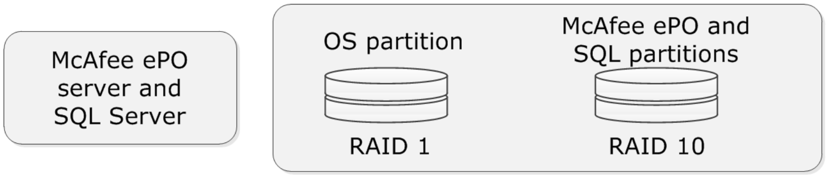

McAfee ePO server and SQL Server
OS partition
RAID 1
McAfee ePO and SQL partitions
RAID 10

**Figure 2-5 Disk partition and RAID configuration for fewer than 5,000 nodes**

## Example 2 — 5,000–10,000 nodes

If you have 5,000–10,000 nodes to manage with the McAfee ePO server, and you use one physical server for the McAfee ePO server and the SQL Server, and another physical server for the Agent Handler, you must provide a physical disk for the:

- Operating system
- McAfee ePO
- SQL database

For the Agent Handler server, use:

- RAID 1 for the operating system
- RAID 10 for the Agent Handler partition

McAfee recommends that you use RAID 1 and RAID 10 for this configuration, especially if you use one physical server for both the McAfee ePO server and the SQL Server. The following example shows this RAID disk configuration.

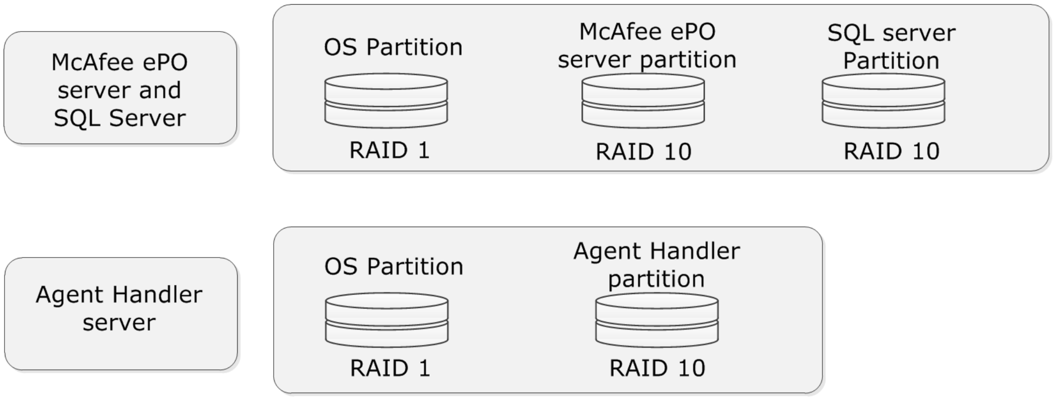


**Figure 2-6 Disk partition and RAID configuration for 5,000–10,000 nodes**

## Example 3 — 10,000–75,000 nodes

If you have 10,000-75,000 nodes to manage with the McAfee ePO server, use three separate servers. For the McAfee ePO server, use:

- RAID 1 for the operating system
- RAID 10 for the McAfee ePO application

For the Agent Handler server, use:

- RAID 1 for the operating system
- RAID 10 for the Agent Handler partition

For the SQL Server, use:

- RAID 1 for the operating system
- RAID 1 for the SQL transaction log partition (the LDF file)
- RAID 10 for the SQL database partition

> To manage an organization of this size with the McAfee ePO server, McAfee recommends that you use RAID 10 for the SQL Server.

The following example shows this RAID disk configuration.

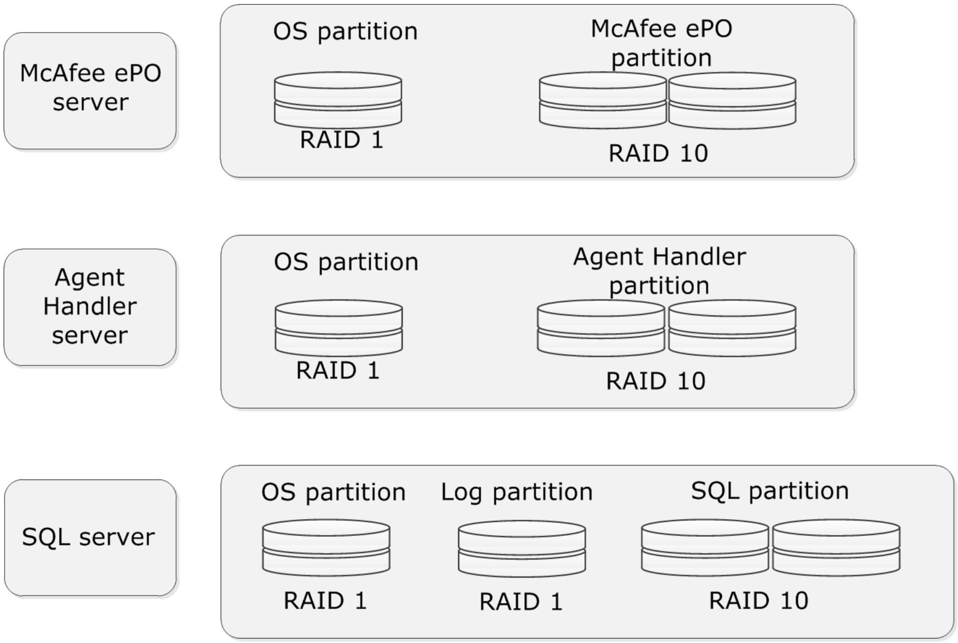


**Figure 2-7 Disk partition and RAID configuration for 10,000–75,000 nodes**

## Example 4 — More than 75,000 nodes

If you have more than 75,000 nodes to manage with the McAfee ePO server, use three separate servers. For the McAfee ePO server, use:

- RAID 1 for the operating system
- RAID 10 for the McAfee ePO application

For the Agent Handler server, use:

- RAID 1 for the operating system
- RAID 10 for the Agent Handler application

For the SQL Server, use:

- RAID 1 for the operating system
- RAID 1 for the SQL transaction log partition (the LDF file)

- RAID 1 for the Temp SQL database partition
- RAID 10 for the SQL database partition

To manage an organization of this size with the McAfee ePO server, McAfee recommends that you use RAID 10 for the SQL Server.

The following example shows this RAID disk configuration.

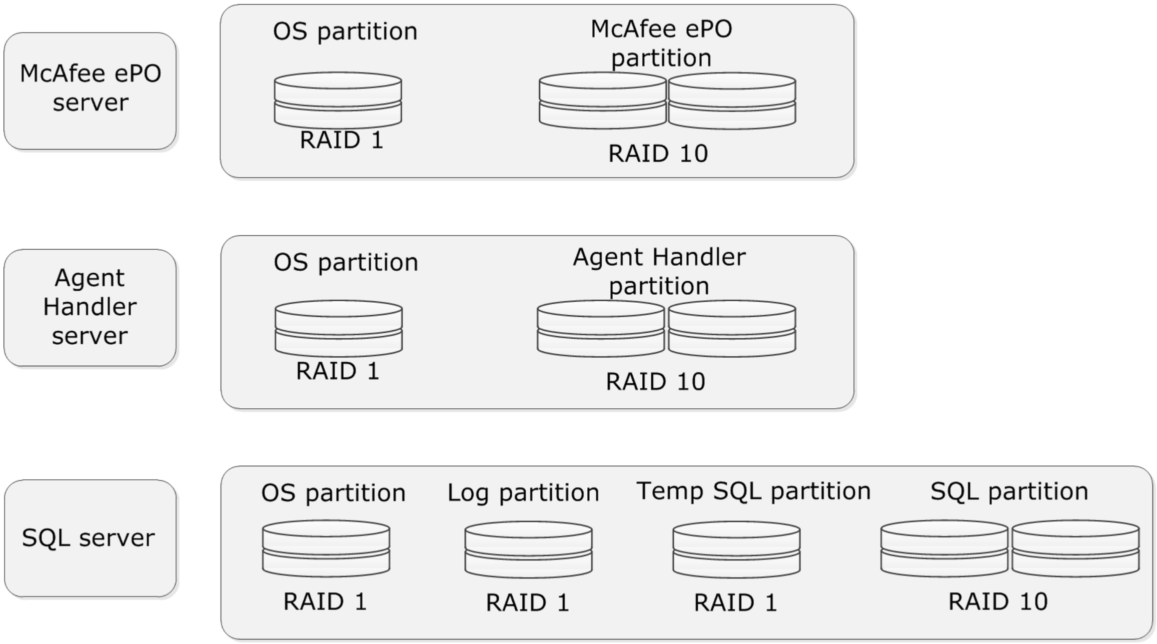


**Figure 2-8 Disk partition and RAID configuration for more than 75,000 nodes**

# Using a SAN with your SQL database

Storage area network (SAN) devices are the standard configuration for SQL databases that require back up and maintenance.

SAN storage is a valid method for storing your SQL database, but adds a potential layer of complexity to your SQL implementation that must understand.

A SAN engineer might maintain the SAN and not be familiar with McAfee ePO and its heavy I/O requirements. If you deploy the McAfee ePO server SQL database on a SAN, you must have your SAN engineer involved early in the process to help plan your architecture.

Many SANs are grouped into a generic classification known as *tiers*. The three tiers are:

- **Tier 1 SAN** — The most expensive, fastest, and redundant storage array. If you have 75,000 nodes or more, use a tier 1 SAN to store your SQL database.
- **Tier 2 SAN** — Used to store critical data that requires redundancy. This data is accessed without causing excessive transactions on the SAN.
- **Tier 3 SAN** — Used for databases that do not require much space or many I/O transactions

3

# Installing and upgrading McAfee ePO software

You can install the McAfee ePO software either as a first-time installation or as a recovery installation where your Microsoft SQL Server already includes a McAfee ePO configuration from a previous installation. If you are upgrading your McAfee ePO software, use the Upgrade Compatibility Utility.

Before installing your McAfee ePO server software, review the hardware requirements in the McAfee ePolicy Orchestrator Installation Guide and follow the preparation steps. Thorough planning and preparation can ensure a successful installation.

**Contents**

## Installing McAfee ePO

If you are installing McAfee ePO software for the first time, run the Setup.exe process and start configuring your server.

You don’t have to transfer any settings from an old McAfee ePO server to manage existing systems. See the McAfee ePolicy Orchestrator Installation Guide for details.

## Upgrading an existing McAfee ePO server

You can use two ways to upgrade an existing version of the McAfee ePO server. You can perform an existing McAfee ePO server upgrade, or perform a clean installation of the McAfee ePO server.

If you are upgrading McAfee ePO software version 4.6 32-bit operating system version to 5.1 64-bit operating system, use the Upgrade Compatibility Utility. See the McAfee ePolicy Orchestrator Installation Guide for details about 32-bit to 64-bit operating system conversion.

> The utility does not copy or move the existing McAfee ePO SQL database. See the Microsoft documentation for details about copying an existing database to a new database server.

See these KnowledgeBase articles for additional upgrade information:

- McAfee ePO 5.1 supported products, KB79169 lists product and Extension versions supported
- McAfee Agent 4.8.0, KB77534 backward compatible and supported McAfee Agent versions
- Supported Platforms, Environments and Operating Systems for Common Management Agent and McAfee Agent 4.x, KB51573

These sections list some of the advantages and disadvantages of upgrading your McAfee ePO server.

## Upgrade benefits

The advantages of upgrading an existing McAfee ePO server include:

- **You retain all your policies and client tasks** — You don't have to rebuild them and you can save time.
- **You retain your directory structure** — If you have invested a lot time building this structure an existing upgrade might be a good idea.
- **You don't have to transfer any agents to a new server** — Because nothing changes with an existing upgrade the upgrade is transparent to all your agents.

## Upgrade disadvantages

The disadvantages of upgrading your existing McAfee ePO server include:

- If your McAfee ePO server has been used for a long time, there might be certain issues you don't want to transfer to the new upgrade. For example, if you ran extensive SQL scripts or altered your database in any way outside of the normal operating procedures you might want start with a clean installation.
- Older policies might not still apply to your existing environment. Do not copy those policies during your existing upgrade.

> Assess your environments and policies periodically to confirm that they still apply to your environment.

## Upgrade tips

Use the Upgrade Compatibility Utility to upgrade your software from a 32-bit environment to 64-bit. The utility runs the Product Compatibility Check that determines if any of your installed McAfee ePO extensions are not compatible with the new upgrade. See the McAfee ePolicy Orchestrator Installation Guide for details about using the Upgrade Compatibility Utility.

Other tips to make sure that your existing upgrade is successful:

- Back up your infrastructure. For example, include your SQL database and any McAfee Agent keys. For detailed back upprocedures, see these KnowledgeBase articles: McAfee ePO server back up and disaster recovery procedure, KB66616, and McAfee ePO cluster back up and disaster recovery procedure, KB75497.
- Make any hardware changes or remove any repositories that you want to decommission. Make sure you remove the repositories from the Policy Catalog for the McAfee Agent.
- Make sure that your hardware and bandwidth meet the minimum requirements before upgrading.
- Confirm that you have the required software, such as the latest version of the McAfee Agent. Remove any unsupported software. For example, Rogue System Detection or System Compliance Profiler.

- Go through your users on the McAfee ePO server and remove any unneeded accounts.

  If an administrator account is removed, any server tasks created by that account are removed.

- Remove all unused policies.

- Remove any old client tasks you no longer use. For example, old deployment tasks or old patch installation tasks. Remove the task if it's not used.

- Validate your tree and remove any agents that have not communicated with the McAfee ePO server in 30 days. In addition, remove any shell systems that were imported into McAfee ePO from Active Directory.

  Shells are placeholders in the tree and do not actually have a McAfee Agent installed.

- Purge events that are not needed. Delete any events older than 60 days from this path:

  `C:\Program Files (x86)\McAfee\ePolicy Orchestrator\DB\Events\Debug\`

- Backup, reindex, and check your disk space on the SQL Server. Confirm that you have plenty of disk space for the SQL database and your SQL transaction log file is set to auto-grow. For a recommended maintenance plan for your McAfee ePO database using SQL Server Management, see KnowledgeBase article Recommended maintenance plan for McAfee ePO database using SQL Server Management Studio, KB67184.

- Remove old versions of McAfee product software that you are no longer using. For example, patches for older versions of products that are no longer used. See Version information for ePolicy Orchestrator, KB59938 for detailed version information.

  Replicate those patches to your distributed repositories before upgrading.

- Remove server tasks that are no longer used.

- Remove Automated Responses that are no longer used.

- Test your upgrade in a VM environment with a copy of your SQL database to make sure that the upgrade works smoothly. For example, you might want to installation the McAfee ePO server software on a VM, link it to a copy of your SQL database, and confirm the installation works.

- Validate all your settings, policies, policy assignments, and client tasks to confirm that they are in place after the upgrade.

See these KnowledgeBase articles for additional information:

- McAfee ePO 5.1 installation and patch upgrade checklist for known issues, KB76739

- Supported Platforms, Environments and Operating Systems for Common Management Agent and McAfee Agent 4.x, KB51573

- Version information for McAfee Agent 4.8.0, KB77534

- Version Information for McAfee Agent 4.6, KB72221

## Using product version numbers

The product version numbers help you determine what software products, new patches, and hotfixes to install.

As with all software products, new patches and hotfixes are released regularly to update bugs and add new features. If you are a new McAfee user, it might help to understand the McAfee product version numbering system.

Using McAfee ePO version "5.1.0.1160" as an example, the number:

- 5. — "5" indicates a major release version
- 5.1. — The "1" indicates a minor version, with "1" indicating it is the second releases of a version 5 product.
- 5.1.0. — The "0" indicates the patch number; in this case, it means no patch.
- 5.1.0.1160 — These four numbers, "1160", indicate the build number.

### McAfee ePO server and McAfee Agent revisions

The two most relevant products for this document are the McAfee ePO server and the McAfee Agent. Many users assume that the McAfee Agent version number must match the McAfee ePO server version number.

The agent and server versions are disjointed and do not have to be on the same major version. For example, the McAfee ePO server 5.1 works fine with McAfee Agent 4.6 or 4.8.

> ⓘ There are limits to how far back the McAfee ePO server supports agents and those limits are clearly defined in the McAfee ePO KnowledgeBase articles for the products.

McAfee recommends that you use the latest McAfee Agent software available.

## Determining the best upgrade strategy

When upgrading your McAfee ePO server and agent, you should upgrade the McAfee ePO server software first.

Upgrading your McAfee ePO server software first makes your backend architecture ready to speak to your newly upgraded agents, when that occurs. When you upgrade the McAfee ePO server, you affect only one device, your McAfee ePO server. When you upgrade the agents, you affect all devices in your environment.

# Moving the server

If you must move your McAfee ePO server from one physical server to another, you can maintain all your settings.

For example, you might want to move your McAfee ePO server configuration to new server hardware if the existing hardware is old, has failed, or is out of warranty. You can use the McAfee ePO Disaster Recovery feature or manually move your McAfee ePO server settings.

> ⓘ The Upgrade Compatibility Utility is used primarily to create a file to move a 32-bit McAfee ePO configuration to new 64-bit server hardware. This utility does not copy or move the existing McAfee ePO SQL database. See the McAfee ePolicy Orchestrator Installation Guide for Upgrade Compatibility Utility details.

### Using the McAfee ePO Disaster Recovery feature

You can use the McAfee ePO Disaster Recovery feature to automatically move your McAfee ePO server settings from one physical server to another. See the McAfee ePolicy Orchestrator Product Guide for Disaster Recovery details.

### Manually moving your McAfee ePO server

The backup and disaster recovery process for McAfee ePO servers is described in KnowledgeBase article McAfee ePO server back upand disaster recovery procedure, KB66616.

To manually move your McAfee ePO server settings from one physical server to another, make sure that you back up the following:

- The SQL database. Before you do anything, make sure that you back up your McAfee ePO server SQL database in case something goes wrong. The database stores everything about McAfee ePO, for example, your tree structure, product policies, administrators, events, and server settings.
- Back up these items that are outside your database:

  > Following is the default 32-bit installation path. However, your installation might differ (for example, the default 64-bit installation path is `C:\Program Files(x86)\McAfee\ePolicy Orchestrator`).

  - The McAfee Agent keys that secure the communication between the server and all your agents. To find the keys, click **Menu** | **Configuration** | **Server Settings** and select **Security Keys**. To export the keys, click **Edit** and export the keys to a file.
  - The Software checked in to the Master Repository are at this path, by default: `C:\Program Files\McAfee\ePolicy Orchestrator\DB\Software\Current\`
  - The Extensions to manage all your product policies are at this path, by default: `C:\Program Files\McAfee\ePolicy Orchestrator\Server\extensions\`
  - The software extension information files, are at this path, by default: `C:\Program Files\McAfee\ePolicy Orchestrator\Server\extensions\`
  - The Secure Sockets Layer (SSL) certificates are at this path, by default: `C:\Program Files\McAfee\ePolicy Orchestrator\Apache2\conf\`
  - The Server settings, such as communication ports, are at these paths, by default:
    - `C:\Program Files (x86)\McAfee\ePolicy Orchestrator\Apache2\conf\`
    - `C:\Program Files (x86)\McAfee\ePolicy Orchestrator\Server\conf\`

After you have backed up all this information, follow the installation instructions in the McAfee ePolicy Orchestrator Installation Guide as if it were a brand new server. You then have a clean database that you replace with your original database, using your original settings. Restore the original SQL database, McAfee Agent keys, and SSL certificates.

When you upgrade your McAfee ePO server from one physical server to another, make sure that your new server has the same DNS name and IP address as the old server. Using the same IP address is the ideal situation and reduces any potential problems.

However, you might change the DNS name or IP address. For example, if you are changing the IP address scheme, a new IP address might be required. Or, if you change the DNS name and keep the old IP address, you must regenerate the local SSL certificates. Once your database has been restored, you can turn off your old McAfee ePO server, then all agents automatically start communicating with the new McAfee ePO server.

It's important to understand how the agents find the McAfee ePO server, especially if you are moving the server. The McAfee Agent tries to connect to the McAfee ePO server using this sequence:

1. IP address
2. NetBIOS name
3. Fully qualified DNS name

If you move the McAfee ePO server or change its IP address, the McAfee Agent attempts to query the DNS to get the IP address for the DNS name. If you are going to move your McAfee ePO server, make sure that you have good DNS name resolution in your environment.

**See also**

*Use Disaster Recovery* on page 197

# Moving agents between servers

If you must create a database, you can copy the settings from the old database and move agents to the new database.

Moving your agents from the old McAfee ePO server to the new McAfee ePO server is a compromise. You can copy your existing McAfee ePO SQL database to your new McAfee ePO server and have the McAfee Agent systems connect to the new server to populate the new, clean, database.

Now, using a combination of the McAfee ePO Disaster Recovery and the Transfer Systems features, you can quickly and easily move your existing configuration from your existing server hardware to your new server. See the McAfee ePolicy Orchestrator Product Guide for Disaster Recovery details

See the following KnowledgeBase articles for detailed backup and disaster recovery procedures:

- McAfee ePO server backup and disaster recovery procedure, KB66616
- McAfee ePO server Cluster Backup and Disaster Recovery procedure, KB75497

### Exporting and importing the ASSC keys

After you install all product extensions, you must export the agent-server secure communication (ASSC) keys from the old server to the new server before moving your clients to the new McAfee ePO server. See the McAfee ePolicy Orchestrator Product Guide for detailed agent-server secure communication key export and import instructions.

## Using the Transfer Systems task

Use the Transfer Systems task to move agents from the old McAfee ePO server to the new server.

**Before you begin**

You must configure a registered server before you can use the Transfer Systems feature. See how to set up registered servers in the McAfee ePolicy Orchestrator Product Guide for details.

The Transfer Systems task gives the existing McAfee Agent a new Sitelist.xml file that points to the new McAfee ePO server. The old and the new McAfee ePO servers must both be running McAfee ePO version 4.6 or later.

The Transfer Systems task lets you:

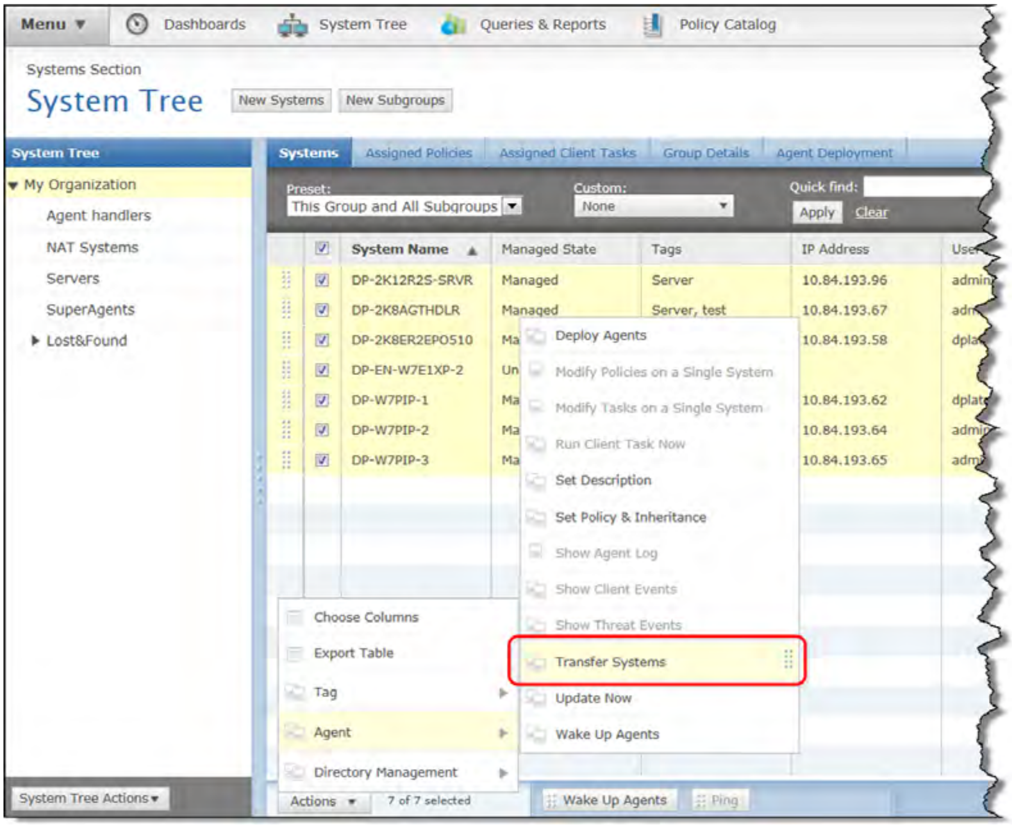
- Stage and thoroughly plan your McAfee Agent moves so you can test their settings during an appropriate Change Control window.
- Test your changes on a development McAfee ePO server before rolling out the changes to the production environment. For example, you can change your test McAfee ePO server and move a group of live production agents to your test server to see the results. When done, you can easily transfer those agents back to the original production McAfee ePO server.

On the existing McAfee ePO server, configure the new server as a registered server. See the McAfee ePolicy Orchestrator Product Guide for details.

## Task

For option definitions, click **?** in the interface.

1. On the old McAfee ePO server, configure the new server as a registered server. See the McAfee ePolicy Orchestrator Product Guide for details.
2. On the old McAfee ePO server, click **Menu** | **Systems Section** | **System Tree** and then the **Systems** tab to open a list of systems.
3. Select the systems to move to the new McAfee ePO server and click **Actions** | **Agent** | **Transfer Systems**.



| ☑ | System Name ▲ | Managed State | Tags | IP Address | Use |
|---|---|---|---|---|---|
| ☑ | DP-2K12R2S-SRVR | Managed | Server | 10.84.193.96 | admin |
| ☑ | DP-2K8AGTHDLR | Managed | Server, test | 10.84.193.67 | adn |
| ☑ | DP-2K8ER2EPO510 | Ma | | 10.84.193.58 | dpla |
| ☑ | DP-EN-W7E1XP-2 | Un | | | |
| ☑ | DP-W7PIP-1 | Ma | | 10.84.193.62 | dplat |
| ☑ | DP-W7PIP-2 | Ma | | 10.84.193.64 | admi |
| ☑ | DP-W7PIP-3 | Ma | | 10.84.193.65 | adm |

**Figure 3-1 System Tree Transfer Systems example**

4. From the Transfer Systems dialog box, select the server from the list and click **OK**.

Once a managed system is selected for transfer, two agent-server communications must occur before the system is displayed in the System Tree of the target server. The length of time required to complete both agent-server communications depends on your configuration. The default agent-server communication interval is one hour.

4

# Using the McAfee Agent and your System Tree

The McAfee Agent is the liaison between all point-products installed on your managed systems and the McAfee ePO server. The System Tree is the logical representation of your managed environment.

**Contents**

## How the McAfee Agent works

The McAfee Agent is not a security product on its own; instead it communicates to all McAfee and partner security products and passes the appropriate information to and from the McAfee ePO server.

The McAfee Agent version does not have to match the McAfee ePO version. For example, you can use McAfee Agent 4.8 with McAfee ePO 5.1.

The core McAfee Agent functionality includes:

- Handling all communication to and from the McAfee ePO server and passing that data to the endpoint products
  - Pulling all product policies from the McAfee ePO server and assigning policies to the appropriate products that are installed on the endpoint clients
  - Pulling all client tasks from the McAfee ePO server and passing them to the appropriate products
- Deploying content such as anti-virus signatures, auditing checks, and engines
- Deploying new product upgrades, new products, patches, and hotfixes
- Upgrading itself silently when a new McAfee Agent is released

Once a McAfee Agent is installed on a system, you can use it to update most products on that client.

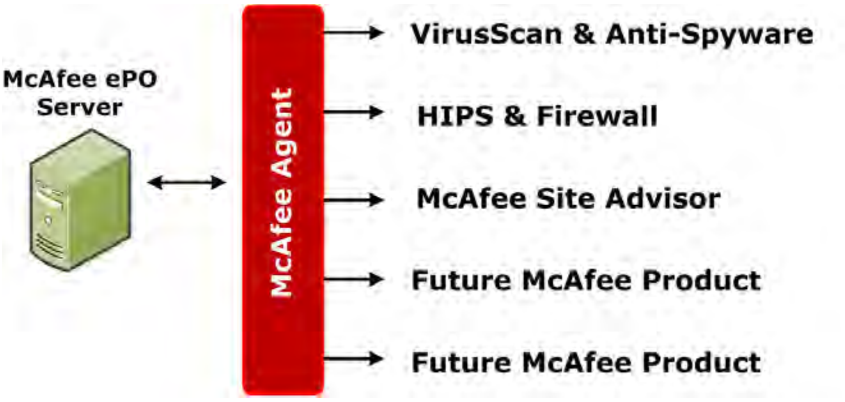


**Figure 4-1 One McAfee Agent communicates with many products**

## McAfee Agent modularity

The modular design of the McAfee Agent allows you to add new security offerings to your environment as your needs change, using the same McAfee Agent framework. McAfee has built a standard of how policies, events, and tasks are passed to endpoint products. You never have to worry about communication or which ports to open when you add a new product such as Host Data Loss Protection to your endpoint. The McAfee Agent controls all these items. The advantages to this modular architecture are:

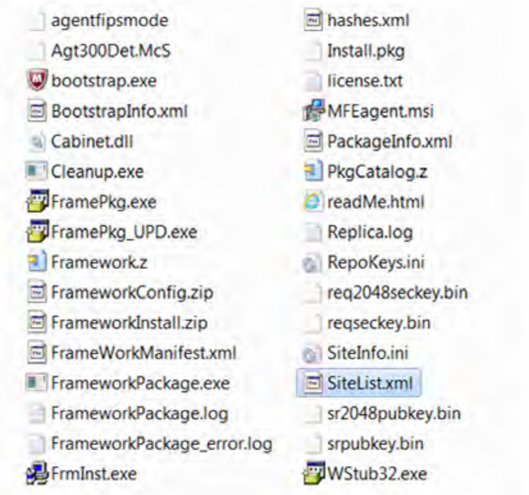
- One component provides communication back to the server instead of multiple solutions with their own proprietary communication language.
- You can choose which products fit your organization instead of being dictated to by your security vendor.
- Because the McAfee ePO server controls the process, the patch process is consistent across all products.
- You can add new products as they are released by McAfee and its partners.
- You can leverage the same McAfee Agent for partner products instead of adding more overhead.

## Inside the McAfee Agent file

If you look inside the installation directory where the McAfee Agent executable file is installed, you can see what makes it unique.

By default, you can find the McAfee Agent executable file at this path on your McAfee ePO server.

```
C:\Program Files (x86)\McAfee\ePolicy Orchestrator\DB\Software\Current
\EPOAGENT3000\Install\0409\
```



agentfipsmode
Agt300Det.McS
bootstrap.exe
BootstrapInfo.xml
Cabinet.dll
Cleanup.exe
FramePkg.exe
FramePkg_UPD.exe
Framework.z
FrameworkConfig.zip
FrameworkInstall.zip
FrameWorkManifest.xml
FrameworkPackage.exe
FrameworkPackage.log
FrameworkPackage_error.log
FrmInst.exe
hashes.xml
Install.pkg
license.txt
MFEagent.msi
PackageInfo.xml
PkgCatalog.z
readMe.html
Replica.log
RepoKeys.ini
req2048seckey.bin
reqseckey.bin
SiteInfo.ini
SiteList.xml
sr2048pubkey.bin
srpubkey.bin
WStub32.exe

**Figure 4-2 McAfee Agent internal file structure**

Your custom McAfee Agent executable file has the communication keys for your specific McAfee ePO server and a Sitelist.xml file. Without these keys the agents cannot talk to your specific McAfee ePO server. The Sitelist.xml file tells all your agents how to find the McAfee ePO server using the IP address and DNS name. This file becomes outdated if you rename your McAfee ePO server or give it a new IP address.

If you have multiple McAfee ePO servers you will have multiple unique McAfee Agent files designed to communicate with the server where the McAfee Agent was created.

### Keep the McAfee Agent file up to date

It is important to download the latest McAfee Agent file and give it to the appropriate teams so they have the latest McAfee Agent file version for new deployments. Make sure that you know who has the McAfee Agent executable in your environment and always control it by choosing a central share that you update every time you make changes to your McAfee Agent.

If you gave this custom McAfee Agent to your desktop team a year ago, it is probably outdated. It becomes outdated if you have made changes to your McAfee ePO server such as rebuilding it with a new IP address, or checked in a newer version of the McAfee Agent into your server.

## Deploying agents

The McAfee Agent is a 5-MB executable file that you can execute manually or more commonly deploy on a larger scale to hundreds or thousands of nodes.

The McAfee Agent can be deployed to your client systems using any of these methods:

- An Agent Deployment URL or McAfee Smart installer.
- A logon script.
- An image that includes the McAfee Agent.
- Manual execution.

- The McAfee ePO server.
- Third-party tools.

See the McAfee Agent Product Guide for details about these deployment methods.

**Tasks**

- *Creating the McAfee Agent file* on page 40
  You must use the specific McAfee Agent executable file obtained from the McAfee ePO server in your environment.
- *Deploy the McAfee Agent using a URL* on page 44
  You can create a client-side McAfee Agent download URL that users can use to download and install the McAfee Agent on the managed system.

## Creating the McAfee Agent file

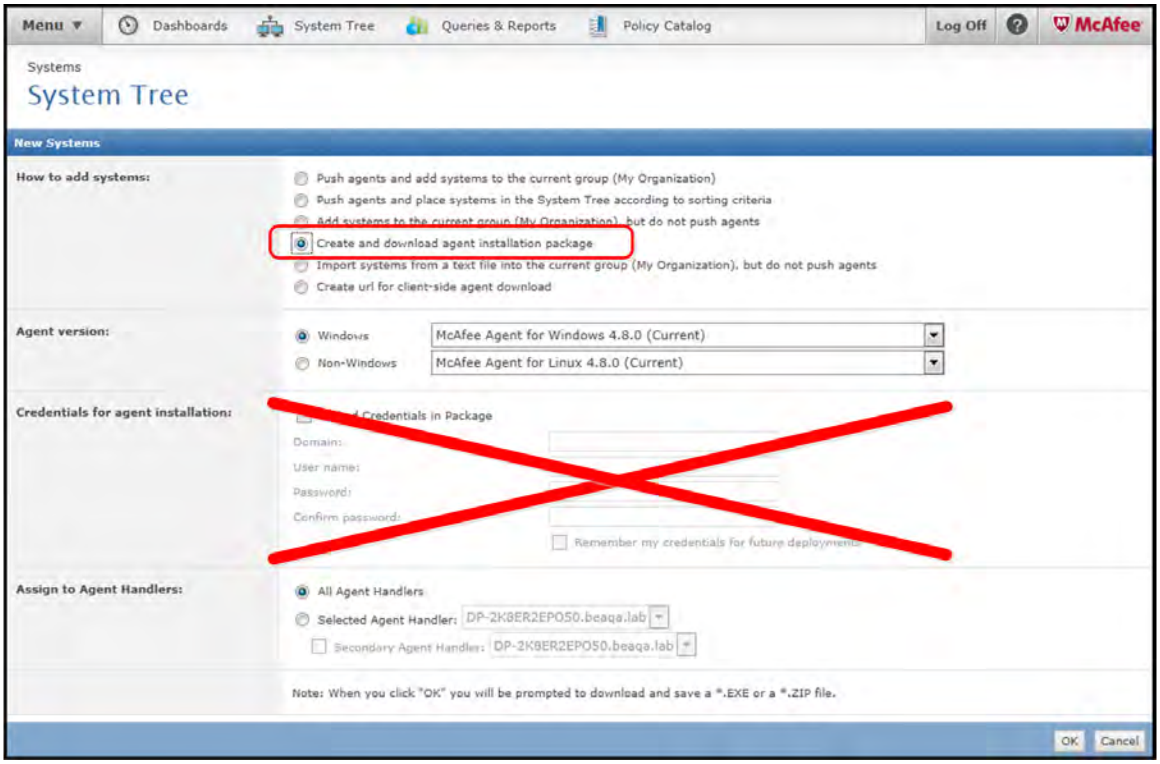
You must use the specific McAfee Agent executable file obtained from the McAfee ePO server in your environment.

Each agent is created dynamically during the initial installation of your McAfee ePO server. There are a few things inside your agent executable that are unique to your environment, which is why the agent can only be obtained from your organization's McAfee ePO server. You cannot download a blank McAfee Agent from the McAfee download site and deploy it.

### Task

For option definitions, click **?** in the interface.

1. Click **Menu** | **System** | **System Tree**, and from the System Tree page, click **New Systems**.
2. From the New Systems dialog box, click **Create and download agent installation package**, then click **OK**.



Systems

System Tree

New Systems

How to add systems:

○ Push agents and add systems to the current group (My Organization)
○ Push agents and place systems in the System Tree according to sorting criteria
○ Add systems to the current group (My Organization), but do not push agents
● Create and download agent installation package
○ Import systems from a text file into the current group (My Organization), but do not push agents
○ Create url for client-side agent download

Agent version:

● Windows — McAfee Agent for Windows 4.8.0 (Current)
○ Non-Windows — McAfee Agent for Linux 4.8.0 (Current)

Credentials for agent installation:

☐ Embed Credentials in Package
Domain:
User name:
Password:
Confirm password:
☐ Remember my credentials for future deployments

Assign to Agent Handlers:

● All Agent Handlers
○ Selected Agent Handler: DP-2K8ER2EPO50.beaqa.lab
☐ Secondary Agent Handler: DP-2K8ER2EPO50.beaqa.lab

Note: When you click "OK" you will be prompted to download and save a *.EXE or a *.ZIP file.

**Figure 4-3 Create agent file from the System Tree**

> It's a security risk to embed credentials in the McAfee Agent binary. Don't use the Credentials for your agent installation fields.

3. From the **Download File** dialog box, save the files to a local system.

> The default name of the McAfee Agent executable file is `FramePkg.exe`.

Now your McAfee Agent file, specifically created for your McAfee ePO server, is ready to deploy.

## Deploying agents from the McAfee ePO server

The quick and easy way to deploy the McAfee Agent is directly from the McAfee ePO server.

This method works well if you have a smaller environment and good control over the environment with the appropriate administrator rights. You can also solve situations where a few agents need to be deployed to new systems on the network. See the McAfee Agent Product Guide for details about deploying agents from the McAfee ePO server.

> Do not use the **Force installation over existing version** parameter when installing McAfee Agents from the McAfee ePO server. This parameter is intended for agent downgrades and troubleshooting.

### Troubleshooting McAfee Agent deployment

The McAfee ePO server requires local administrator rights to deploy agents remotely. In addition, the system you are deploying to must have:

- Admin$ share enabled
- NetBIOS enabled
- No firewall blocking inbound communications

An easy way to troubleshoot the agent deployment is by attempting to connect to the potential agent from the McAfee ePO server itself. To test the connection use the Microsoft Windows Run prompt and type:

```
\\<system_name>\admin$
```

Where "<system_name>" is the name of the system being tested.

If you can connect to the share using credentials, you know the McAfee ePO server can deploy an agent to the target system. If you cannot open this share, there is no way the McAfee ePO server can deploy an agent remotely.

Failure to connect to the target system is usually caused by incorrect credentials or a firewall that is blocking NetBIOS communication. Confirm that you have the appropriate rights on the target system before trying to deploy the agent from the McAfee ePO server.

See Environmental requirements for agent deployment from the ePO server, KB56386, for detailed McAfee ePO troubleshooting procedures.

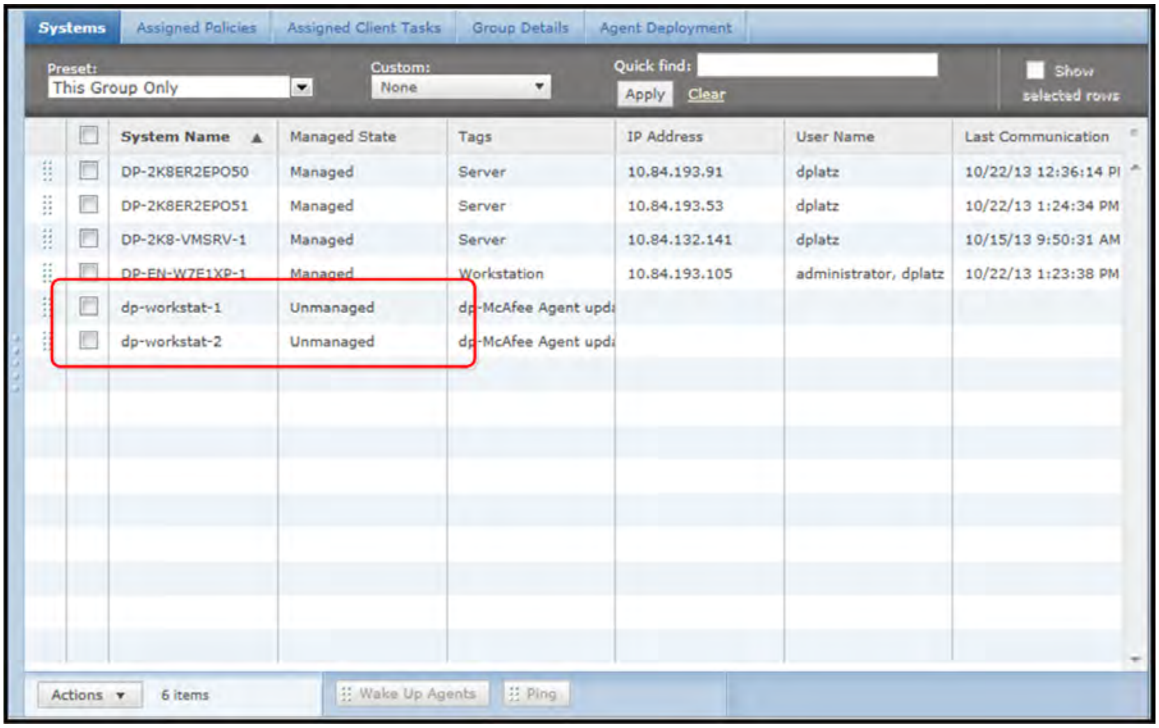
## Using the Active Directory to synchronize McAfee Agent deployment

You can use deployment from the McAfee ePO server on its own or with Active Directory (AD) synchronization.

McAfee ePO can import your systems from AD and subsequently push agents from the McAfee ePO server using the remote deployment functionality. Use server tasks to run remote deployment at a specific interval, such as once a day. This process requires the following:

- The systems in your AD tree must be well maintained. A well maintained AD is not always the case in many larger organizations. Place systems into the appropriate containers in AD for McAfee ePO to properly mirror your AD structure.
- You must have the proper credentials, admin$ share enabled, and no local firewall blocking the NetBIOS ports on the destination client.
- The target system must be turned on. Just because the system exists in AD does not mean it is turned on and active on your network.

Agent deployment from the McAfee ePO server works well as long you have a well maintained AD structure. If not, you will end up with excessive shell systems, or placeholders, in your System Tree. These shells are systems that have been imported from your AD server but have never received a McAfee Agent. The following figure is an example of shell systems without agents installed.



Preset: This Group Only
Custom: None

| System Name | Managed State | Tags | IP Address | User Name | Last Communication |
|---|---|---|---|---|---|
| DP-2K8ER2EPO50 | Managed | Server | 10.84.193.91 | dplatz | 10/22/13 12:36:14 PI |
| DP-2K8ER2EPO51 | Managed | Server | 10.84.193.53 | dplatz | 10/22/13 1:24:34 PM |
| DP-2K8-VMSRV-1 | Managed | Server | 10.84.132.141 | dplatz | 10/15/13 9:50:31 AM |
| DP-EN-W7E1XP-1 | Managed | Workstation | 10.84.193.105 | administrator, dplatz | 10/22/13 1:23:38 PM |
| dp-workstat-1 | Unmanaged | dp-McAfee Agent upd: | | | |
| dp-workstat-2 | Unmanaged | dp-McAfee Agent upd: | | | |

6 items

**Figure 4-4 System Tree systems list showing shell systems**

Shell systems appear in this figure with "Unmanaged" in the Managed State column.

Make sure that your environment is properly covered with agents to avoid these shell systems. These shell systems cause the following problems:

- They leave your System Tree cluttered and unorganized.
- They skew your reports and queries because they are only placeholders for systems, not systems that are actively talking to the McAfee ePO server.

You can filter out these shell systems in your reports, but it is much better to make sure that your environment is properly covered with McAfee Agents.

Delete these shell systems using a McAfee ePO server task on a regular basis.

## Deploy the McAfee Agent using a URL

You can create a client-side McAfee Agent download URL that users can use to download and install the McAfee Agent on the managed system.

### Task

1. Click **Menu** | **Systems Section** | **System Tree** and click the **Agent Deployment** tab.

2. From the **Actions** menu, click **Create agent deployment Url**.

3. Specify the **URL name**, the **Agent version**, and whether the URL applies to all Agent Handlers, or only specific Agent Handlers.

   When a user opens the URL, they are prompted to download or run the McAfee Agent installer. The installation executable can also be saved and then included in a log-on script. For more details about creating URLs for McAfee Agent deployment, see the McAfee Agent Product Guide.

## Adding the McAfee Agent to your image

Adding the McAfee Agent during the imaging process is a good McAfee ePO compliance strategy. It makes sure that all your systems get a McAfee Agent installed.

It requires planning and communication with your build team to obtain complete McAfee ePO compliance. This communication and planning ensures:

- A McAfee Agent is part of every system from the beginning.
- Any required McAfee product and associated policy is pulled from the McAfee ePO server by the McAfee Agent on your systems.
- Maximum security coverage for all systems in your environment.

There are two options when making the McAfee Agent part of your build process:

- **Option 1** — Include the McAfee Agent in your Windows image before freezing or finalizing the image.

  ! Make sure that you delete the McAfee Agent GUID before freezing the image if you choose option 1.

- **Option 2** — Run the McAfee Agent executable after your image is created using a repeatable script.

Both of these options install the McAfee Agent on the managed systems.

You can install all endpoint products on your managed systems by:

- Letting the McAfee Agent automatically call into the McAfee ePO server within 10 minutes and receive whatever policy and products are dictated by McAfee ePO.
- Making the endpoint products part of your build process and include them in the original image.

> See the McAfee Agent Product Guide to install the McAfee Agent on a non-persistent virtual image, or in Virtual Desktop Infrastructure (VDI) mode.

Here are some pointers to help you decide which option to use:

- The initial pull of multiple McAfee endpoint products can take a lot of bandwidth. If you have bandwidth constraints, make the products part of your original image.
- Make sure the endpoint products are part of your imaging process, if your build process occurs on a network where your imaged systems don't have connectivity to the McAfee ePO server.
- Once you install the McAfee Agent on a client it takes several more minutes to download, install, and update the VirusScan Enterprise product using a client task. This lag occurs even though the first agent-server communication occurs almost immediately. If timing is a concern make the McAfee products part of your image. This avoids the 15 minutes or 20 minutes wait for the products to install,

### Confirm that you deleted the McAfee Agent GUID before freezing the image

If you choose option 1, *Include the McAfee Agent in your Windows image*, make sure you reset the McAfee Agent global unique identifier (GUID). This causes the systems to not appear in the System Tree.

Make sure that you delete the McAfee Agent GUID before freezing the image when you make the McAfee Agent part of your image. If this registry key is not deleted, all systems with this same image use the same GUID and causes problems in your environment. See the McAfee Agent Product Guide.

Failure to delete the McAfee Agent GUID from the registry before finalizing your image can be difficult to manage in larger environments. There might be several imaging teams involved or an outsourcing organization might be building the images. Make sure that your imaging teams understand how to reset the McAfee Agent GUIDs if the computers are not displayed in the McAfee ePO directory. See KnowledgeBase article How to reset the agent GUID if computers are not displayed in the McAfee ePO directory, KB56086 for details.

**See also**

*Find systems with the same GUID* on page 169

## Deploying the McAfee Agent using third-party tools

You can deploy the McAfee Agent using a third-party tool that you already use for patches and new product deployments.

Using third-party tools is not a requirement, but your organization might have strict policies that dictate how products are deployed for consistency and change control reasons. Some common deployment tools include:

- Microsoft SCCM (formerly known as SMS)
- IBM Tivoli
- Novell Zenworks
- BMC Client Automation (formerly Marimba)
- Simple logon scripts

The process used to deploy the McAfee Agent for the first time using these third-party tools is straightforward. See the McAfee Agent Product Guide for details.

The McAfee Agent file, named FramePkg.exe, has several installation switches. Configure the McAfee Agent to install itself, at a minimum. Optionally, you can use the /s switch to hide the installation GUI from the user. Following is an example of this command:

```
FramePkg.exe /install=agent /s
```

# What the System Tree does

The System Tree is the logical representation of your managed network within the McAfee ePO console.

Your System Tree dictates these items:

- How your policies for different products are inherited
- How your client tasks are inherited
- Which groups your systems go into
- Which permissions your administrators have to access and change the groups in the System Tree

If you are creating your System Tree for the first time, these are the primary options available for organizing your systems dynamically:

- Using Active Directory (AD) synchronization
- Dynamically sorting your systems

> AD synchronization can be used with dynamic System Tree sorting, but ideally try to pick one or the other. There can be some confusion and conflicts when using both.

See the McAfee ePolicy Orchestrator Product Guide for System Tree details.

## Using Active Directory synchronization

You can use Active Directory synchronization to pull your systems and organizational units from your AD structure and mirror them in McAfee ePO.

Active Directory is an ideal option if your AD structure is well organized for you by business unit, system type, and others. Unfortunately, AD structure is not always well organized.

## Sorting your systems dynamically

You can dynamically sort your systems into your McAfee ePO System Tree using a combination of system criteria and other elements into their appropriate System Tree groups.

This requires that you create some basic groups for your tree structure. For smaller organizations, your System Tree might not be that complex and contain only a few groups. For larger organizations, you could create the following building blocks and assess the advantages and disadvantages of a few designs:

- **GEO** — Geographic location
- **NET** — Network location
- **BU** — Business unit
- **SBU** — Sub-business unit
- **FUNC** — Function of the system (web, SQL, app server)
- **CHS** — Chassis (server, workstation, laptop)

After you decide on the basic building blocks for groups in the System Tree, you must determine which building blocks to use and in which order based on the following factors:

- **Policy Assignment** — Will you have many different custom product policies to assign to groups based on chassis or function? Will certain business units require their own custom product policy?
- **Network Topology** — Do you have sensitive WANs in your organization that can never risk being saturated by a content update? Or do you only have major locations and this is not a concern?

- **Client Task Assignment** — When it comes time to create a client task, such as an on-demand scan, will you need to do it at a group level, such as a business unit, or system type, like a web server?
- **Content Distribution** — Will you have an agent policy that specifies certain groups must go to a specific repository for content?
- **Operational Controls** — Will you need specific rights delegated to your McAfee ePO administrators that will allow them to administer specific locations in the tree?
- **Queries** — Will you need many options when filtering your queries to return results from a specific group in the System Tree? This is another factor that might be important when designing your System Tree.

After you choose the basics for your tree structure, create a few sample System Trees and look at the pros and cons of each design. There is no right way or wrong way to build your System Tree, just pluses and minuses depending on what you choose. Following are a few of the most common System Tree designs users tend to use:

- GEO -> CHS -> FUNC
- NET -> CHS -> FUNC
- GEO -> BU -> FUNC

This is an example of GEO -> CHS -> FUNC, or geographic location, chassis, and function.

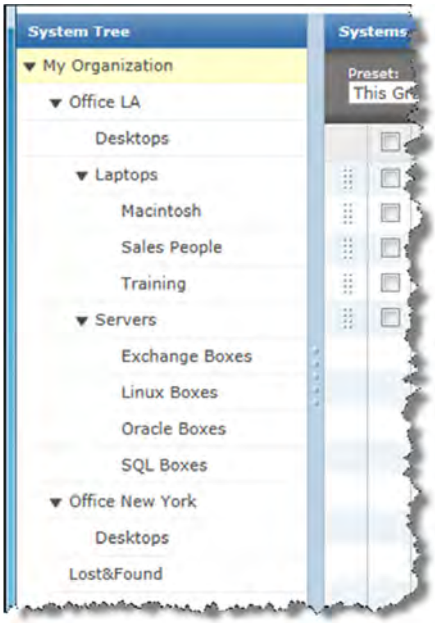


**Figure 4-5 System Tree groups configured by geographic location, chassis, and function**

# Managing and reporting

Keeping your McAfee products updated with the latest security content and reporting on threats and status are essential parts of protecting your organization's systems.

# 5

# Managing endpoint security with policies and packages

Policies are the settings that govern each product on the endpoint. The McAfee Agent can deploy these package binaries to your endpoints.

Policies include the settings for any supported products from VirusScan Enterprise to McAfee Endpoint Encryption. These policies include every checkbox and setting that dictates what the endpoint product does on each one of your systems.

Deployment packages are the actual binaries deployed by the McAfee Agent to your endpoint systems. These packages include deploying a full product, such as, a new version of VirusScan Enterprise or SiteAdvisor Enterprise to your endpoint systems. Policies and packages **do not** rely on each other and are not connected. In other words, just because you want to manage VirusScan Enterprise policies with McAfee ePO does not mean that you have to *deploy* VirusScan Enterprise with McAfee ePO.

**Contents**

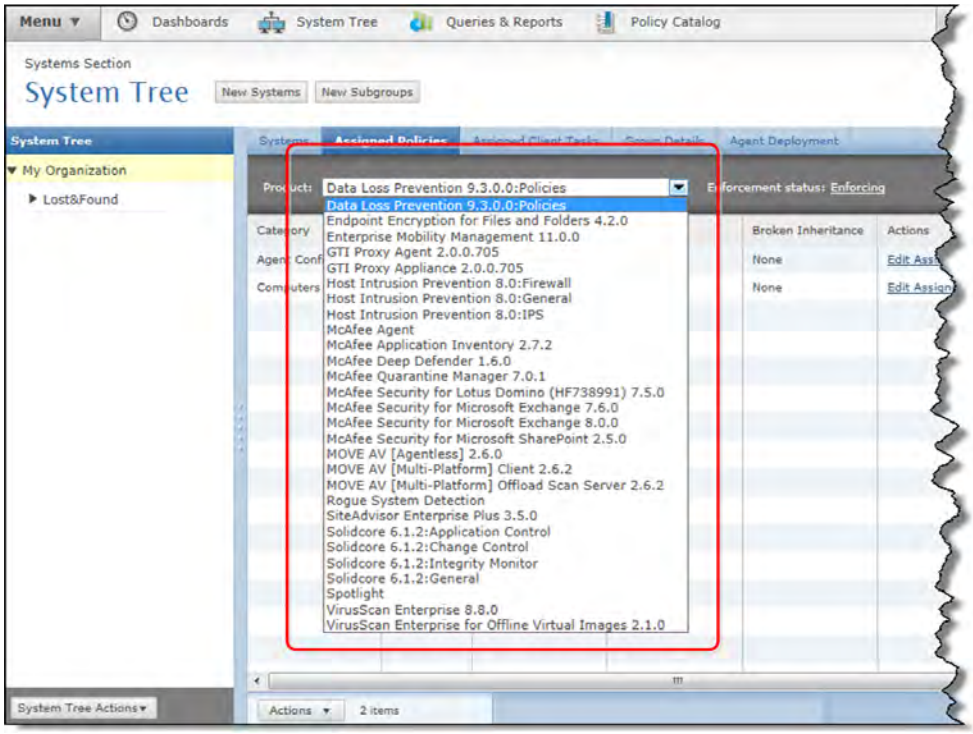
## Managing policies

A policy is a collection of settings that you create and configure, then enforce. Policies ensure that managed security software products are configured and perform accordingly.

McAfee ePO manages policies for all point-products that the McAfee Agent can manage.

> Whenever you change a policy, configuration, client or server task, automatic response, or report, export the settings prior to and after the change. For detailed instructions about exporting objects, see the McAfee ePolicy Orchestrator Product Guide.

This example shows some of the products that the McAfee ePO server can manage. New products are added as McAfee expands its solution portfolio.



Product: Data Loss Prevention 9.3.0.0:Policies
Enforcement status: Enforcing

Data Loss Prevention 9.3.0.0:Policies
Endpoint Encryption for Files and Folders 4.2.0
Enterprise Mobility Management 11.0.0
GTI Proxy Agent 2.0.0.705
GTI Proxy Appliance 2.0.0.705
Host Intrusion Prevention 8.0:Firewall
Host Intrusion Prevention 8.0:General
Host Intrusion Prevention 8.0:IPS
McAfee Agent
McAfee Application Inventory 2.7.2
McAfee Deep Defender 1.6.0
McAfee Quarantine Manager 7.0.1
McAfee Security for Lotus Domino (HF738991) 7.5.0
McAfee Security for Microsoft Exchange 7.6.0
McAfee Security for Microsoft Exchange 8.0.0
McAfee Security for Microsoft SharePoint 2.5.0
MOVE AV [Agentless] 2.6.0
MOVE AV [Multi-Platform] Client 2.6.2
MOVE AV [Multi-Platform] Offload Scan Server 2.6.2
Rogue System Detection
SiteAdvisor Enterprise Plus 3.5.0
Solidcore 6.1.2:Application Control
Solidcore 6.1.2:Change Control
Solidcore 6.1.2:Integrity Monitor
Solidcore 6.1.2:General
Spotlight
VirusScan Enterprise 8.8.0
VirusScan Enterprise for Offline Virtual Images 2.1.0

| Category | Broken Inheritance | Actions |
|---|---|---|
| Agent Conf | None | Edit Ass |
| Computers | None | Edit Assign |

**Figure 5-1 System Tree Assigned Policies products list**

You can add new product policies to manage simply by checking in a product extension. An extension is a .zip file released by McAfee or a partner vendor. For a list of partner vendors, see the McAfee Security Innovation Alliance (SIA) webpage.

> The Software Manager is the easiest way to find and install new products.

By default all policies are inherited from the My Organization level, the highest point in the System Tree. All policies for all products flow downward into the groups and subgroups below it. If possible, set your policies at the My Organization level so that they include all groups and subgroups below.

Try to find a middle ground for all your policies that apply to as many systems as possible in your System Tree. This might not be realistic for all products, for example complex products like VirusScan Enterprise or Host Intrusion Prevention. Less complex policies can apply to all systems, for example the McAfee Agent policies govern all settings for the McAfee Agent itself.

# McAfee Agent policy

The McAfee Agent policy is a universal policy that applies to every system in your environment and is required for all other point-products.

See the McAfee ePolicy Orchestrator Product Guide and the McAfee Agent Product Guide for details about the McAfee Agent policy default settings.

**See also**
*Estimating and adjusting the ASCI* on page 149

## Configure an agent-server communication interval

The agent-server communication interval (ASCI) dictates how often every McAfee Agent calls the McAfee ePO server.

The ASCI is set to 60 minutes by default and performs these functions:

- Collects and sends its properties to the McAfee ePO server or Agent Handler.
- Checks to see if any policy or client task changes have occurred on the McAfee ePO server and pulls down the changes to the client.
- If configured to do so, sends product and system properties and events from the client to the McAfee ePO Server or Agent Handler.

For example, when the ASCI occurs, the McAfee Agent pulls down any change made to a policy for a product managed by McAfee ePO and applies that change to the endpoints.

## Send a policy change immediately

Execute a McAfee Agent wake-up call if you need to send a policy change or add a client task immediately.

The McAfee Agent wake-up call is a communication from the McAfee ePO server to agents or a group that instructs the McAfee Agent to perform its agent-server communication immediately.

> ⚠ Use the McAfee Agent wake-up call only in critical situations, because these calls can put a resource strain on the McAfee ePO server. If you need to wake-up thousands of systems, stagger the process by waking up a few hundred at a time. See the McAfee ePolicy Orchestrator Product Guide for details.

McAfee Agent wake-up calls from the McAfee ePO server occur at about 10-per-second maximum per Agent Handler. But McAfee Agent wake-up calls can take longer because of network lookups and other processes. Usually, with one Agent Handler, 1,000 McAfee Agent wake-up calls should take only a 100 seconds, but actually take 10 or 20 minutes.

### Task

For option definitions, click **?** in the interface.

1. Click **Menu** | **Systems Section** | **System Tree**.
2. Select the target group from the **System Tree**, then click the **Group Details** tab.
3. Click **Actions** | **Wake Up Agents**.
4. Make sure that the selected group appears next to **Target group**.
5. Select whether to send the McAfee Agent wake-up call to **All systems in this group** or to **All systems in this group and subgroups**.
6. Next to **Type**, select whether to send an **Agent wake-up** call or **SuperAgent wake-up call**.
7. To send minimal product properties as a result of this wake-up call, deselect **Retrieve all properties even if they haven't changed since the last time they were collected. If unchecked only retrieve changed properties**.

   The default is to send full product properties.
8. To update all policies and tasks during this wake-up call, select **Force complete policy and task update**.

   > ⚠ The Force complete policy and task update option can cause a serious performance penalty on the McAfee ePO server. This feature causes the McAfee Agent to delete all local policies. Then McAfee ePO server deletes all properties and resends everything to the agents. Only use this option when you think the incremental state between the McAfee Agent and the McAfee ePO server are not synchronized.

The policy change or client task is executed immediately by the wake-up call.

## Deploy packages

Packages are the binaries or files that you can deploy to an endpoint. All packages that you can deploy from the McAfee ePO server are located in the Master Repository and distributed repositories.

You do not have to check all packages into the Master Repository if you do not plan to deploy them with the McAfee ePO server. If you plan to use a third-party tool to deploy McAfee products, you do not need to check the package into the Master Repository. All content that is updated frequently, for example patches and signature files, can be checked in manually or checked in using an automated server task.

McAfee ePO tracks package versions, both major and minor, and allows you to check in packages to all three McAfee ePO repository branches: Current, Previous, and Evaluation.

> The branch a package is checked into is selected at the time the package is checked in and can be modified manually.

The repository branches of McAfee ePO allow multiple versions of the same package in the same repository. This allows installation of that package on a subset of the environment for testing prior to production rollout.

6

# Using client and server tasks in your managed environment

Client and server tasks are performed on your McAfee ePO server or the clients it manages. Using these tasks effectively can help with the overhead of managing your secure network.

**Contents**

## How client tasks deploy products

Client tasks run on the clients to deploy products and are typically scheduled to run at a specific time.

> ℹ Whenever you change a policy, configuration, client or server task, automatic response, or report, export the settings before and after the change. For detailed instructions about exporting objects, see the McAfee ePolicy Orchestrator Product Guide

Client tasks are different from policies because they are an action that the client must perform at a predetermined time.

Many of the tasks are specific to certain products, but you must have the product extensions checked in to McAfee ePO. These are the major tasks dedicated to the McAfee Agent.

- **Product deployment** — Tells the agent which products you want it to deploy to the client
- **Product update** — Uses the McAfee Agent to update content such as VirusScan Enterprise signatures, engine, or product patches

Client tasks can be set at a group or system level and always inherit to the group or system below them. Set your client tasks at the highest point of your directory tree, like the My Organization level. This group setting reduces the number of tasks you have to manage and keeps your administration overhead to a minimum.

**See also**

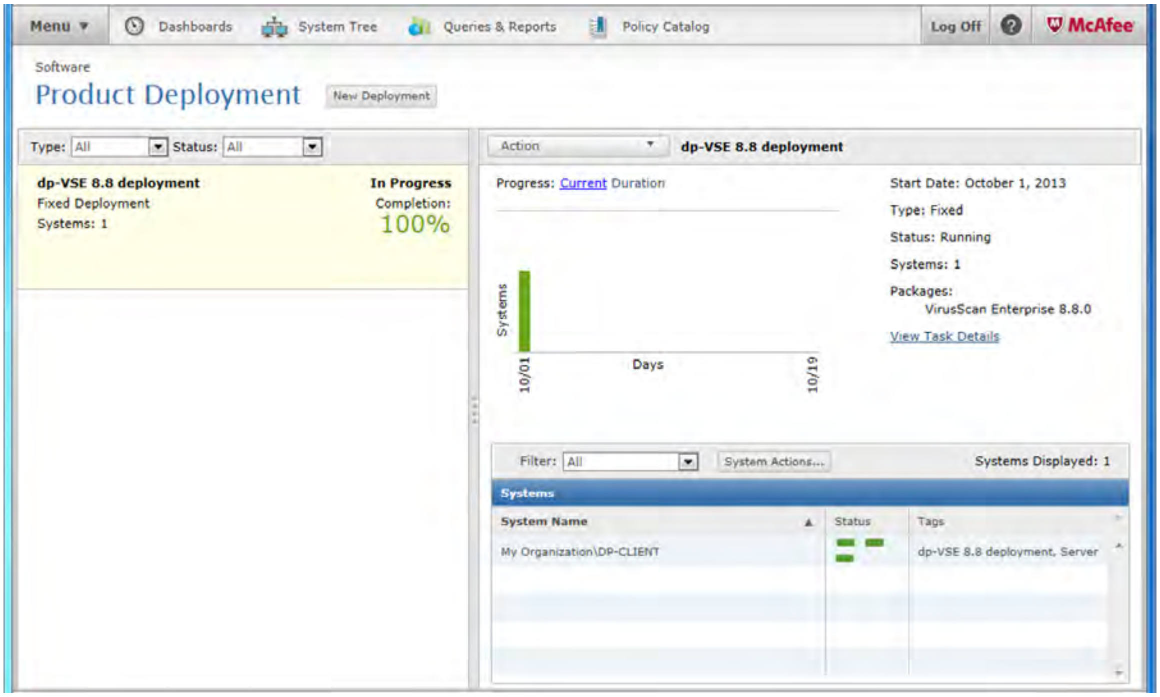
*Scheduling product deployment with randomization* on page 56
*Estimating the best ASCI* on page 149

## Product deployment workflows

Product deployment tells the agent which products you want deployed to the client and when.

You can use two workflows to deploy products with McAfee ePO:

1. Product Deployment projects streamline the deployment process and provide additional deployment functionality. See the McAfee ePolicy Orchestrator Product Guide for Product Deployment details.



Type: All Status: All

dp-VSE 8.8 deployment
Fixed Deployment
Systems: 1
In Progress
Completion:
100%

dp-VSE 8.8 deployment

Progress: Current Duration

Start Date: October 1, 2013
Type: Fixed
Status: Running
Systems: 1
Packages:
VirusScan Enterprise 8.8.0

Filter: All Systems Displayed: 1

| System Name | Status | Tags |
|---|---|---|
| My Organization\DP-CLIENT | | dp-VSE 8.8 deployment, Server |

**Figure 6-1 Deploy Products project page**

2. Individually created and managed client task objects and tasks are described in the following two tasks.

To deploy a product using individually created and managed client task objects, create a task and either link it to policy enforcement or schedule it to occur. The agent deploys the products in the order you specify until all products are installed using the schedule you specify.

## Configure the client task to deploy products

Product deployment client tasks distribute the most current content to client systems. The content might be DAT files, engines, or product patches.

To configure the client task to deploy products, see the McAfee ePolicy Orchestrator Product Guide for details.

## Scheduling product deployment with randomization

After you have configured your deployment tasks, schedule the deployment and enable randomization.

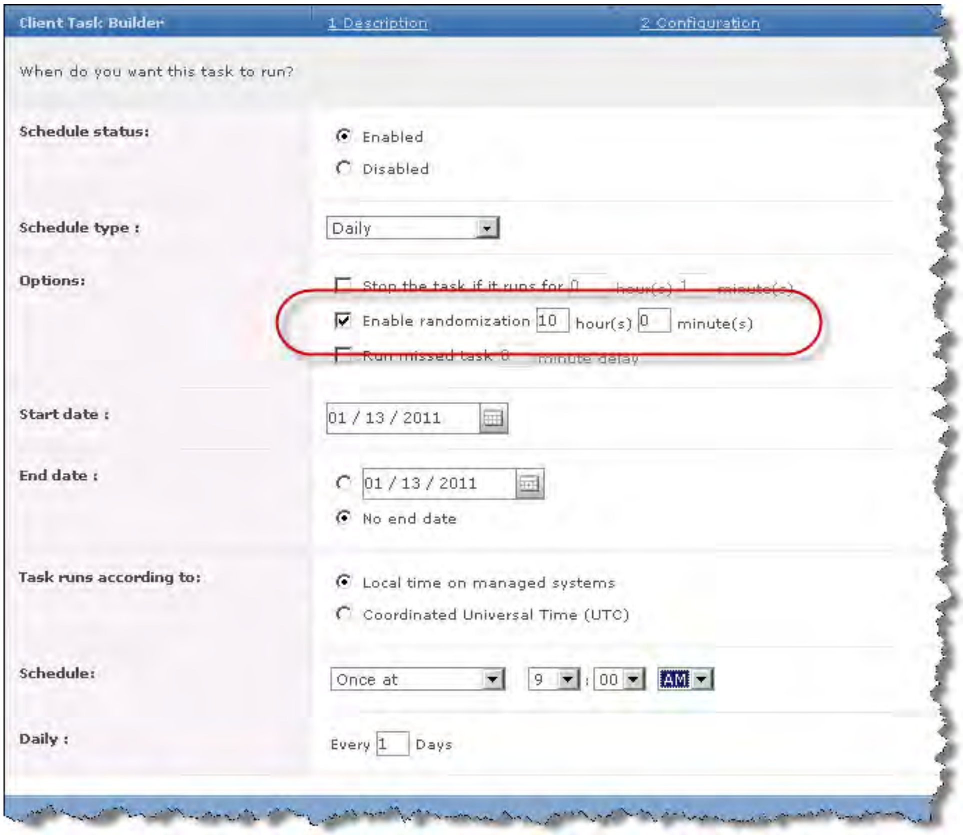
The schedule you choose for your client task is critical because it affects:

- Bandwidth
- Which systems have the latest content for protection
- The quality of your compliance reports

If a deployment task is being deployed to multiple client systems for the first time, you want to gradually roll out the products to some targeted test systems. The schedule you configure depends on the bandwidth available in your environment. For example, if you are upgrading from VirusScan Enterprise 8.7 to 8.8, you can look at the VirusScan Enterprise 8.8 package that you checked in to the McAfee ePO repository and see it is 56 MB. That means each system you target for deployment is pulling 56 MB from its nearest repository. If your McAfee ePO server is managing 5,000 nodes and you only have one repository, those 5,000 nodes are pulling a total of 280 GB of data from that one repository when the deployment task is executed. You must randomize your deployment to keep that repository from being overwhelmed.

To find the exact size of the product installation files in Windows Explorer, right-click the Install folder and click Properties. The product files are at this default path:

```
C:\Program Files(X86)\McAfee\ePolicy Orchestrator\DB\Software\Current\<ProductName>
\Install\
```



Client Task Builder | 1 Description | 2 Configuration

When do you want this task to run?

Schedule status: ● Enabled ○ Disabled

Schedule type : Daily

Options:
□ Stop the task if it runs for 0 hour(s) 1 minute(s)
☑ Enable randomization 10 hour(s) 0 minute(s)
□ Run missed task 0 minute delay

Start date : 01 / 13 / 2011

End date : ○ 01 / 13 / 2011 ● No end date

Task runs according to: ● Local time on managed systems ○ Coordinated Universal Time (UTC)

Schedule: Once at 9 : 00 AM

Daily : Every 1 Days

**Figure 6-2 Client Task Builder page with randomization enabled**

Many customers forget to enable randomization on their tasks and choose a specific time for their task to run, for example noon daily. Configure randomization before you deploy a daily product or signature update. This update could generate a significant daily spike in traffic to your repositories and could affect network performance.

Randomization is critical to any client task that uses bandwidth. Always calculate how much bandwidth the deployment needs before starting a product update. See Calculating bandwidth for repository replication and product updates on page 166.

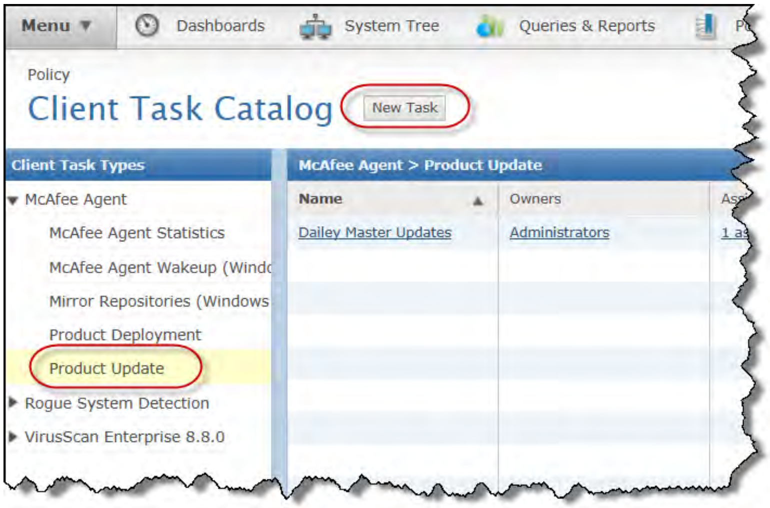
## Configure product updates

Create a Daily Master Update at the My Organization level.

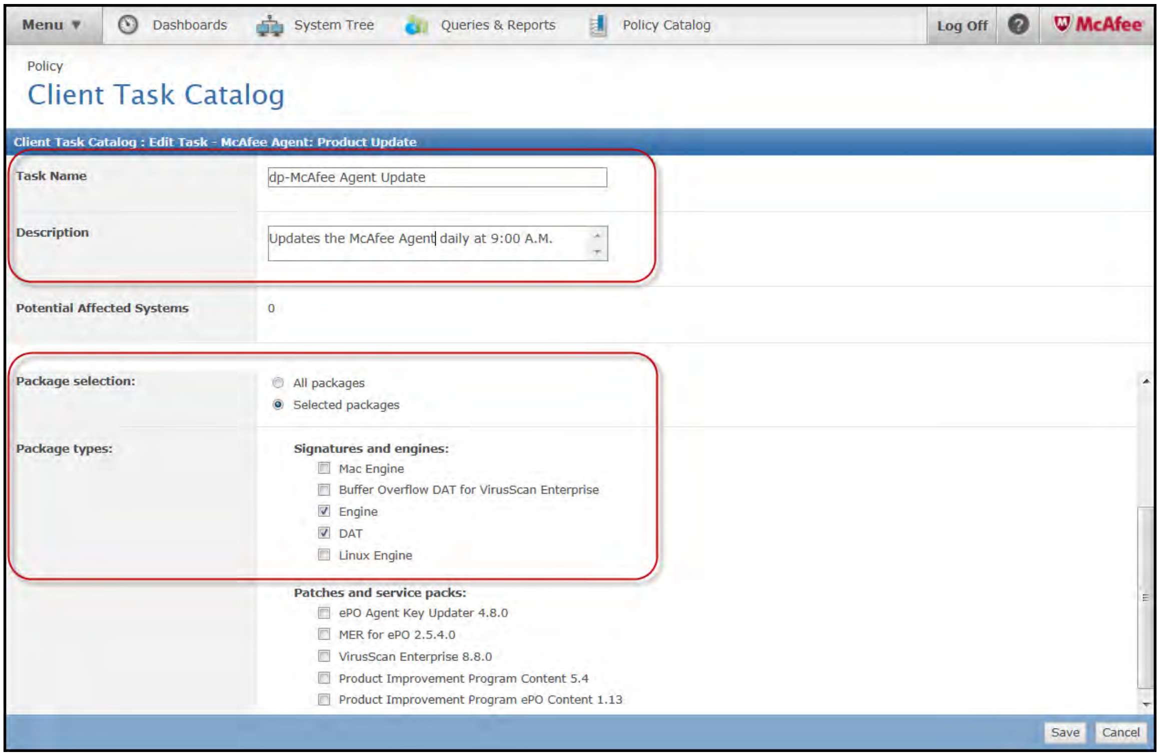
### Task

For option definitions, click **?** in the interface.

1. Click **Menu** | **Policy** | **Client Task Catalog**.
2. From the **Client Task Types** list, expand **McAfee Agent**, select **Product Update**, and click **New Task** at the top of the page.



3. From the **New Task** dialog box, select **Product Update** from the list and click **OK**.
4. On the new **Client Task Catalog** page, configure these settings and click **Save**.
   a. **Task Name** and **Description** — Type a descriptive name and description.
   b. **Package selection** — Click **Selected packages**.
   c. **Package types** — Select:
      - **Engine**
      - **DAT**



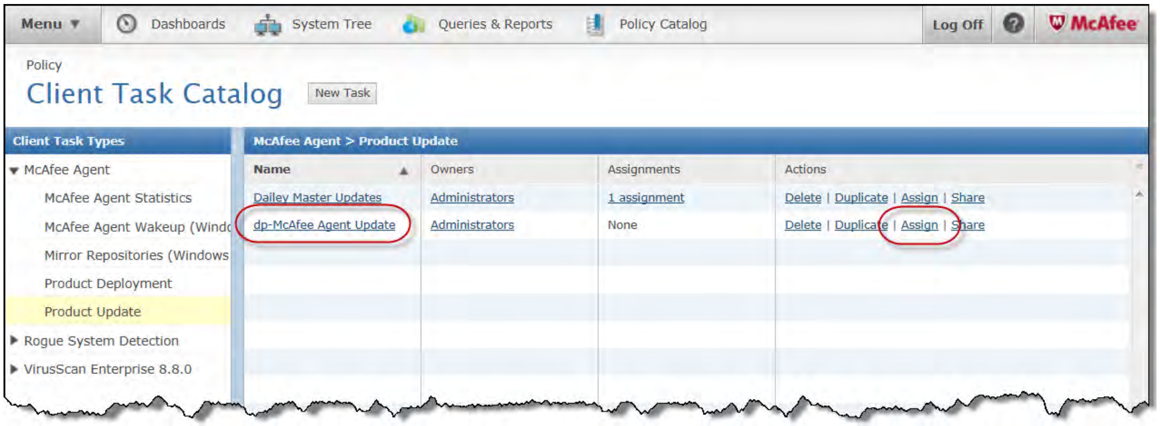
Policy

Client Task Catalog

**Client Task Catalog : Edit Task - McAfee Agent: Product Update**

| | |
|---|---|
| **Task Name** | dp-McAfee Agent Update |
| **Description** | Updates the McAfee Agent daily at 9:00 A.M. |
| **Potential Affected Systems** | 0 |
| **Package selection:** | ○ All packages<br>● Selected packages |
| **Package types:** | **Signatures and engines:**<br>☐ Mac Engine<br>☐ Buffer Overflow DAT for VirusScan Enterprise<br>☑ Engine<br>☑ DAT<br>☐ Linux Engine<br>**Patches and service packs:**<br>☐ ePO Agent Key Updater 4.8.0<br>☐ MER for ePO 2.5.4.0<br>☐ VirusScan Enterprise 8.8.0<br>☐ Product Improvement Program Content 5.4<br>☐ Product Improvement Program ePO Content 1.13 |

5 On the **Client Task Catalog** page, find the task you created and click **Assign** in the **Actions** column.



Policy

Client Task Catalog

**Client Task Types**

- ▼ McAfee Agent
  - McAfee Agent Statistics
  - McAfee Agent Wakeup (Windo
  - Mirror Repositories (Windows
  - Product Deployment
  - Product Update
- ▶ Rogue System Detection
- ▶ VirusScan Enterprise 8.8.0

**McAfee Agent > Product Update**

| Name ▲ | Owners | Assignments | Actions |
|---|---|---|---|
| Dailey Master Updates | Administrators | 1 assignment | Delete \| Duplicate \| Assign \| Share |
| dp-McAfee Agent Update | Administrators | None | Delete \| Duplicate \| Assign \| Share |

6 From the list of System Tree groups, select the group to use the new client task, and click **OK**.

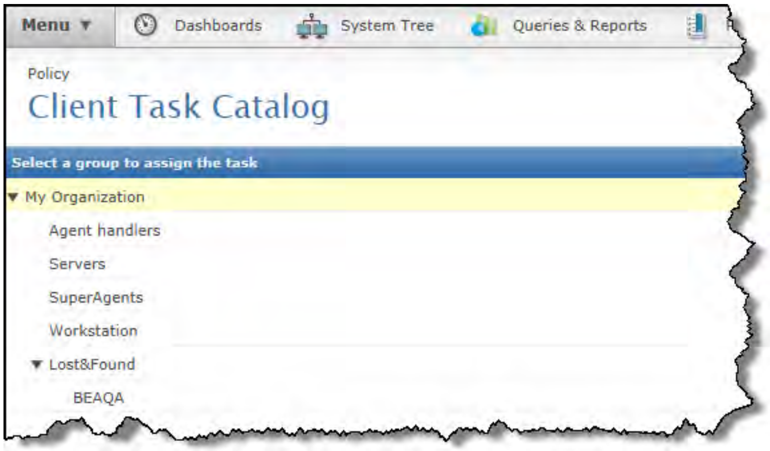
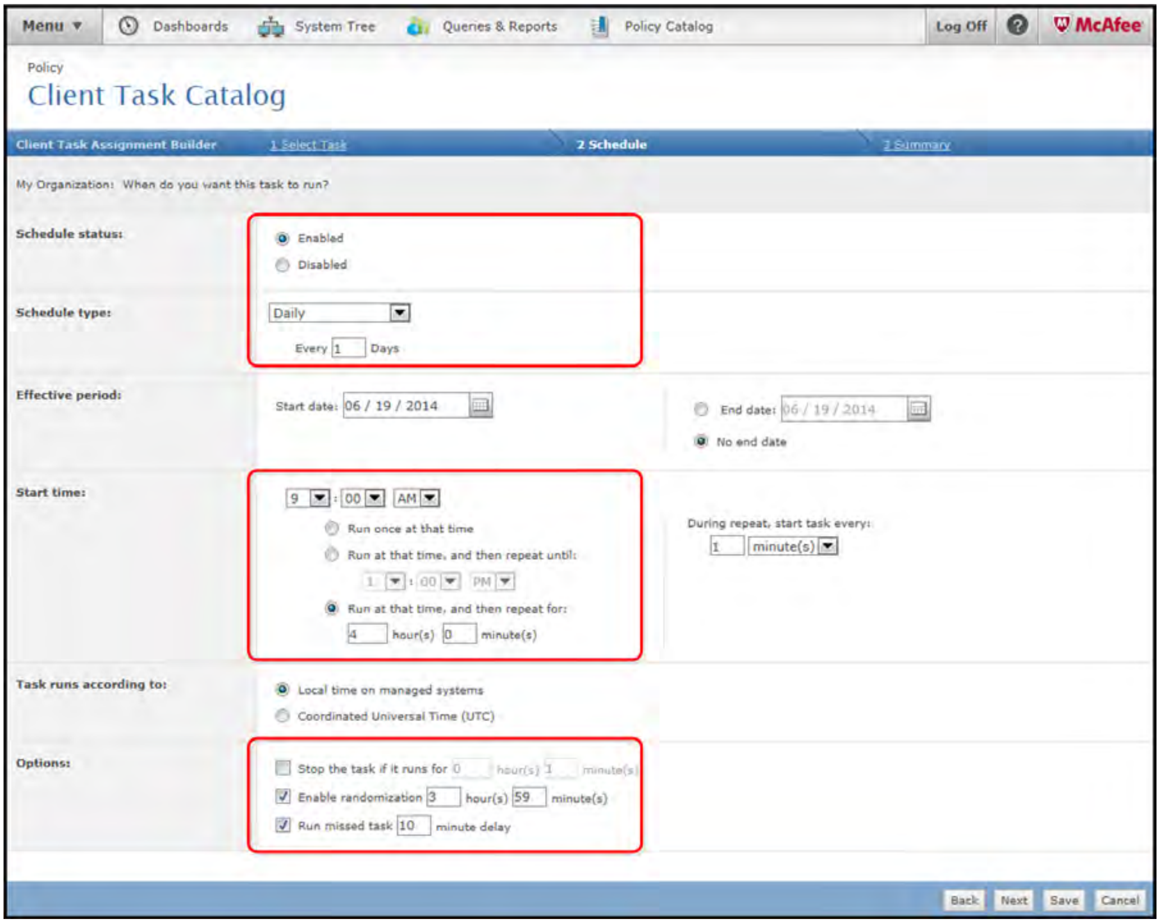


**Figure 6-3 Client Task Catalog group assignment**

7 On the **Client Task Assignment Builder** page again, click the **Schedule** tab, configure these settings, then click **Next**:

- **Schedule status** — **Enabled**
- **Schedule type** — **Daily**
- **Effective period** — Select **No end date**
- **Start time** — Set to start at **9:00 AM**, click **Run at that time, and then repeat for**, then set to **4 hour(s)**.

- **Options** — Select **Enable randomization** and set to **3 hour(s) 59 minute(s)**
- **Options** — Select **Run missed task** and set to **10 minute delay**. Once a system is connected to the managed network, after a 10 minute delay, the update packages are added to the system.



Policy

Client Task Catalog

My Organization: When do you want this task to run?

Schedule status: ● Enabled ○ Disabled

Schedule type: Daily
Every 1 Days

Effective period: Start date: 06 / 19 / 2014 ○ End date: 06 / 19 / 2014 ● No end date

Start time: 9 : 00 AM
○ Run once at that time
○ Run at that time, and then repeat until: 1 : 00 PM
● Run at that time, and then repeat for: 4 hour(s) 0 minute(s)

During repeat, start task every: 1 minute(s)

Task runs according to: ● Local time on managed systems ○ Coordinated Universal Time (UTC)

Options:
☐ Stop the task if it runs for 0 hour(s) 1 minute(s)
☑ Enable randomization 3 hour(s) 59 minute(s)
☑ Run missed task 10 minute delay

**Figure 6-4 Client Task Assignment Builder with schedule configured**

8 Click the **Summary** tab, confirm that the client task settings are correct, then click **Save**.

Now you have an update client task configured to update starting at 9:00 a.m. every four hours and randomized during that time. To confirm that your client task is configured correctly, click **Menu** | **Systems Section** | **System Tree** and the **Assigned Client Tasks** tab. You can click your new task and confirm its configuration.

**See also**
*Automating DAT file testing* on page 183

# Modifying McAfee ePO with server tasks

You can significantly improve how you manage the systems in your organization by scheduling server tasks to run on the McAfee ePO server

Whenever you change a policy, configuration, client or server task, automatic response, or report, export the settings before and after the change. For detailed instructions about exporting objects, see the McAfee ePolicy Orchestrator Product Guide.

Server tasks automate many of the common items you manually perform on a daily or weekly basis. Server tasks are automatically added as new extensions are added to McAfee ePO. For example, encryption-related server tasks appear when the encryption extension is installed. This relationship means that McAfee ePO is configured around the components you actually manage instead of having options for products you never use. Some common server tasks include:

- Performing an action using the results of a query
- Emailing and exporting reports automatically and regularly
- Pulling and replicating content automatically from the McAfee site
- Purging older events automatically from the McAfee ePO server database
- Deleting inactive systems automatically from your System Tree

**See also**

*Measuring malware events* on page 180
*Creating an automatic content pull and replication* on page 172
*Purging events automatically* on page 170
*Finding inactive systems* on page 178
*Create a server task to run compliance queries* on page 193

7

# Reporting with queries

McAfee ePO provides built in querying and reporting capabilities. These are highly customizable, flexible, and easy to use.

Both the **Query Builder** and **Report Builder** create and run queries and reports that organize user-configured data in user-specified charts and tables. The data for these queries and reports can be obtained from any registered internal or external database used with your McAfee ePO system.

### Contents

## Reporting features

You can use the preconfigured queries, create custom queries, use the output of the queries to perform tasks, and create reports as output.

> Whenever you change a policy, configuration, client or server task, automatic response, or report, export the settings before and after the change. For detailed instructions about exporting objects, see the McAfee ePolicy Orchestrator Product Guide.

The McAfee ePO software allows you to create custom reports by configuring these four basic items:

- **Result Type** — Identifies the type of data the query retrieves and determines the available selections.
- **Chart Type** — Specifies the type of chart or table to display the data.
- **Columns** — Selects the data to display. Selecting Table configures the table. Selecting a type of chart configures the drill-down table.
- **Filter** — Limits the data retrieved by the query to the specified criteria.

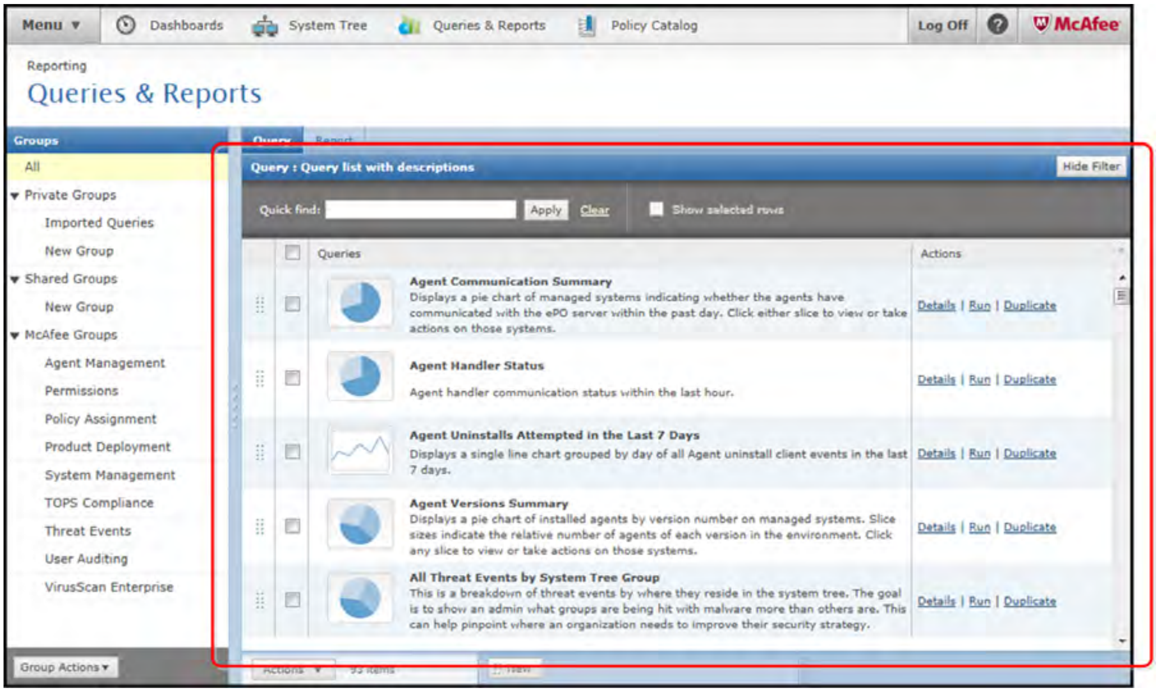
To view one of the preconfigured queries, click **Run**. You can then perform the following tasks:

- Save the output as a report.
- Duplicate the query and change the output.

- View results in the query system.
- Take action on the results as you normally would in the System Tree.

> As you add new products using extensions to McAfee ePO, new preconfigured queries and reports become available.

The following example shows some of the categories included with the preconfigured queries.



| □ | Queries | Actions |
|---|---|---|
| □ | **Agent Communication Summary**<br>Displays a pie chart of managed systems indicating whether the agents have communicated with the ePO server within the past day. Click either slice to view or take actions on those systems. | Details \| Run \| Duplicate |
| □ | **Agent Handler Status**<br>Agent handler communication status within the last hour. | Details \| Run \| Duplicate |
| □ | **Agent Uninstalls Attempted in the Last 7 Days**<br>Displays a single line chart grouped by day of all Agent uninstall client events in the last 7 days. | Details \| Run \| Duplicate |
| □ | **Agent Versions Summary**<br>Displays a pie chart of installed agents by version number on managed systems. Slice sizes indicate the relative number of agents of each version in the environment. Click any slice to view or take actions on those systems. | Details \| Run \| Duplicate |
| □ | **All Threat Events by System Tree Group**<br>This is a breakdown of threat events by where they reside in the system tree. The goal is to show an admin what groups are being hit with malware more than others are. This can help pinpoint where an organization needs to improve their security strategy. | Details \| Run \| Duplicate |

**Figure 7-1 Example of report categories**

See the McAfee ePolicy Orchestrator Product Guide for additional information about reporting.

## Reporting lag time

When you run McAfee ePO query reports, you must be aware that reports have a lag-time. This lag-time means information is not added to the report during the time when it's actually being run. This information lag-time begins when you start the query, lasts until the query is done, and varies depending on the time it takes to run the query.

Report lag-time example:

- You run a query hourly and the query takes 10 minutes to run.
- Events that occur during the 10 minutes, while the query is being run, are not included in that report, but are written to the database.
- Those events appear in the next query report run an hour later.

# How to use custom queries

Creating custom queries on the McAfee ePO server is easy, plus you can duplicate and modify existing queries to suit your needs.

You create custom queries using the Query Builder wizard. To access the Query Builder wizard, click **Menu | Reporting | Queries and Reporting**, then click **Actions | New**.

There are two ways to approach custom queries:

1. You can determine exactly which kind of query that you want to create before you create it.
2. You can explore the Query Builder wizard and try different variables to see the different types of available queries.

Both approaches are valid and can yield interesting data about your environment. If you are new to the query system, try exploring different variables to see the types of data that McAfee ePO can return.

Once you have created your report, you can take action on the results. The type of action depends on the type of output created by the report. You can do anything that you could do in the System Tree for example, you can wake up systems, update them, delete them, or move them to another group. This action is useful when running reports on systems that:

- Have not communicated with the McAfee ePO server recently
- Are suspected of not working properly when you attempt to wake them up
- Need a new agent deployed to them directly from McAfee ePO

## Create custom event queries

You can create a custom query from scratch or duplicate and change an existing query.

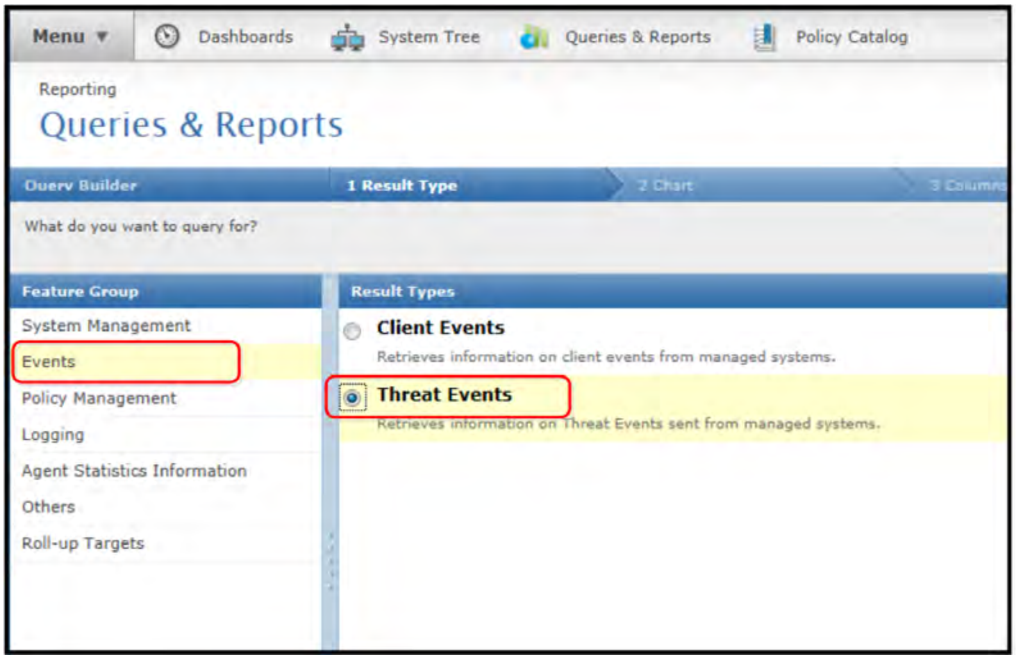
### Task

For option definitions, click **?** in the interface.

1. Click **Menu** | **Reporting** | **Queries & Reports**, then **Actions** | **New**. The Query wizard opens and displays the Result Types tab.

The result types are organized into groups on the left side of the page. Depending on what extensions have been checked in to McAfee ePO, these groups vary. Most of the result types are self-explanatory, but two of the more powerful result types are Threat Events and Managed Systems. You can access these two events types as shown in the following examples.

- **Threat Events** — In the Feature Group, select **Events**. Under Result Types, select **Threat Events**.



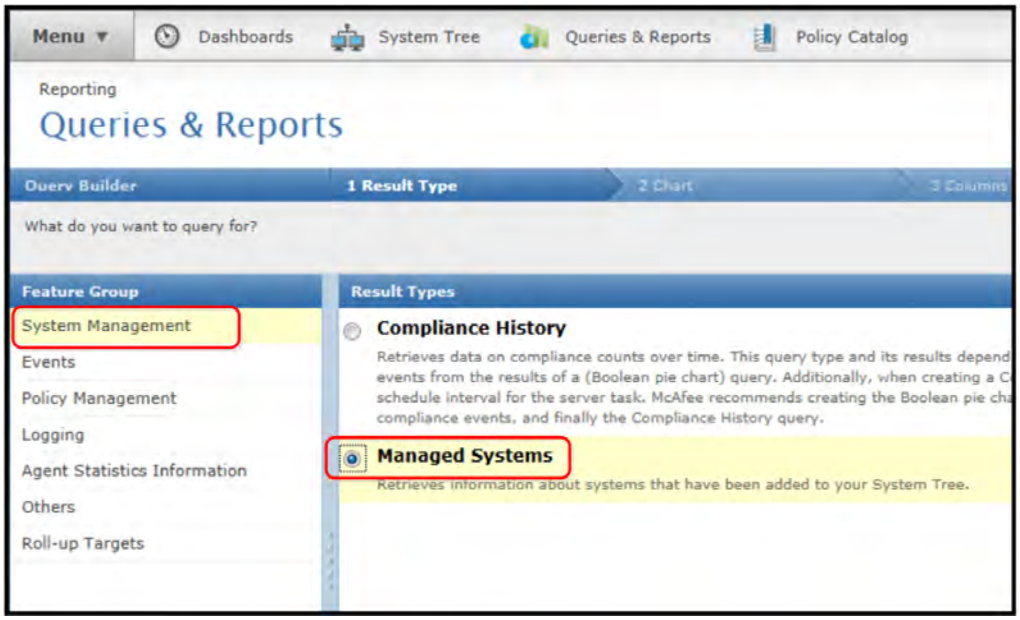
What do you want to query for?

○ **Client Events**
Retrieves information on client events from managed systems.

● **Threat Events**
Retrieves information on Threat Events sent from managed systems.

**Figure 7-2 Query Builder with Threat Events selected**

- **Managed Systems** — In the Feature Group, select **System Management**. Under Result Types, select **Managed Systems**.



What do you want to query for?

○ **Compliance History**
Retrieves data on compliance counts over time. This query type and its results depend
events from the results of a (Boolean pie chart) query. Additionally, when creating a C
schedule interval for the server task. McAfee recommends creating the Boolean pie cha
compliance events, and finally the Compliance History query.

● **Managed Systems**
Retrieves information about systems that have been added to your System Tree.

**Figure 7-3 Query Builder with Managed Systems selected**

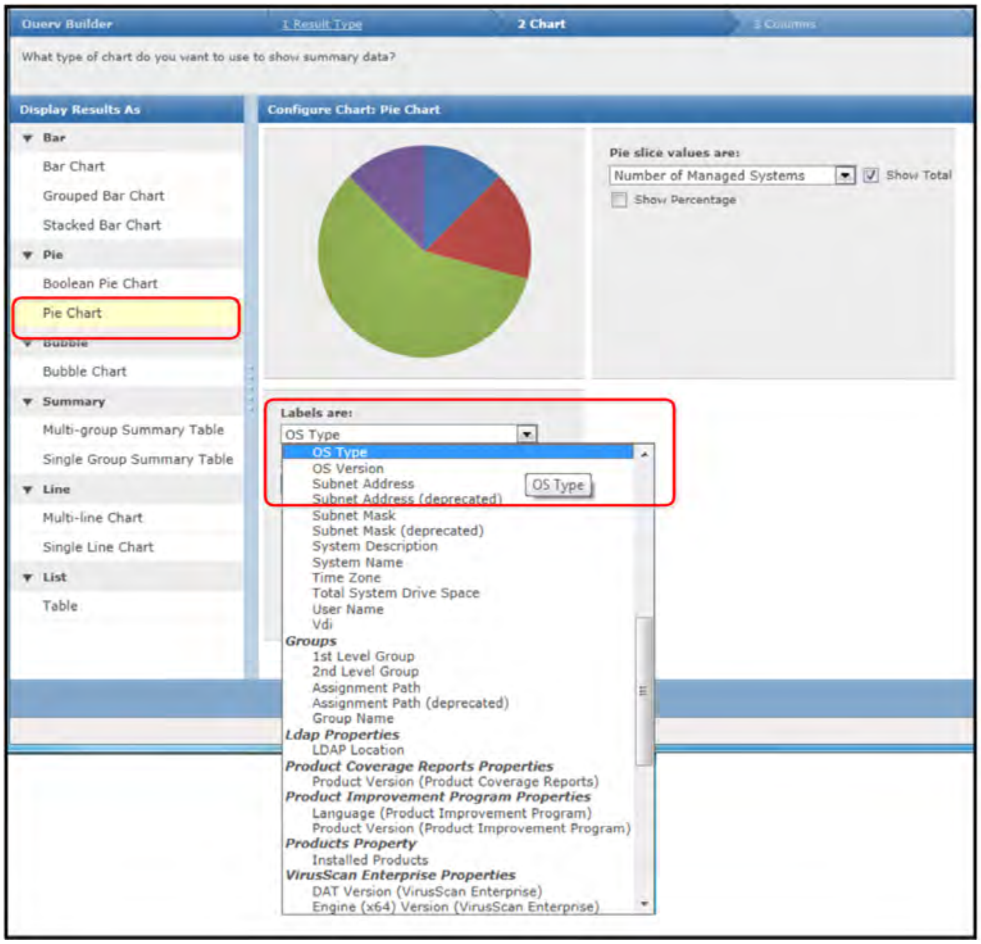
2 Choose your chart type. There are several chart types to choose from and some are more complex than others. The two simplest charts are the pie chart and the single group summary table. The pie chart compares multiple values in a graphic format, and the summary table displays a data set with over 20 results.

To create a pie chart, in the Display Results Type, click **Pie Chart**.

3 Choose the label or variable that you want the report to display.

> Many times the report does not have to return data on McAfee products. For example you can report on the operating system versions used in your environment.

In the Labels are list, click **OS Type**.



Query Builder

What type of chart do you want to use to show summary data?

Configure Chart: Pie Chart

Pie slice values are: Number of Managed Systems ☑ Show Total

☐ Show Percentage

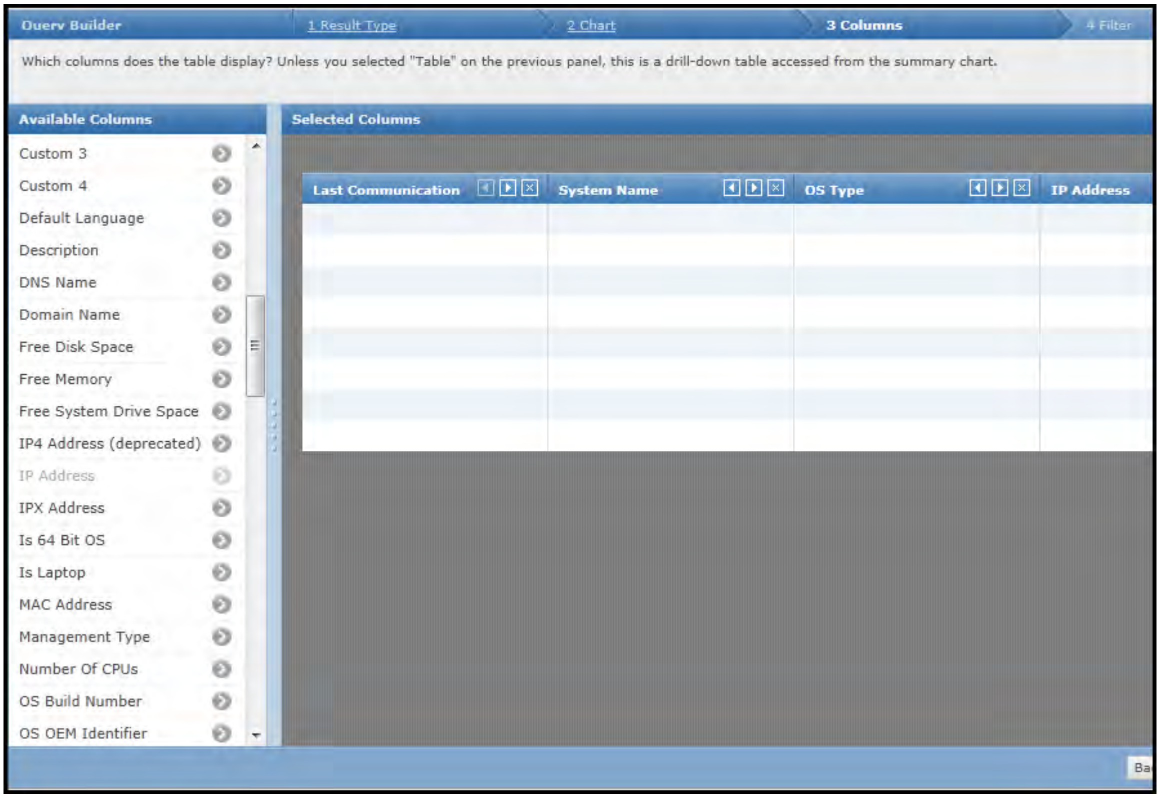
Labels are: OS Type

**Figure 7-4 Query Builder Labels selection list**

4 Choose the columns that you want to see when you drill down on any of the variables in the report. This is not a critical component when building a query and can be adjusted at a later time.

> You can also drag-and-drop columns from left to right and add and remove columns to display.

To use the default columns, click **Next**.



Which columns does the table display? Unless you selected "Table" on the previous panel, this is a drill-down table accessed from the summary chart.

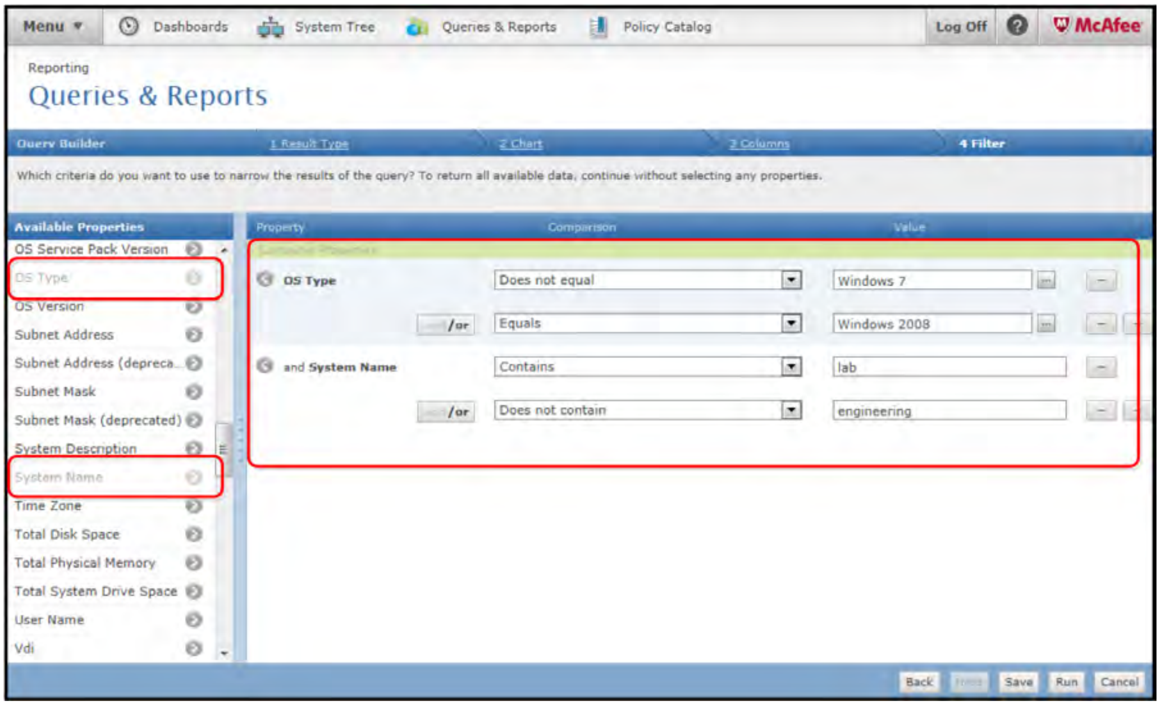
**Figure 7-5 Query Builder Columns selection**

You can filter the data that you want the query to return. You can leave the filter area blank, which returns every device in your tree, or specify the return results you are interested in. Examples of filter options include:

- A group in your System Tree where the report applies. For example, a geographic location or office.
- Only include laptop or desktop systems.
- Only specific operating system platforms. For example, servers or workstations.
- Only include systems that have an older DAT version.

- Only include systems with an older version of VirusScan Enterprise.
- Only return systems that have communicated with the McAfee ePO server in the past 14 days

The following example shows how you might configure some of these filter examples.



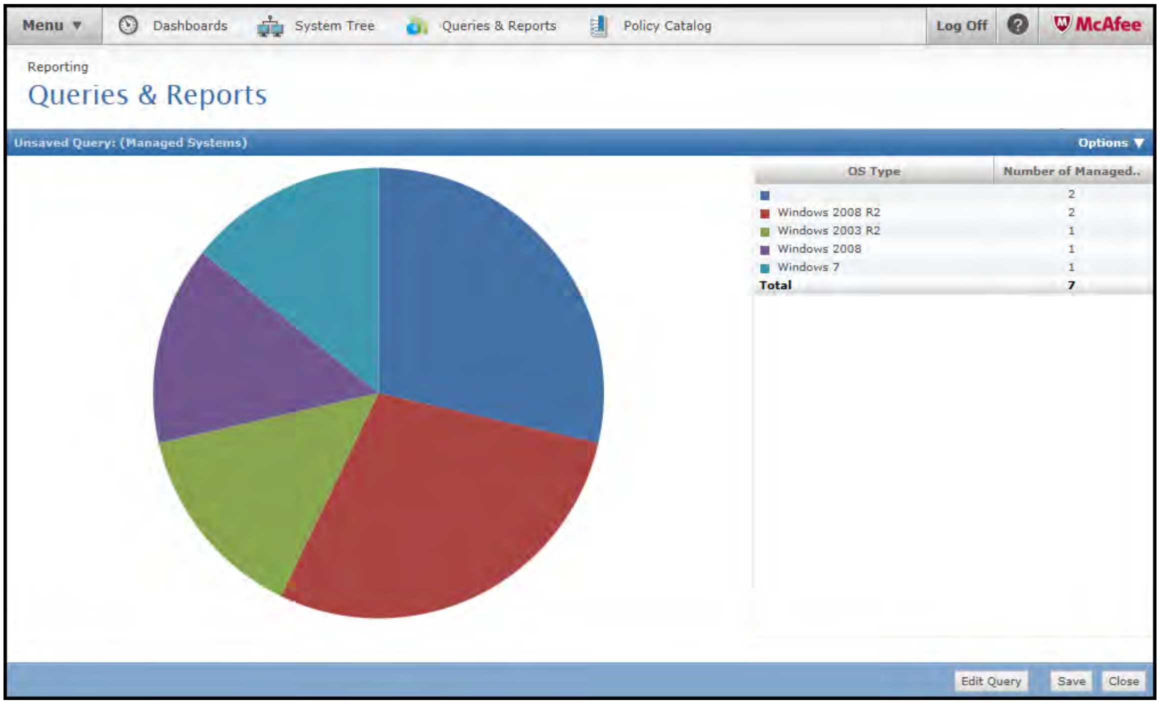
Which criteria do you want to use to narrow the results of the query? To return all available data, continue without selecting any properties.

| Property | | Comparison | Value |
|---|---|---|---|
| OS Type | | Does not equal | Windows 7 |
| | /or | Equals | Windows 2008 |
| and System Name | | Contains | lab |
| | /or | Does not contain | engineering |

**Figure 7-6  Query Builder Filters selection**

5 Click **Next** to not create any filters and display all operating system types.

6 Click **Run** to generate the report and see the results.



| OS Type | Number of Managed.. |
|---|---|
| 🟦 | 2 |
| 🟥 Windows 2008 R2 | 2 |
| 🟩 Windows 2003 R2 | 1 |
| 🟪 Windows 2008 | 1 |
| 🟦 Windows 7 | 1 |
| **Total** | **7** |

**Figure 7-7 Query Builder Edit Query option**

After you create the reports and display the output, you can fine-tune your report without starting again from the beginning. To do this, click **Edit Query**. This allows you to go back and adjust your report and run it again within seconds.

When you have made all changes to your report, click **Save** to save it permanently. Then it is included with your dashboards and you can run it any time.

## How event summary queries work

Client events and threat events make up most of the event data in your database. Queries help you track how many events are stored in your database.

Event summary queries help you manage any performance problems that these events might cause for your McAfee ePO server and database.

Client events from your agents relate their task status to McAfee ePO. Items like update complete, update failed, deployment completed, or encryption started are considered client events. Threat events include a virus was found, a DLP event was triggered, or an intrusion was detected. Depending on which products you have installed and which events you are collecting, there might be thousands or even millions of these events in your database.

**See also**

*Purging events automatically* on page 170

## Create client event summary queries

To display events sent from your McAfee Agents to McAfee ePO, create client event summary queries that send threat notifications to your administrator.

This example creates a new client events summary query. It displays events sent from each McAfee Agent to McAfee ePO. Items like update complete, update failed, deployment completed, or encryption started are considered client events.

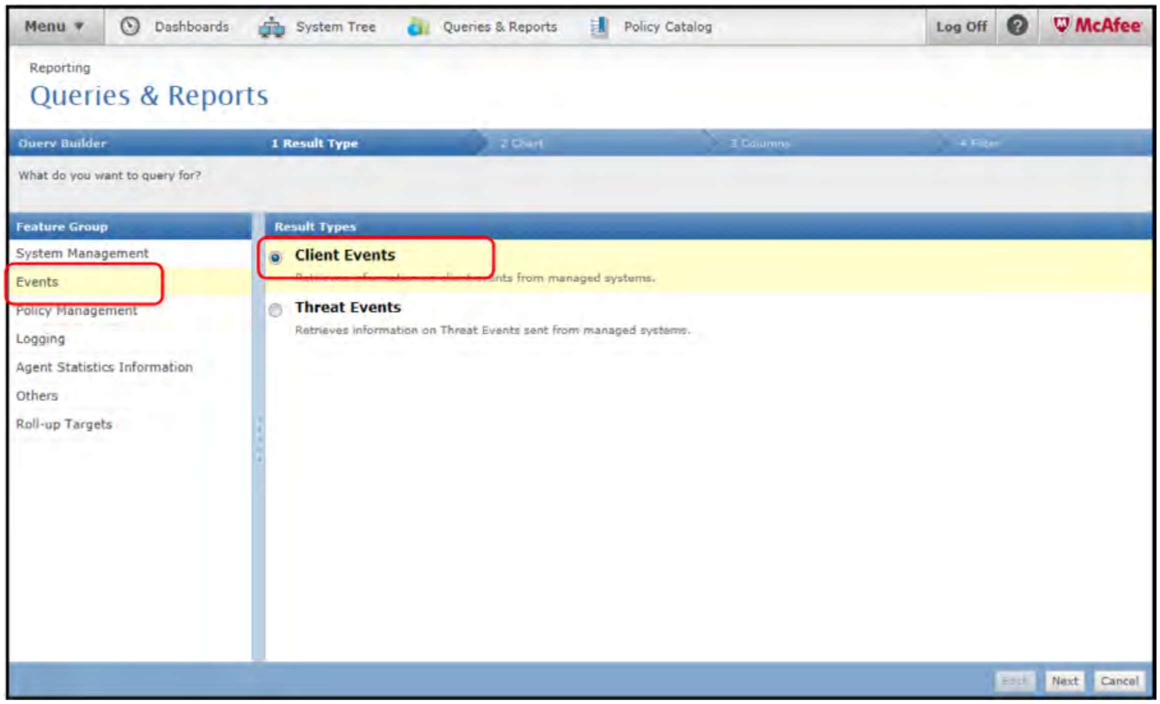
### Task

For option definitions, click **?** in the interface.

1 To create a new client events summary query, click **Menu** | **Reporting** | **Queries & Reports**.

2 From the Queries page, click **Actions** | **New**.

3 From the Query Wizard, starting with the **Result Types** tab, click **Events** in the Features Group, **Client Events** in **Result Types**, then click **Next**.



What do you want to query for?

● Client Events
Retrieves information on client events from managed systems.

○ Threat Events
Retrieves information on Threat Events sent from managed systems.

**Figure 7-8 Query Builder with Client Events selected**

4 On the Chart page under Summary, click **Single Group Summary Table** to display a total count of all the client events in the events table.

5 To create a filter with a good human-readable description of the events, click **Event Description**, in the Labels are list under Threat Event Descriptions.

Optionally, you can filter by the Event ID, which is the number that represents client event data in McAfee ePO. For details about point product generated event IDs listed in McAfee ePO, see KnowledgeBase article McAfee point product generated Event IDs listed in ePO, KB54677.

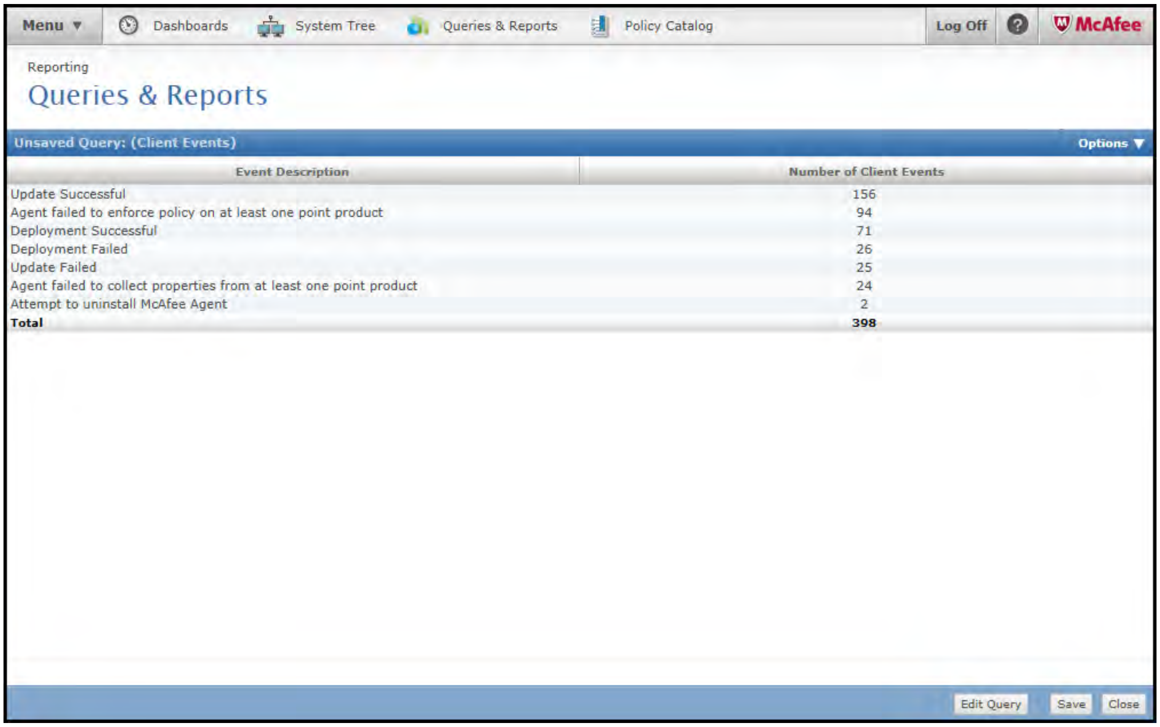
6 If needed, adjust the column information based on the type that you want displayed.

This step is not critical for the creation of the query.

7 Click **Next**, the Filter page appears.

You do not need any filtering because you want every single client event returned in the database. Optionally, you can create a query based on events generated within a certain time, for example, the last 24 hours, or the last 7 days.

8 Click **Run** to display the query report.



| Event Description | Number of Client Events |
|---|---|
| Update Successful | 156 |
| Agent failed to enforce policy on at least one point product | 94 |
| Deployment Successful | 71 |
| Deployment Failed | 26 |
| Update Failed | 25 |
| Agent failed to collect properties from at least one point product | 24 |
| Attempt to uninstall McAfee Agent | 2 |
| **Total** | **398** |

**Figure 7-9 Query Builder output**

In this example, there are a total of 308 client events. You can click one event and drill down to display more information about it.

9 Click **Save** and type an appropriate name for the report. For example, `All Client Events by Event Description`.

## Create a threat events summary query

To provide threat notification to your administrators, create a threat events summary query to display threat events sent from your agents to the McAfee ePO server.

In this example, threat events include a virus found, a Data Loss Protection event triggered, or an intrusion detected.

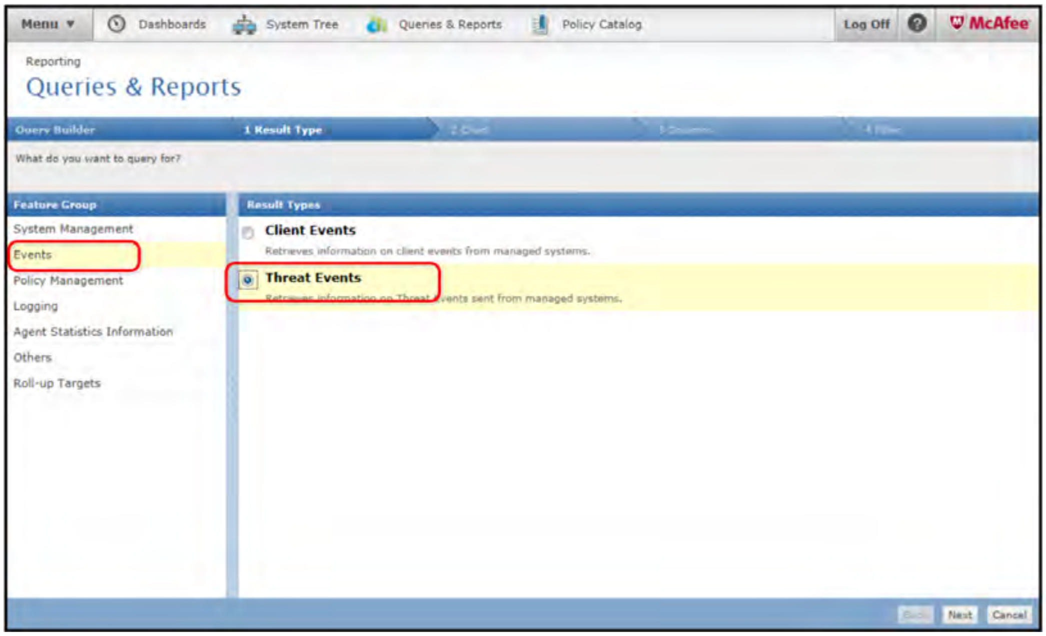
### Task

For option definitions, click **?** in the interface.

1 To start the query configuration, click **Menu** | **Reporting** | **Queries & Reports**.

2 From the Queries page, click **Actions** | **New**.

3 From the Query Wizard page, starting with the Result Types tab, click **Events** in the Features Group and **Threat Events** in the Result Type, and click **Next**.



Reporting

Queries & Reports

What do you want to query for?

**Feature Group**

- System Management
- Events
- Policy Management
- Logging
- Agent Statistics Information
- Others
- Roll-up Targets

**Result Types**

○ **Client Events**
Retrieves information on client events from managed systems.

● **Threat Events**
Retrieves information on Threat Events sent from managed systems.

**Figure 7-10 Query Builder with Threat Events selected**

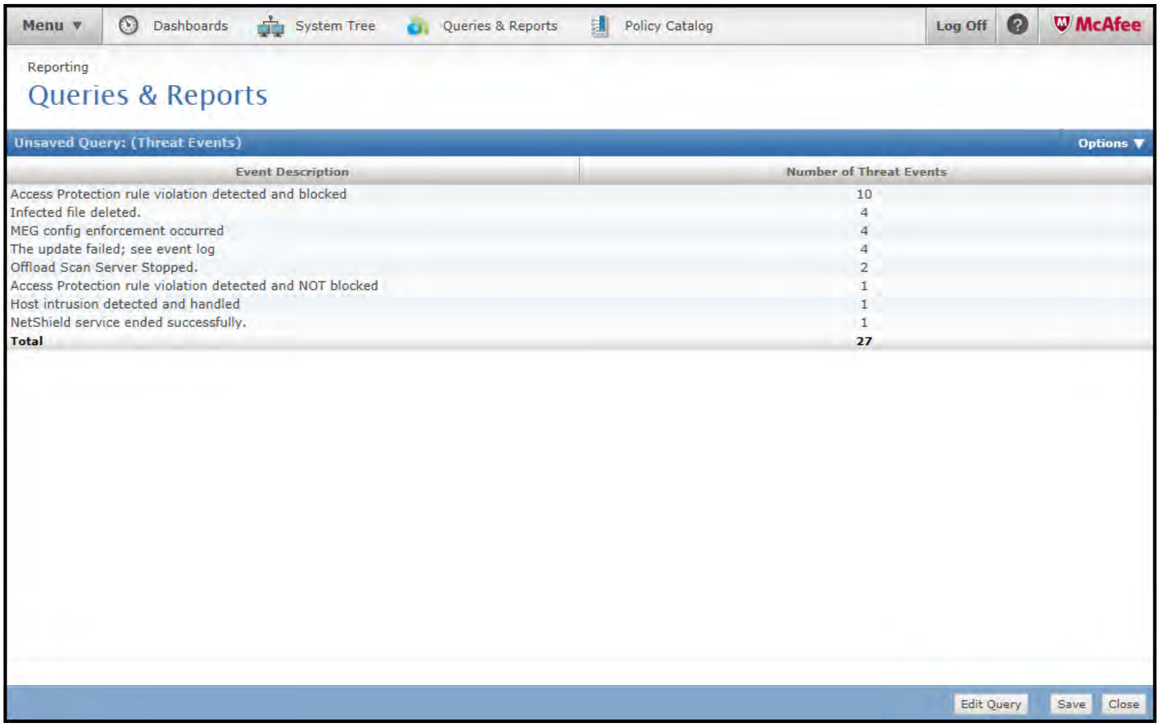
4 From the Chart page, under Summary, click **Single Group Summary Table**, to display a total count of all the client events in the events table.

5 To create a filter with a good human-readable description of the events, click **Event Description**, in the Labels are list, under Threat Event Descriptions.

Optionally, you can filter by the Event ID which is the number that represents client event data in McAfee ePO. For details about point product generated event IDs listed in McAfee ePO, see KnowledgeBase article McAfee point product generated Event IDs listed in ePO, KB54677.

6 If needed, adjust the columns information based on the type that you want displayed, then click **Next**.

7 On the Filter page, you do not need any filtering because you want every single client event returned in the database. Optionally, you can create a query based on events generated within a certain time, for example the last 24 hours, or the last 7 days. Click **Run** to display the query report.



| Event Description | Number of Threat Events |
|---|---|
| Access Protection rule violation detected and blocked | 10 |
| Infected file deleted. | 4 |
| MEG config enforcement occurred | 4 |
| The update failed; see event log | 4 |
| Offload Scan Server Stopped. | 2 |
| Access Protection rule violation detected and NOT blocked | 1 |
| Host intrusion detected and handled | 1 |
| NetShield service ended successfully. | 1 |
| **Total** | **27** |

**Figure 7-11 Query Builder output**

The data shown in this example comes from a McAfee ePO server that is managing only a few nodes, so these numbers are small. A real production McAfee ePO database might have millions of threat and client events.

8 To determine approximately how many events you should have on your network, use the following formula:

**(10,000 nodes) x (5 million events) = estimated number of events**

For example, if you have 50,000 nodes, your range is 25 million total client and threat events.

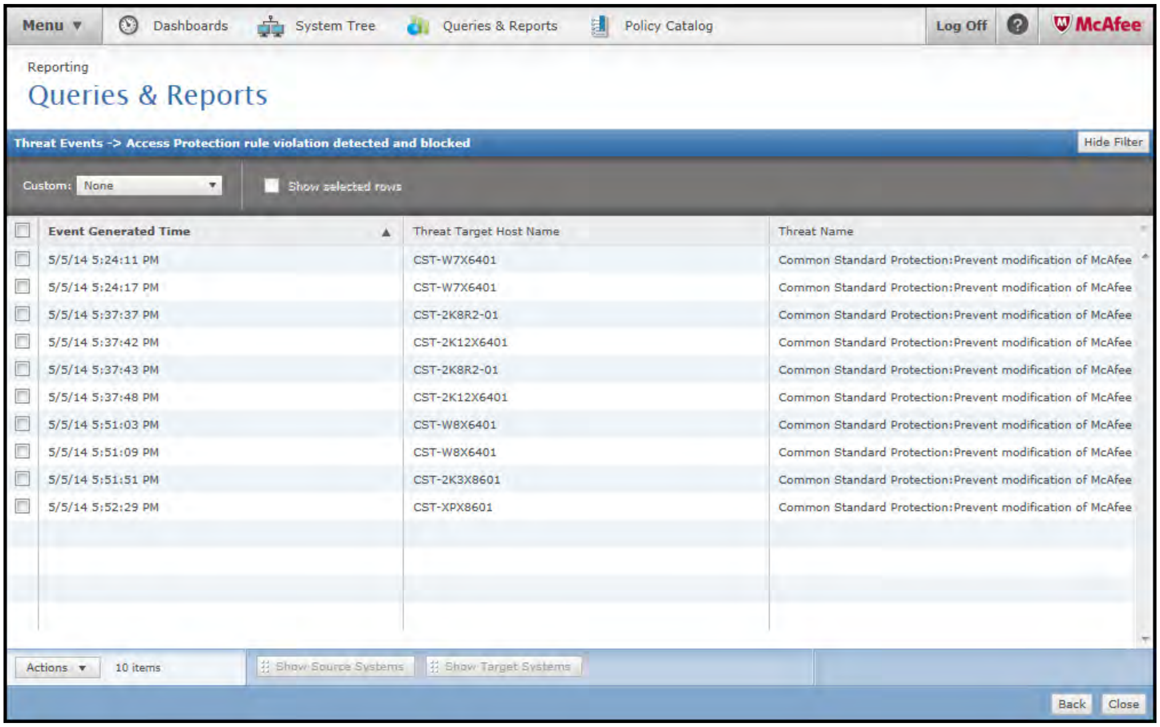
This number varies greatly based on the number of products and policies you have and your data retention rate. Do not panic if you exceed this number.

If you significantly exceed this number, determine why you have so many events. Sometimes this can be normal if you receive a significant number of viruses. This is common in unrestricted networks, such as those for universities or college campuses. Another reason for a high event count could be how long you keep the events in your database before purging. Here is what to check:

- Are you purging your events on a regular basis, as described in Purging events automatically on page 170?
- Is there a specific event in the query that comprises most of your events?

Remember, it's very common to forget to include a purge task. This causes McAfee ePO to retain every single event that has occurred since the McAfee ePO server was built. You can fix this simply by creating a purge task.

If you notice one or two events make up a disproportionate number of your events, you can then determine what they are by drilling down into those events. For example, in the previous figure you see that the event with the most instances is an access protection rule from VirusScan Enterprise. This is a very common event. If you double-click on the Access Protection rule event to drill down on the cause, you can see that a few access protection rules are being triggered repeatedly on VirusScan Enterprise, as shown in this figure.



Threat Events -> Access Protection rule violation detected and blocked

| Event Generated Time | Threat Target Host Name | Threat Name |
|---|---|---|
| 5/5/14 5:24:11 PM | CST-W7X6401 | Common Standard Protection:Prevent modification of McAfee |
| 5/5/14 5:24:17 PM | CST-W7X6401 | Common Standard Protection:Prevent modification of McAfee |
| 5/5/14 5:37:37 PM | CST-2K8R2-01 | Common Standard Protection:Prevent modification of McAfee |
| 5/5/14 5:37:42 PM | CST-2K12X6401 | Common Standard Protection:Prevent modification of McAfee |
| 5/5/14 5:37:43 PM | CST-2K8R2-01 | Common Standard Protection:Prevent modification of McAfee |
| 5/5/14 5:37:48 PM | CST-2K12X6401 | Common Standard Protection:Prevent modification of McAfee |
| 5/5/14 5:51:03 PM | CST-W8X6401 | Common Standard Protection:Prevent modification of McAfee |
| 5/5/14 5:51:09 PM | CST-W8X6401 | Common Standard Protection:Prevent modification of McAfee |
| 5/5/14 5:51:51 PM | CST-2K3X8601 | Common Standard Protection:Prevent modification of McAfee |
| 5/5/14 5:52:29 PM | CST-XPX8601 | Common Standard Protection:Prevent modification of McAfee |

10 items

**Figure 7-12 Query wizard output showing drill down of Access Protection rule**

9 At this point, determine whether these are important events in your organization and if they are being looked at by administrators. Ignoring some events is very common by some administrators.

Ultimately, whenever dealing with excessive events in your database, you must follow this process:

a Create a query that shows all the events you are questioning, then use the information in this section to analyze these threat events.

b Determine if anyone is looking at these excessive events in the first place.

c If events are not being analyzed, change your policy to stop the event forwarding.

d If the event is important, make sure that you are monitoring the number of events. See How event summary queries work on page 70, and Purging events automatically on page 170.

If no one is looking at these events, then you might consider disabling them completely in the VirusScan Enterprise access protection policy to stop them from being sent to the McAfee ePO server. See Filter 1051 and 1059 events on page 175 for details. Alternatively, you can adjust your policy to send only the access protection events that you are concerned with instead of excessive events that are not being analyzed. If you do want to see these events, you can leave the policy as configured, but confirm that you are following the rules about purging events from the McAfee ePO server so that these events do not overrun your database.

**See also**

*Purge events by query* on page 171
*Purging events automatically* on page 170
*How event summary queries work* on page 70
*Filter 1051 and 1059 events* on page 175
*Filtering 1051 and 1059 events* on page 174

## Create custom table queries

Create a simple table query that includes taking action on certain types of events, for example events that purge data or events based on a query.

For example, you might need to purge data or events based on a query. Or you might have events of a specific type that are overwhelming your database, such as 1051 and 1059 events. Plus, you can use this technique to purge other threat events based on the custom table queries you create.

A table query is used to return data in a simple table format, without graphs or charts. Simple table data can be acted upon by a McAfee ePO server task. For example, you can automatically delete this data.

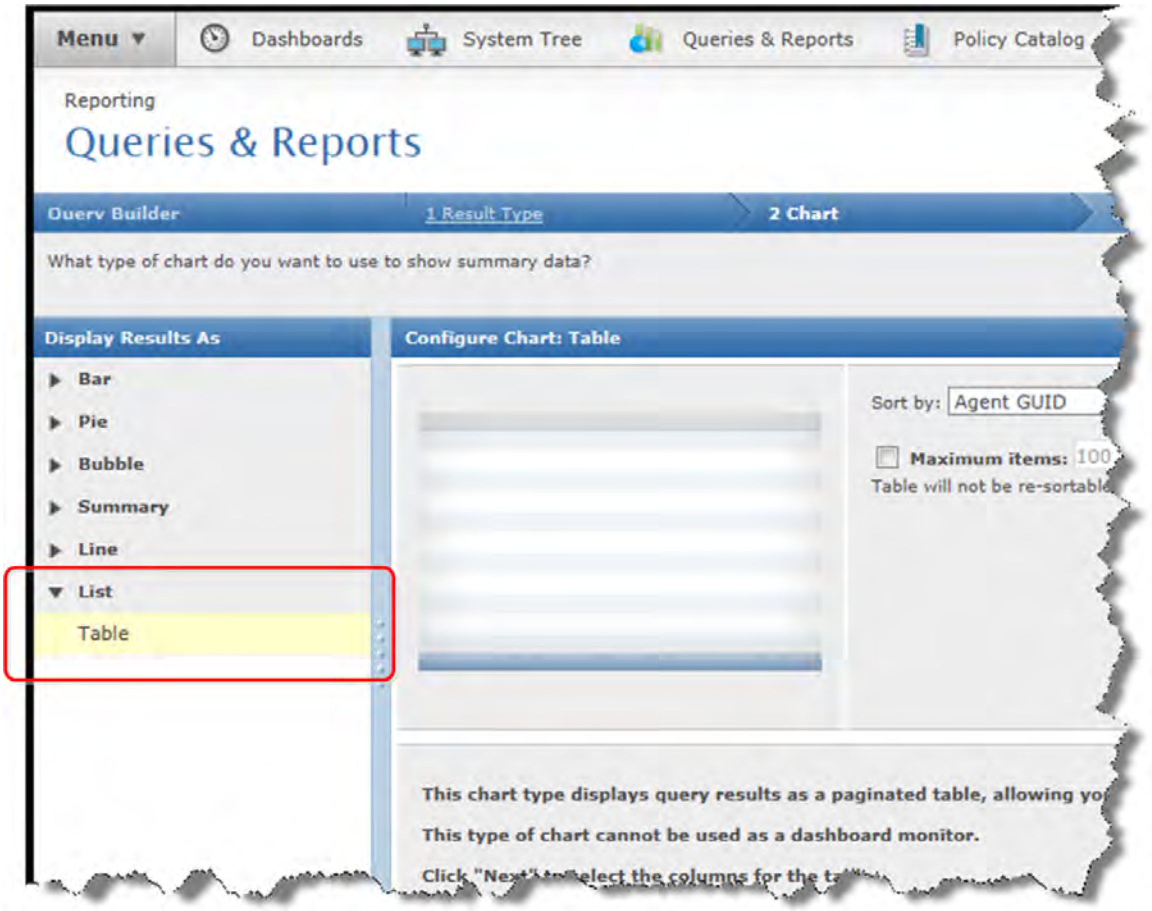
This task creates a custom query that returns all 1051 and 1059 events in the database.

### Task

For option definitions, click **?** in the interface.

1. To open the Queries dialog box, click **Menu** | **Reporting** | **Queries & Reports**, then click **Actions** | **New**.
2. Click **Events** in the Features Group and **Client Events** in the Result Types, and click **Next**.

3 In the **Display Results As** pane, click **List**, then click **Table**, then click **Next**.



What type of chart do you want to use to show summary data?

Table will not be re-sortabl

This chart type displays query results as a paginated table, allowing yo

This type of chart cannot be used as a dashboard monitor.

Click "Next" to select the columns for the ta

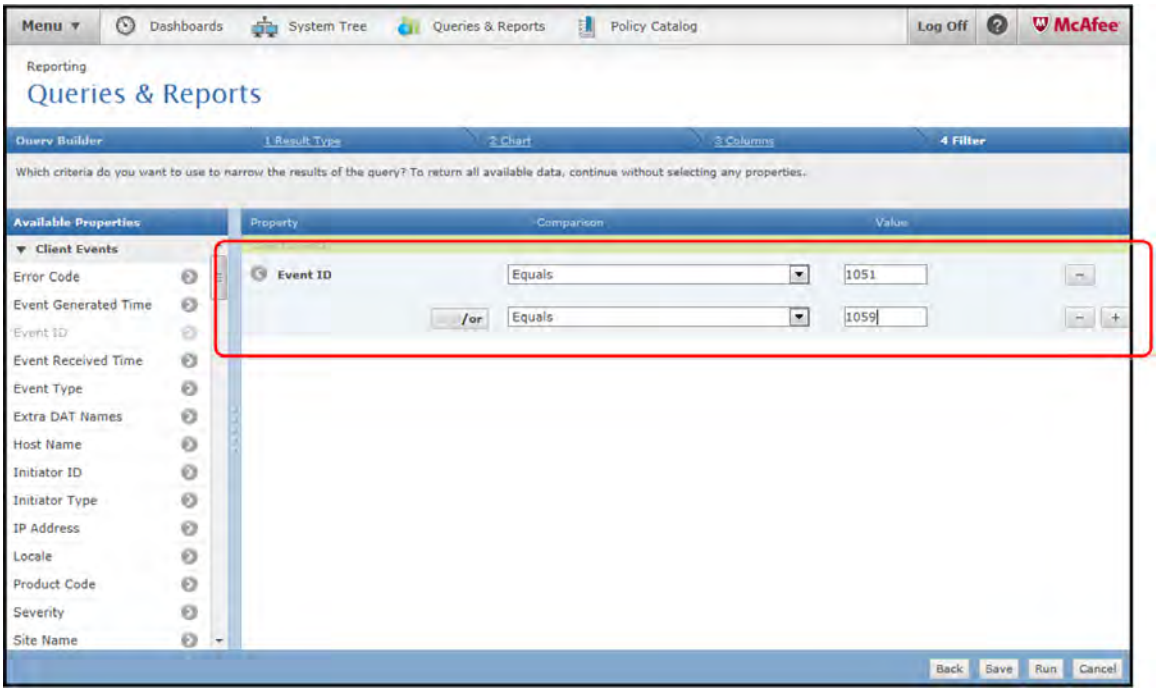
**Figure 7-13 Query Builder showing table format selected**

4 Click **Next** to skip the Columns dialog box.

> You can skip this step because McAfee ePO does not use the columns you choose in the server task.

5 In **Available Properties** under **Client Events**, click **Event ID** to create an Event ID filter.

An Event ID row is added in the Filter pane.



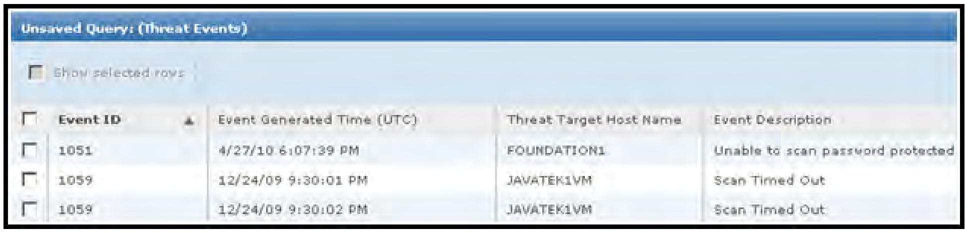
Which criteria do you want to use to narrow the results of the query? To return all available data, continue without selecting any properties.

Event ID — Equals — 1051
/or — Equals — 1059

**Figure 7-14 Query Builder with Event ID filter**

6 Click the plus sign, **+**, at the right to add another Event ID comparison row, select equals in the Comparison column, add `1051` and `1059` in the Value column; then click **Save** and **Run**.

This setting filters the query and returns only 1051 and 1059 events, as shown in the following output figure.


Unsaved Query: (Threat Events)

□ Show selected rows

| □ | Event ID ▲ | Event Generated Time (UTC) | Threat Target Host Name | Event Description |
|---|---|---|---|---|
| □ | 1051 | 4/27/10 6:07:39 PM | FOUNDATION1 | Unable to scan password protected |
| □ | 1059 | 12/24/09 9:30:01 PM | JAVATEK1VM | Scan Timed Out |
| □ | 1059 | 12/24/09 9:30:02 PM | JAVATEK1VM | Scan Timed Out |

**Figure 7-15 Query Builder output**

7 (Optional) You can select all these 1051 and 1059 events, then click **Actions | Purge** to purge them in real time. You can filter which events to purge based on those events older than X Days, Weeks, Months, or Years. Or you can Purge using a specific previously defined query.

> Instead of purging the events in real time during business hours, you can create a server task that runs the purge nightly during off hours.

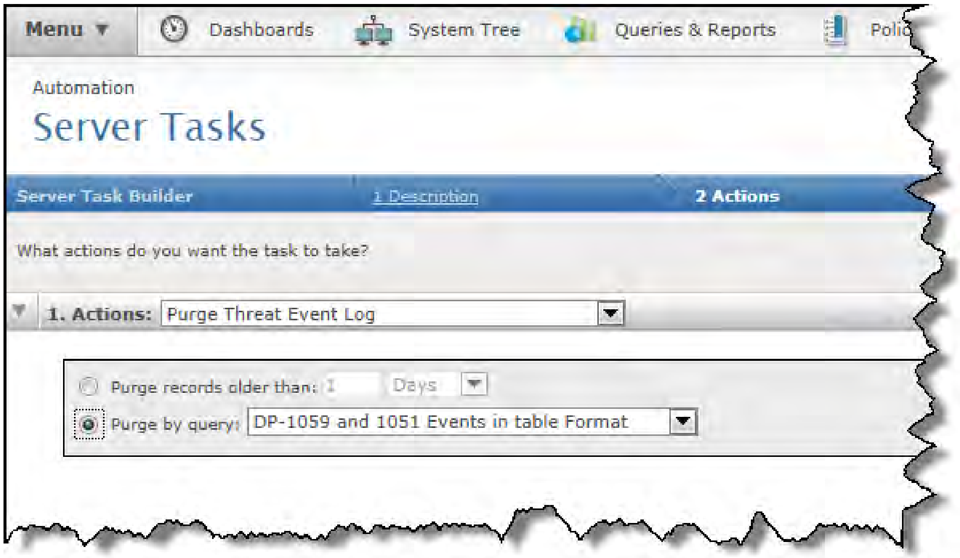
8 To create a new server task, click **Menu** | **Automation** | **Server Tasks** and click **Actions** | **New Task**.

9 Give the task an appropriate name and Description; then click **Next**.

For example, `Purge of 1051 and 1059 Events Nightly`.

10 Click **Purge Threat Event Log** from the Actions list, then click **Purge by Query**.

11 In the list, find and click the custom query that you just created.



What actions do you want the task to take?

1. Actions: Purge Threat Event Log

○ Purge records older than: 1 Days

● Purge by query: DP-1059 and 1051 Events in table Format

**Figure 7-16 Query Builder with Purge Threat Event Log selected**

12 Schedule the task to run every night, then click **Save**.

**See also**

*Filtering 1051 and 1059 events* on page 174
*Purging events automatically* on page 170

8

# Running reports with the web API

The McAfee ePO API framework allows you to run commands from a web URL or use any scripting language to create command-line scripts to automate common management activities.

This section describes creating web URLs to run queries. For detailed examples of command-line scripts and tools, see the McAfee ePolicy Orchestrator web API Scripting Guide.

**Contents**

## Using the web URL API or the McAfee ePO user interface

You can run queries using the web URL application programming interface (API) instead of using the McAfee ePO user interface.

Using the web URL API or the McAfee ePO user interface, you can:

- Run the URL and display the output as a list of text
- Manipulate the text output using other scripts and tools
- Modify the query
- Filter the output using Boolean operators that aren't available in the user interface

For example, you can run the **New Agents Added to ePO per Week** query in the McAfee ePO user interface and get this output.

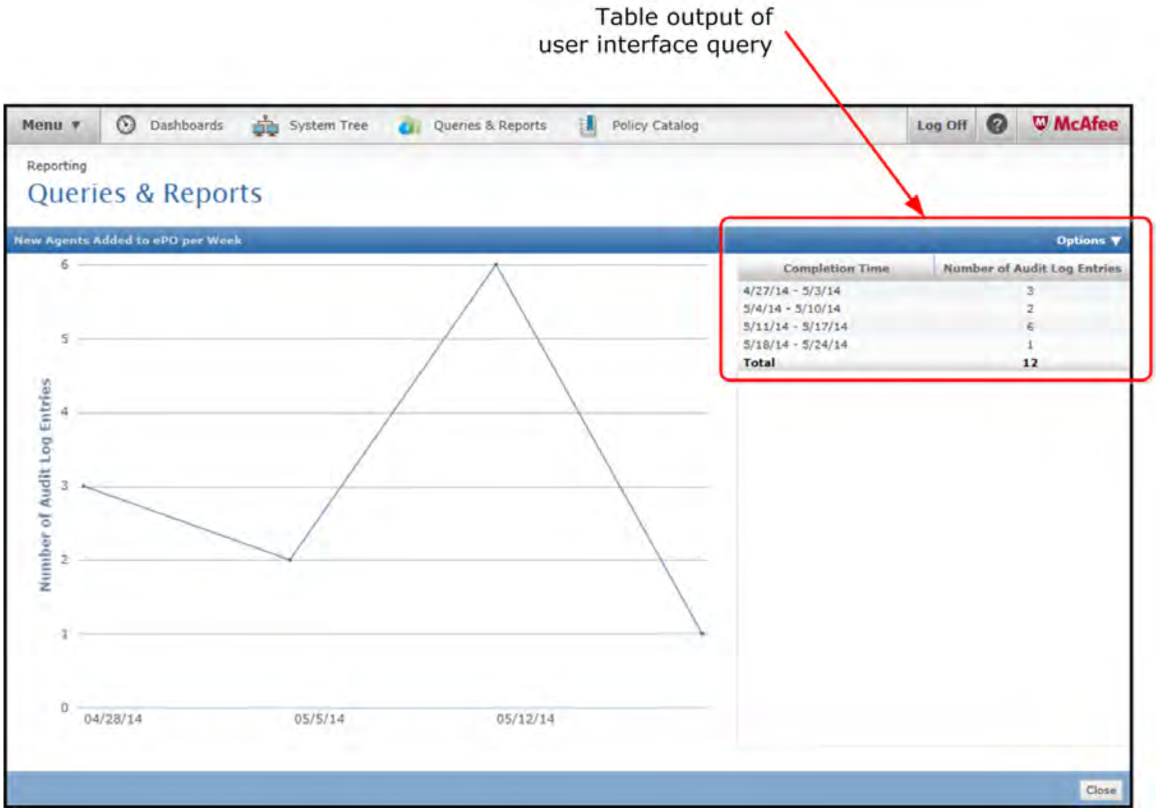


Table output of user interface query

| Completion Time | Number of Audit Log Entries |
|---|---|
| 4/27/14 - 5/3/14 | 3 |
| 5/4/14 - 5/10/14 | 2 |
| 5/11/14 - 5/17/14 | 6 |
| 5/18/14 - 5/24/14 | 1 |
| **Total** | **12** |

**Figure 8-1 Query output with the user interface**

To run this query, click **Menu** | **Reporting** | **Queries & reports**, select **New Agents Added to ePO per Week** query, then click **Actions** | **Run**.

Or you can paste this web URL query in your browser address bar.

```
https://<localHost>:8443/remote/core.executeQuery?queryId=34&:output=terse
```

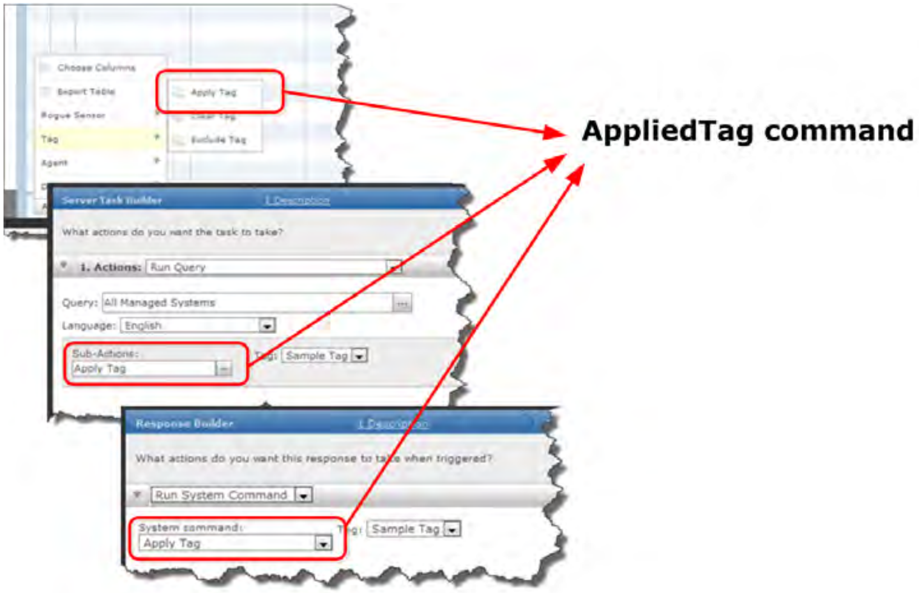
```
OK:
count Completion Time (Week)
----- ----------------------
3     4/27/14 - 5/3/14
2     5/4/14 - 5/10/14
6     5/11/14 - 5/17/14
1     5/18/14 - 5/24/14
```

## McAfee ePO command framework

The structure of the McAfee ePO framework allows you to access all McAfee ePO command objects and their parameters using the API or the user interface.

To understand the McAfee ePO framework, you can compare how the `AppliedTag` command is accessed from multiple places in the McAfee ePO user interface and the web URL.

This figure shows how the AppliedTag command is accessed from multiple places in the McAfee ePO user interface.



What actions do you want the task to take?

1. Actions: Run Query

Query: All Managed Systems

Language: English

Sub-Actions: Apply Tag

Tag: Sample Tag

What actions do you want this response to take when triggered?

Run System Command

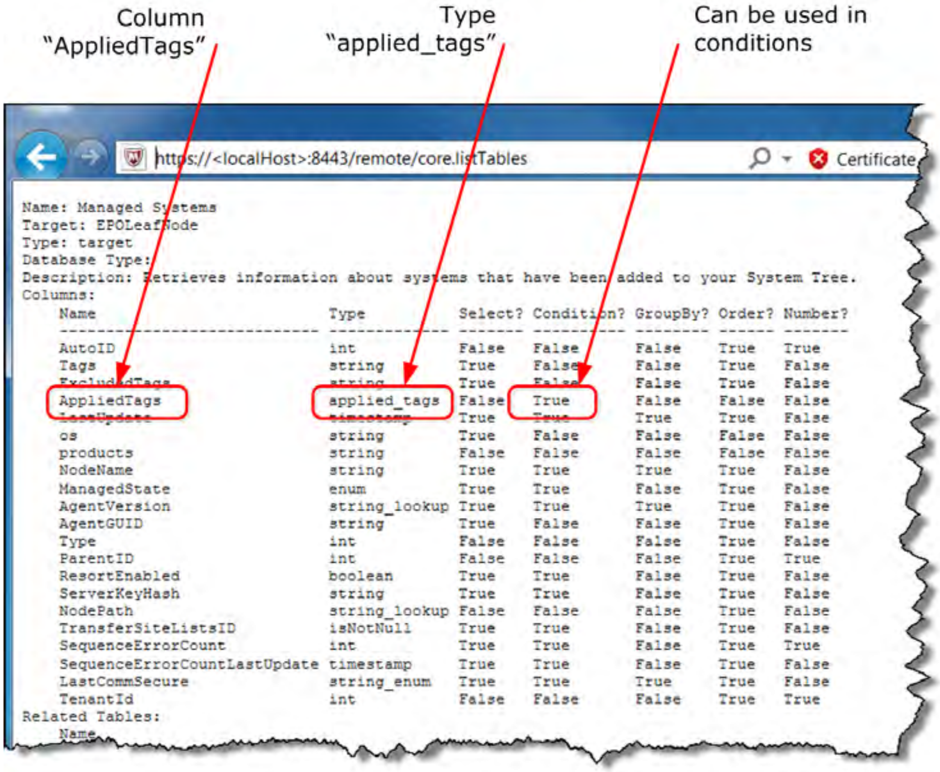
System command: Apply Tag

Tag: Sample Tag

**Figure 8-2 McAfee ePO framework command example**

This figure shows how to find valid AppliedTag command parameters using this core.listTables web URL command:

```
https://<localHost>:8443/remote/core.listTables
```



```
https://<localHost>:8443/remote/core.listTables
```

```
Name: Managed Systems
Target: EPOLeafNode
Type: target
Database Type:
Description: Retrieves information about systems that have been added to your System Tree.
Columns:
    Name                           Type          Select? Condition? GroupBy? Order? Number?
    ------------------------------ ------------- ------- ---------- -------- ------ -------
    AutoID                         int           False   False      False    True   True
    Tags                           string        True    False      False    True   False
    ExcludedTags                   string        True    False      False    True   False
    AppliedTags                    applied_tags  False   True       False    False  False
    LastUpdate                     timestamp     True    True       True     True   False
    os                             string        True    False      False    False  False
    products                       string        False   False      False    False  False
    NodeName                       string        True    True       True     True   False
    ManagedState                   enum          True    True       False    True   False
    AgentVersion                   string_lookup True    True       True     True   False
    AgentGUID                      string        True    False      False    True   False
    Type                           int           False   False      False    True   False
    ParentID                       int           False   False      False    True   True
    ResortEnabled                  boolean       True    True       False    True   False
    ServerKeyHash                  string        True    True       False    True   False
    NodePath                       string_lookup False   False      False    True   False
    TransferSiteListsID            isNotNull     True    True       False    True   False
    SequenceErrorCount             int           True    True       False    True   True
    SequenceErrorCountLastUpdate   timestamp     True    True       False    True   False
    LastCommSecure                 string_enum   True    True       True     True   False
    TenantId                       int           False   False      False    True   True
Related Tables:
    Name
```

**Figure 8-3 Applied Tag command valid parameters found using the core.listTables command**

This figure shows the Web URL command structure, and its parts, used to find the `AppliedTags` command.

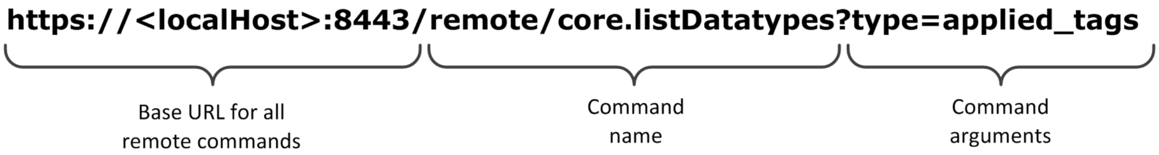

https://<localHost>:8443/remote/core.listDatatypes?type=applied_tags
Base URL for all remote commands
Command name
Command arguments

**Figure 8-4 Web URL command structure**

Following are the parts of the web URL command.

- **Basic URL** — Your remote console connection URL.

  The default port number is 8443.

- **Command name** — Appears before the `?` and is listed in the web API Help. See Using the web URL Help on page 84 to access this output.
- **Command argument** — Appears after the `?` and is separated by `&` (ampersands).

  You can also add S-Expressions to your commands. See Using S-Expressions in web URL queries on page 89 for details.

# Using the web URL Help

Use the web URL Help to learn which preconfigured queries, SQL tables, and arguments are available for your McAfee ePO web URL queries.

Use these Help commands when creating web URL queries:

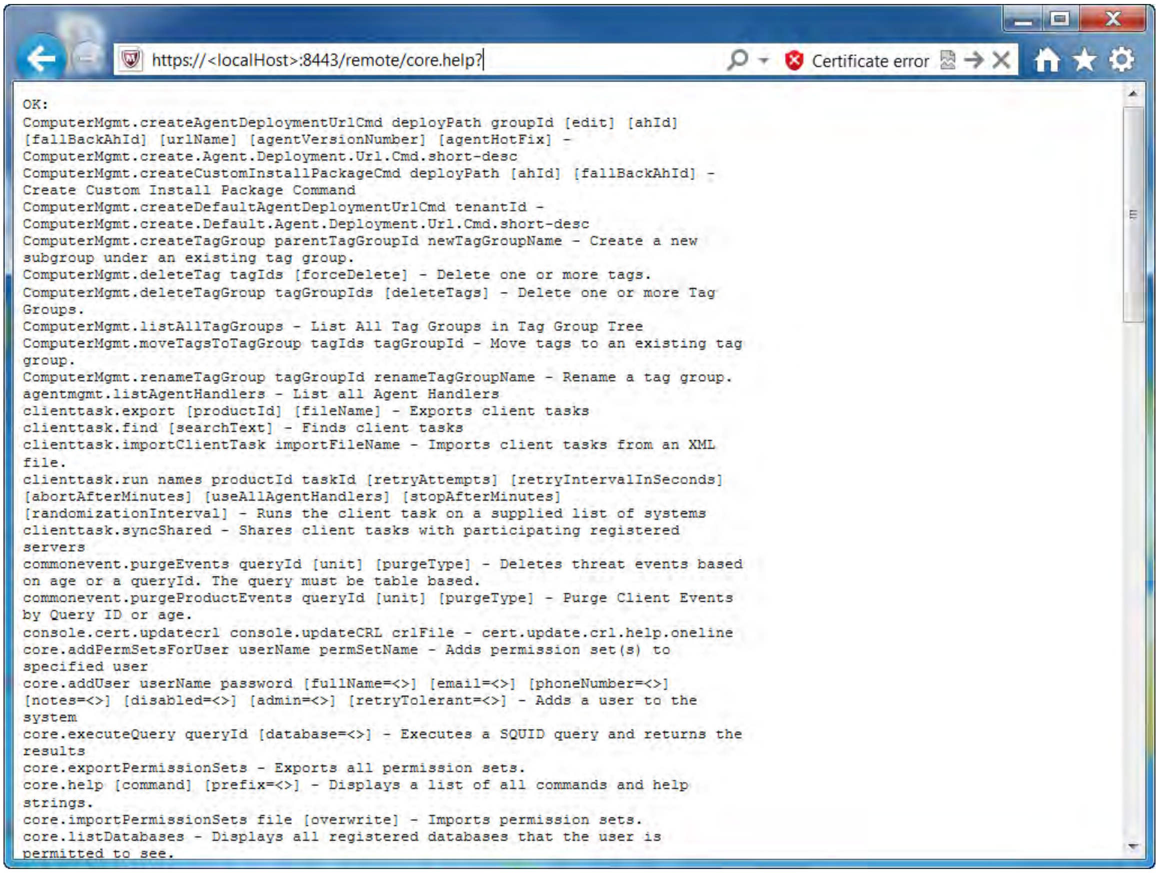
- `https://<localHost>:8443/remote/core.help?`
- `https://<localHost>:8443/remote/core.listQueries?:output=terse`
- `https://<localHost>:8443/remote/core.help?command=core.executeQuery`
- `https://<localHost>:8443/remote/core.listTables`

## Using the core.help command

All commands and their basic parameters for creating McAfee ePO web URLs are listed in the `core.help` command output.

Type this command to see the following Help.

```
https://<localHost>:8443/remote/core.help?
```



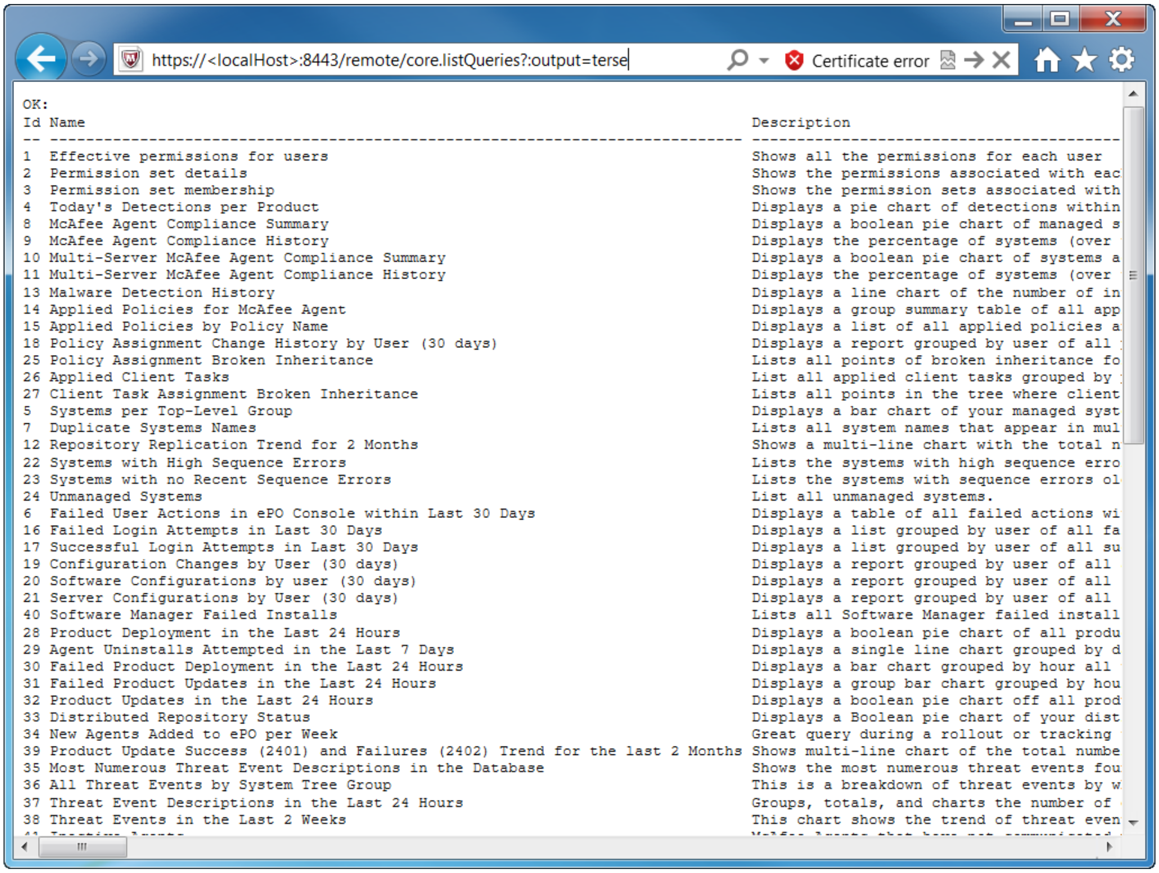
```
OK:
ComputerMgmt.createAgentDeploymentUrlCmd deployPath groupId [edit] [ahId]
[fallBackAhId] [urlName] [agentVersionNumber] [agentHotFix] -
ComputerMgmt.create.Agent.Deployment.Url.Cmd.short-desc
ComputerMgmt.createCustomInstallPackageCmd deployPath [ahId] [fallBackAhId] -
Create Custom Install Package Command
ComputerMgmt.createDefaultAgentDeploymentUrlCmd tenantId -
ComputerMgmt.create.Default.Agent.Deployment.Url.Cmd.short-desc
ComputerMgmt.createTagGroup parentTagGroupId newTagGroupName - Create a new
subgroup under an existing tag group.
ComputerMgmt.deleteTag tagIds [forceDelete] - Delete one or more tags.
ComputerMgmt.deleteTagGroup tagGroupIds [deleteTags] - Delete one or more Tag
Groups.
ComputerMgmt.listAllTagGroups - List All Tag Groups in Tag Group Tree
ComputerMgmt.moveTagsToTagGroup tagIds tagGroupId - Move tags to an existing tag
group.
ComputerMgmt.renameTagGroup tagGroupId renameTagGroupName - Rename a tag group.
agentmgmt.listAgentHandlers - List all Agent Handlers
clienttask.export [productId] [fileName] - Exports client tasks
clienttask.find [searchText] - Finds client tasks
clienttask.importClientTask importFileName - Imports client tasks from an XML
file.
clienttask.run names productId taskId [retryAttempts] [retryIntervalInSeconds]
[abortAfterMinutes] [useAllAgentHandlers] [stopAfterMinutes]
[randomizationInterval] - Runs the client task on a supplied list of systems
clienttask.syncShared - Shares client tasks with participating registered
servers
commonevent.purgeEvents queryId [unit] [purgeType] - Deletes threat events based
on age or a queryId. The query must be table based.
commonevent.purgeProductEvents queryId [unit] [purgeType] - Purge Client Events
by Query ID or age.
console.cert.updatecrl console.updateCRL crlFile - cert.update.crl.help.oneline
core.addPermSetsForUser userName permSetName - Adds permission set(s) to
specified user
core.addUser userName password [fullName=<>] [email=<>] [phoneNumber=<>]
[notes=<>] [disabled=<>] [admin=<>] [retryTolerant=<>] - Adds a user to the
system
core.executeQuery queryId [database=<>] - Executes a SQUID query and returns the
results
core.exportPermissionSets - Exports all permission sets.
core.help [command] [prefix=<>] - Displays a list of all commands and help
strings.
core.importPermissionSets file [overwrite] - Imports permission sets.
core.listDatabases - Displays all registered databases that the user is
permitted to see.
```

**Figure 8-5  Web URL core.help command output**

## Using the core.listQueries Help command

To run an existing query using the McAfee ePO web URL, use the queryID number appended to the base `core.executeQuery` command. Type this command to see the `listQueries` Help.

```
https://<localHost>:8443/remote/core.listQueries?:output=terse
```



https://<localHost>:8443/remote/core.listQueries?:output=terse
Certificate error

```
OK:
Id Name                                                                          Description
-- ----------------------------------------------------------------------------- -----------------------------------------
1  Effective permissions for users                                               Shows all the permissions for each user
2  Permission set details                                                        Shows the permissions associated with eac
3  Permission set membership                                                     Shows the permission sets associated with
4  Today's Detections per Product                                                Displays a pie chart of detections within
8  McAfee Agent Compliance Summary                                               Displays a boolean pie chart of managed s
9  McAfee Agent Compliance History                                               Displays the percentage of systems (over
10 Multi-Server McAfee Agent Compliance Summary                                  Displays a boolean pie chart of systems a
11 Multi-Server McAfee Agent Compliance History                                  Displays the percentage of systems (over
13 Malware Detection History                                                     Displays a line chart of the number of in
14 Applied Policies for McAfee Agent                                             Displays a group summary table of all app
15 Applied Policies by Policy Name                                               Displays a list of all applied policies a
18 Policy Assignment Change History by User (30 days)                            Displays a report grouped by user of all
25 Policy Assignment Broken Inheritance                                          Lists all points of broken inheritance fo
26 Applied Client Tasks                                                          List all applied client tasks grouped by
27 Client Task Assignment Broken Inheritance                                     Lists all points in the tree where client
5  Systems per Top-Level Group                                                   Displays a bar chart of your managed syst
7  Duplicate Systems Names                                                       Lists all system names that appear in mul
12 Repository Replication Trend for 2 Months                                     Shows a multi-line chart with the total n
22 Systems with High Sequence Errors                                             Lists the systems with high sequence erro
23 Systems with no Recent Sequence Errors                                        Lists the systems with sequence errors ol
24 Unmanaged Systems                                                             List all unmanaged systems.
6  Failed User Actions in ePO Console within Last 30 Days                        Displays a table of all failed actions wi
16 Failed Login Attempts in Last 30 Days                                         Displays a list grouped by user of all fa
17 Successful Login Attempts in Last 30 Days                                     Displays a list grouped by user of all su
19 Configuration Changes by User (30 days)                                       Displays a report grouped by user of all
20 Software Configurations by user (30 days)                                     Displays a report grouped by user of all
21 Server Configurations by User (30 days)                                       Displays a report grouped by user of all
40 Software Manager Failed Installs                                              Lists all Software Manager failed install
28 Product Deployment in the Last 24 Hours                                       Displays a boolean pie chart of all produ
29 Agent Uninstalls Attempted in the Last 7 Days                                 Displays a single line chart grouped by d
30 Failed Product Deployment in the Last 24 Hours                                Displays a bar chart grouped by hour all
31 Failed Product Updates in the Last 24 Hours                                   Displays a group bar chart grouped by hou
32 Product Updates in the Last 24 Hours                                          Displays a boolean pie chart off all prod
33 Distributed Repository Status                                                 Displays a Boolean pie chart of your dist
34 New Agents Added to ePO per Week                                              Great query during a rollout or tracking
39 Product Update Success (2401) and Failures (2402) Trend for the last 2 Months Shows multi-line chart of the total numbe
35 Most Numerous Threat Event Descriptions in the Database                       Shows the most numerous threat events fou
36 All Threat Events by System Tree Group                                        This is a breakdown of threat events by w
37 Threat Event Descriptions in the Last 24 Hours                                Groups, totals, and charts the number of
38 Threat Events in the Last 2 Weeks                                             This chart shows the trend of threat even
41 Inactive Agents                                                               McAfee Agents that have not communicated
```

**Figure 8-6  Web URL listQueries command output**

See Query with ID number on page 95 for an example of running the following command:

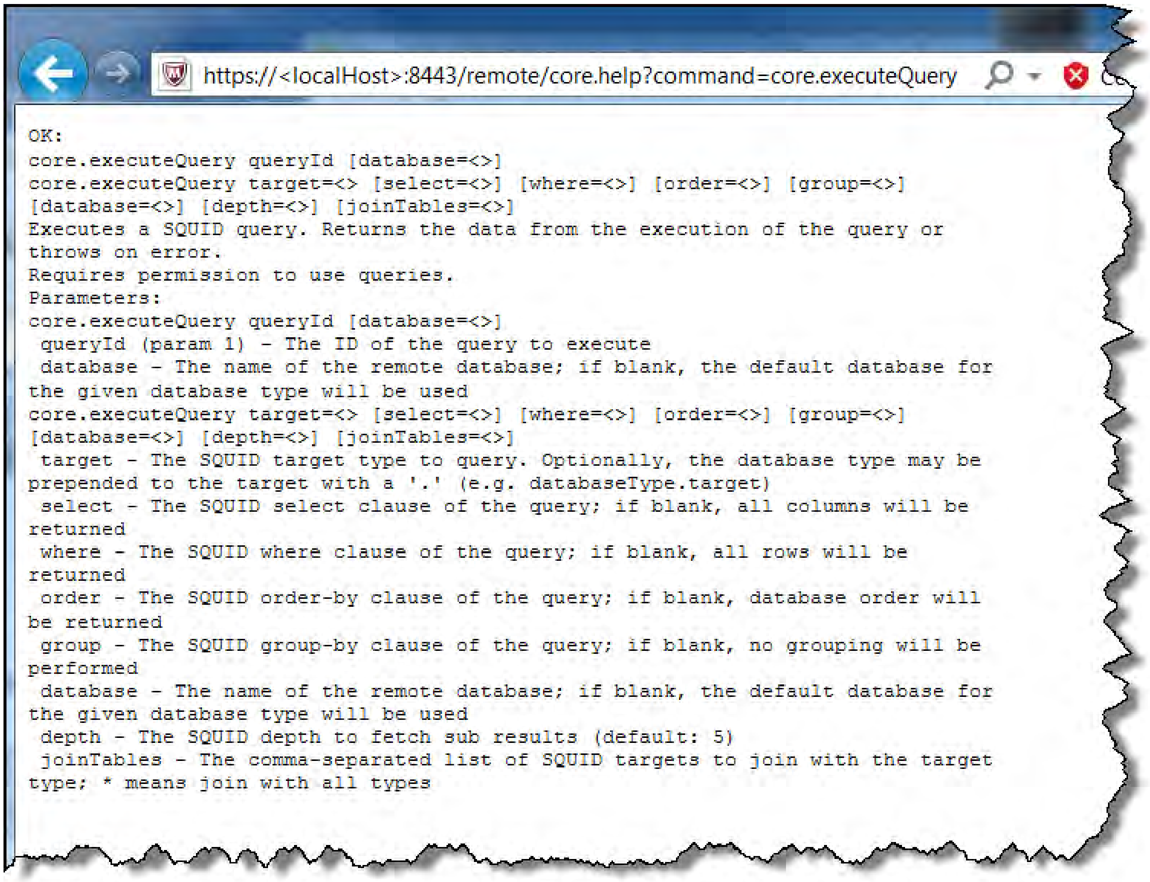
```
https://<localHost>:8443/remote/core.executeQuery?queryId=<IdNumber>
```

## Using the core.executeQuery Help command

Before you can create a McAfee ePO web URL query, or modify query parameters exported from an existing query, you must know which commands and arguments are available.

Type this command to see the `core.executeQuery` Help.

`https://<localHost>:8443/remote/core.help?command=core.executeQuery`



https://<localHost>:8443/remote/core.help?command=core.executeQuery

```
OK:
core.executeQuery queryId [database=<>]
core.executeQuery target=<> [select=<>] [where=<>] [order=<>] [group=<>]
[database=<>] [depth=<>] [joinTables=<>]
Executes a SQUID query. Returns the data from the execution of the query or
throws on error.
Requires permission to use queries.
Parameters:
core.executeQuery queryId [database=<>]
 queryId (param 1) - The ID of the query to execute
 database - The name of the remote database; if blank, the default database for
the given database type will be used
core.executeQuery target=<> [select=<>] [where=<>] [order=<>] [group=<>]
[database=<>] [depth=<>] [joinTables=<>]
 target - The SQUID target type to query. Optionally, the database type may be
prepended to the target with a '.' (e.g. databaseType.target)
 select - The SQUID select clause of the query; if blank, all columns will be
returned
 where - The SQUID where clause of the query; if blank, all rows will be
returned
 order - The SQUID order-by clause of the query; if blank, database order will
be returned
 group - The SQUID group-by clause of the query; if blank, no grouping will be
performed
 database - The name of the remote database; if blank, the default database for
the given database type will be used
 depth - The SQUID depth to fetch sub results (default: 5)
 joinTables - The comma-separated list of SQUID targets to join with the target
type; * means join with all types
```

**Figure 8-7 Web URL core.executeQuery output**

This table lists `core.executeQuery` Help.

Optional parameters and options appear in square brackets "[...]."

**Table 8-1 Web URL core.executeQuery Help**

| Command | Arguments | Parameters | Options | Description |
|---|---|---|---|---|
| core.executeQuery | queryId | — | — | Executes a SQUID query. Returns the data from the execution of the query or displays on error. |
| | | [database=<>] | — | The name of the remote database; if blank, the default database for the given database type is used. |
| core.executeQuery | | target= | — | The SQUID target type to query. Optionally, you can add "." and the database type before the target. For example, `databaseType.target`. |
| | | | [select=<>] | The SQUID select clause of the query; if blank, all columns are returned. |

**Table 8-1 Web URL core.executeQuery Help** *(continued)*

| Command | Arguments | Parameters | Options | Description |
|---|---|---|---|---|
| | | | [where=<>] | The SQUID where clause of the query; if blank, all rows are returned. |
| | | | [order=<>] | The SQUID order-by clause of the query; if blank, database order is returned. |
| | | | [group=<>] | The SQUID group-by clause of the query; if blank, no grouping is performed. |
| | | | [database=<>] | The name of the remote database; if blank, the default database for the given database type is used. |
| | | | [depth=<>] | The SQUID depth to fetch sub-results. (default: 5). |
| | | | [joinTables=<>] | The comma-separated list of SQUID targets to join with the target type; "*" means join all types. |

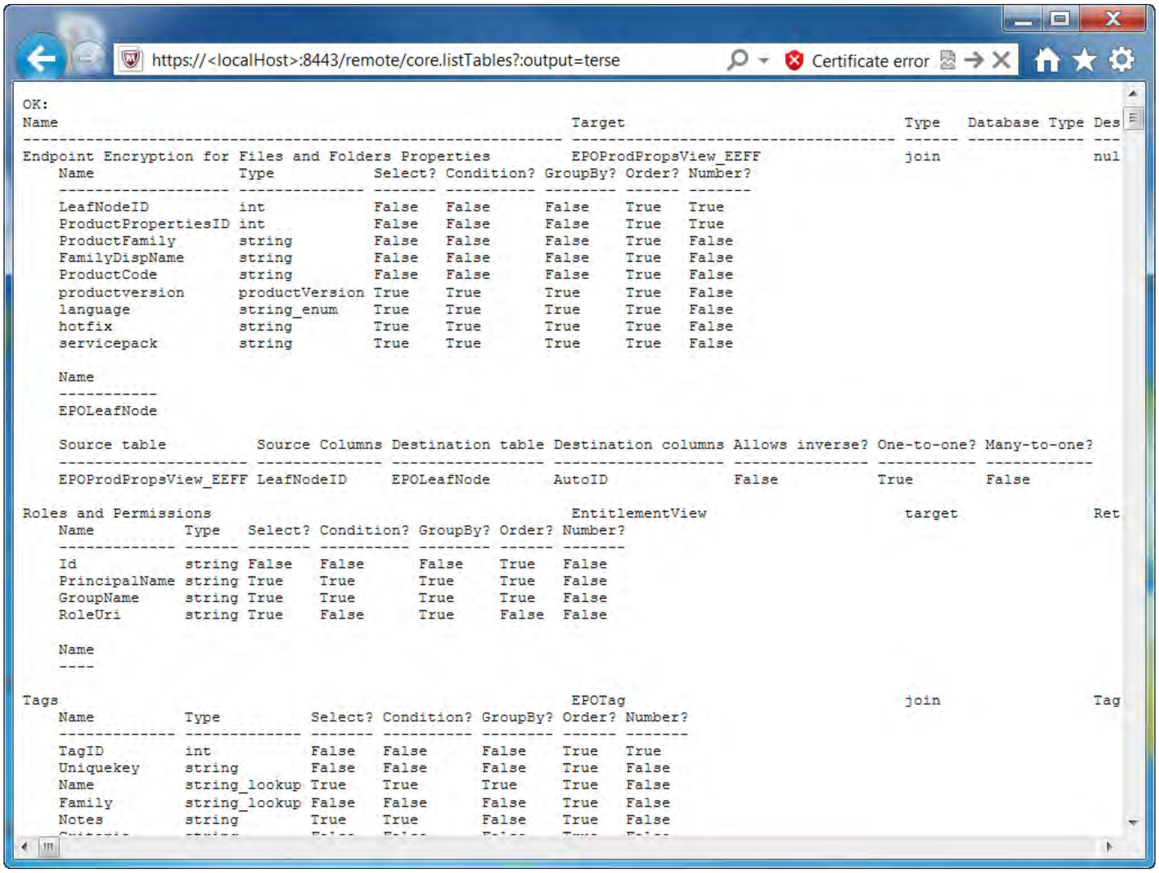
## Using the core.listTables Help command

To create a McAfee ePO web URL query or to modify query parameters exported from an existing query, you must know the names of the SQL tables and their parameters. These three commands provide that information.

- **https://<localHost>:8443/remote/core.listTables** — Lists all SQL tables and their parameters
- **https://<localHost>:8443/remote/core.listTables?:output=terse** — Lists a summary of all SQL tables and their parameters
- **https://<localHost>:8443/remote/core.listTables?table=<tableName>** — Lists all arguments for a specific SQL table

Type this command to see the `core.listTables` Help.

```
https://<localHost>:8443/remote/core.listTables?:output=terse
```


https://<localHost>:8443/remote/core.listTables?:output=terse
Certificate error

```
OK:
Name                                                         Target                                Type   Database Type Des
------------------------------------------------------------ ------------------------------------  ------ ------------- ---
Endpoint Encryption for Files and Folders Properties         EPOProdPropsView_EEFF                 join                 nul
    Name                Type           Select? Condition? GroupBy? Order? Number?
    ------------------- -------------- ------- ---------- -------- ------ -------
    LeafNodeID          int            False   False      False    True   True
    ProductPropertiesID int            False   False      False    True   True
    ProductFamily       string         False   False      False    True   False
    FamilyDispName      string         False   False      False    True   False
    ProductCode         string         False   False      False    True   False
    productversion      productVersion True    True       True     True   False
    language            string_enum    True    True       True     True   False
    hotfix              string         True    True       True     True   False
    servicepack         string         True    True       True     True   False

    Name
    -----------
    EPOLeafNode

    Source table          Source Columns Destination table Destination columns Allows inverse? One-to-one? Many-to-one?
    --------------------- -------------- ----------------- ------------------- --------------- ----------- ------------
    EPOProdPropsView_EEFF LeafNodeID     EPOLeafNode       AutoID              False           True        False

Roles and Permissions                                        EntitlementView                       target               Ret
    Name          Type   Select? Condition? GroupBy? Order? Number?
    ------------- ------ ------- ---------- -------- ------ -------
    Id            string False   False      False    True   False
    PrincipalName string True    True       True     True   False
    GroupName     string True    True       True     True   False
    RoleUri       string True    False      True     False  False

    Name
    ----

Tags                                                         EPOTag                                join                 Tag
    Name          Type          Select? Condition? GroupBy? Order? Number?
    ------------- ------------- ------- ---------- -------- ------ -------
    TagID         int           False   False      False    True   True
    Uniquekey     string        False   False      False    True   False
    Name          string_lookup True    True       True     True   False
    Family        string_lookup False   False      False    True   False
    Notes         string        True    True       False    True   False
```

**Figure 8-8 Web URL core.listTables output**

To list only the parameters for a specific table, use this command:

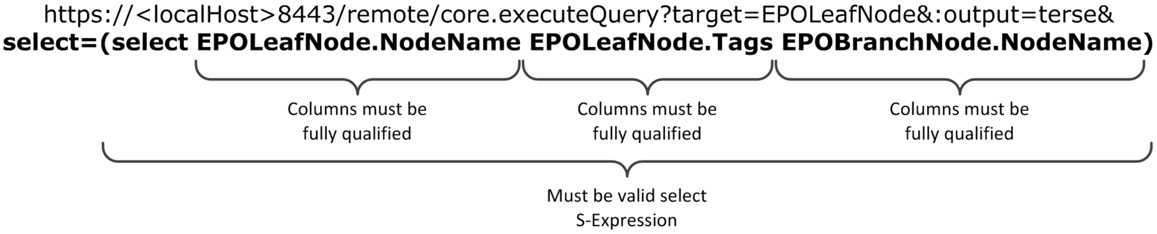
```
https://<localHost>:8443/remote/core.listTables?table=<tableName>
```

# Using S-Expressions in web URL queries

You can use S-Expressions (Symbolic Expressions) in your McAfee ePO web URL commands to select specific command objects and their parameters and joint tables, then group, sort, and order the output.

Use the `core.executeQuery` command with the `[select=<>]` option to create S-Expressions.

This figure shows the basic requirements for a fully qualified S-Expression query.



https://<localHost>8443/remote/core.executeQuery?target=EPOLeafNode&:output=terse&
**select=(select EPOLeafNode.NodeName EPOLeafNode.Tags EPOBranchNode.NodeName)**

Columns must be fully qualified
Columns must be fully qualified
Columns must be fully qualified
Must be valid select S-Expression

**Figure 8-9 Web URL query with S-Expression**

A fully qualified S-Expression has these parts:

- `select=(select ...)` — S-Expression function format.
- `<tableName>.<argumentName>` — The names of the SQL table columns you want to display and manipulate. For example, **EPOLeafNode.NodeName** is a managed system name and **EPOBranchNode.NodeName** is a System Tree group name.

In this example web URL query, the **EPOLeafNode** and **EPOBranchNode** tables are automatically joined to fulfill the query.

> The two tables in this example must be fully qualified, or related, for the automatic join to work.

To find the valid parameters for the target tables and to confirm the table relationships, see Using the web URL Help on page 84.

## Group, sort, order, and filter web URL query output

Within your web URL query S-Expressions, you can group, sort, order, and filter web URL query using the arguments listed for the `core.executeQuery` command. See Using the web URL Help on page 84, for a partial list of the core.`executeQuery` command options.

### Ordering the output

Before you can configure a sort order for your web URL query output, you must determine if the data in a table column can be sorted. Use this command to confirm the column data can be sort ordered.

```
https://<localHost>:8443/remote/core.listTables?table=<tableName>
```

This example confirms you can sort the `EPOBranchNode` table `NodeName` column data. In the `NodeName` row, `True` is listed in the `Order ?` column.

```
https://<localHost>:8443/remote/core.listTables?table=EPOBranchNode
```

This command displays this Help.

```
OK:
Name: Groups
Target: EPOBranchNode
Type: join
Database Type:
Description: null
Columns:
    Name          Type          Select? Condition? GroupBy? Order? Number?
    ------------- ------------- ------- ---------- -------- ------ -------
    AutoID        group         False   True       False    True   True
    NodeName      string        True    False      True     True   False
    L1ParentID    group         False   False      True     True   True
    L2ParentID    group         False   False      True     True   True
    Type          int           False   False      False    True   True
    BranchState   int           False   False      False    True   True
    Notes         string        True    True       False    True   False
    NodePath      string        False   False      False    True   False
    NodeTextPath  string_lookup True    True       True     True   False
    NodeTextPath2 string_lookup True    True       True     True   False
Related Tables:
    Name
    ----
Foreign Keys: None
```

This `Order` command is used to sort the McAfee ePO branch nodes, or System Tree Group Names, in descending order.

```
https://<localHost>:8443//remote/core.executeQuery?
target=EPOLeafNode&:output=terse&select=(select EPOLeafNode.NodeName EPOLeafNode.Tags
EPOBranchNode.NodeName&order=(order(desc EPOBranchNode.NodeName)
```

This is the command output.

```
OK:
System Name     Tags         Group Name
--------------- ------------ --------------
DP-2K12R2S-SRVR Server       SuperAgents
DP-2K8ER2EPO510 Server       Servers
DP-W7PIP-1      Workstation  NAT Systems
DP-W7PIP-2      Workstation  NAT Systems
DP-W7PIP-3      Workstation  NAT Systems
DP-EN-W7E1XP-2               Lost&Found
DP-2K8AGTHDLR   Server, test Agent handlers
```

### Grouping the output

This command groups, or counts, the System Tree system names, and groups them by McAfee ePO branch nodes, or System Tree Group Names.

```
https://<localHost>:8443/remote/core.executeQuery?
target=EPOLeafNode&:output=terse&select=(select EPOBranchNode.NodeName (count))&group=(group
EPOBranchNode.NodeName)
```

This is the command output.

```
OK:
Group Name     count
-------------- -----
Agent handlers 1
Lost&Found     1
NAT Systems    3
Servers        1
SuperAgents    1
```

## Filtering the output using a string

This command filters the System Tree system names to display only the names with the string "2k8" in the name.

```
https://<localHost>:8443/remote/core.executeQuery?
target=EPOLeafNode&:output=terse&select=(select EPOLeafNode.NodeName EPOLeafNode.Tags
EPOBranchNode.NodeName)&where=(contains EPOLeafNode.NodeName "2k8")
```

This is the command output displaying only the names with the string "2k8" in the name.

```
OK:
System Name     Tags         Group Name
--------------- ------------ --------------
DP-2K8ER2EPO510 Server       Servers
DP-2K8AGTHDLR   Server, test Agent handlers
```

## Filtering the output using the top <number> of the list

This command filters the System Tree system names to only display the top 3 names in the list.

```
https://<localHost>:8443/remote/core.executeQuery?
target=EPOLeafNode&:output=terse&select=(select (top 3) EPOLeafNode.NodeName
EPOLeafNode.Tags EPOBranchNode.NodeName)
```

This is the command output displaying the top 3 names in the list.

```
OK:
System Name     Tags   Group Name
--------------- ------ -----------
```

```
DP-2K8ER2EPO510 Server Servers
DP-2K12R2S-SRVR Server SuperAgents
DP-EN-W7E1XP-2         Lost&Found
```

### Filtering the output using common attributes

This command filters the System Tree systems to display only a specific number of common attributes.

```
https://<localHost>:8443/remote/core.executeQuery?
target=EPOLeafNode&:output=terse&select=(select EPOLeafNode.NodeName EPOLeafNode.Tags
EPOBranchNode.NodeName)&where=(hasTag EPOLeafNode.AppliedTags 4)
```

This is the command output with 4 common attributes.

```
OK:
System Name Tags           Group Name
----------- -------------- -----------
DP-W7PIP-1  7, Workstation Workstation
DP-W7PIP-2  7, Workstation Workstation
DP-W7PIP-3  7, Workstation Workstation
```

#### You can combine filters

You can use the most common filters `AND` and `OR`. For example:

- `(AND <expression> <expression> …)`
- `(OR <expression> <expression> …)`
- They can be combined in any combination. For example: `(AND (hasTag EPOLeafNode.AppliedTags 3) (contains EPOLeafNode.NodeName “100”))`

  Parentheses must be matched.

You can also use filters that can’t be constructed in the McAfee ePO user interface. For example:

```
(OR
    (AND (hasTag EPOLeafNode.AppliedTags 3)
              (contains EPOLeafNode.NodeName “100”))
    (AND (hasTag EPOLeafNode.AppliedTags 4)
              (contains EPOLeafNode.NodeName “100”))
)
```

## Parsing query export data to create web URL queries

You can use the data exported from existing queries to create valid web URL queries and S-Expressions.

See the McAfee ePolicy Orchestrator Product Guide for details about exporting query definitions.

The following example is the exported data from the preconfigured VSE: DAT Deployment query. This exported file is used to describe the steps and processes to create a web URL queries.

```
<list id="1">
  <query id="2">
    <dictionary id="3"/>
    <name>VSE: DAT Deployment</name>
    <description>Displays the three highest DAT versions, and a slice for all the other
versions.</description>
    <target>EPOLeafNode</target>
    <table-uri>query:table?orion.table.columns=EPOComputerProperties.ComputerName
%3AEPOComputerProperties.DomainName%3AEPOLeafNode.os%3AEPOComputerProperties.Description
```

```
%3AEPOLeafNode.Tags%3AEPOProdPropsView_VIRUSCAN.productversion
%3AEPOProdPropsView_VIRUSCAN.hotfix%3AEPOProdPropsView_VIRUSCAN.servicepack
%3AEPOProdPropsView_VIRUSCAN.enginever
%3AEPOProdPropsView_VIRUSCAN.enginever64%3AEPOProdPropsView_VIRUSCAN.datver
%3AEPOLeafNode.LastUpdate&amp;orion.table.order.by=EPOComputerProperties.ComputerName
%3AEPOComputerProperties.DomainName%3AEPOLeafNode.os%3AEPOComputerProperties.Description
%3AEPOLeafNode.Tags%3AEPOProdPropsView_VIRUSCAN.productversion
%3AEPOProdPropsView_VIRUSCAN.hotfix%3AEPOProdPropsView_VIRUSCAN.servicepack
%3AEPOProdPropsView_VIRUSCAN.enginever
%3AEPOProdPropsView_VIRUSCAN.enginever64%3AEPOProdPropsView_VIRUSCAN.datver
%3AEPOLeafNode.LastUpdate&amp;orion.table.order=az</table-uri>
    <condition-uri>query:condition?orion.condition.sexp=%28+where+%28+version_ge
+EPOProdPropsView_VIRUSCAN.productversion+%228%22+%29+%29</condition-uri>
    <summary-uri>query:summary?
pie.slice.title=EPOProdPropsView_VIRUSCAN.datver&amp;pie.count.title=EPOLeafNode&amp;orion.qu
ery.type=pie.pie&amp;orion.sum.query=true&amp;orion.sum.group.by=EPOProdPropsView_VIRUSCAN.da
tver&amp;orion.sum.order=desc&amp;orion.show.other=true&amp;orion.sum.aggregation=count&amp;o
rion.sum.aggregation.showTotal=true</summary-uri>
  </query>
</list>
```

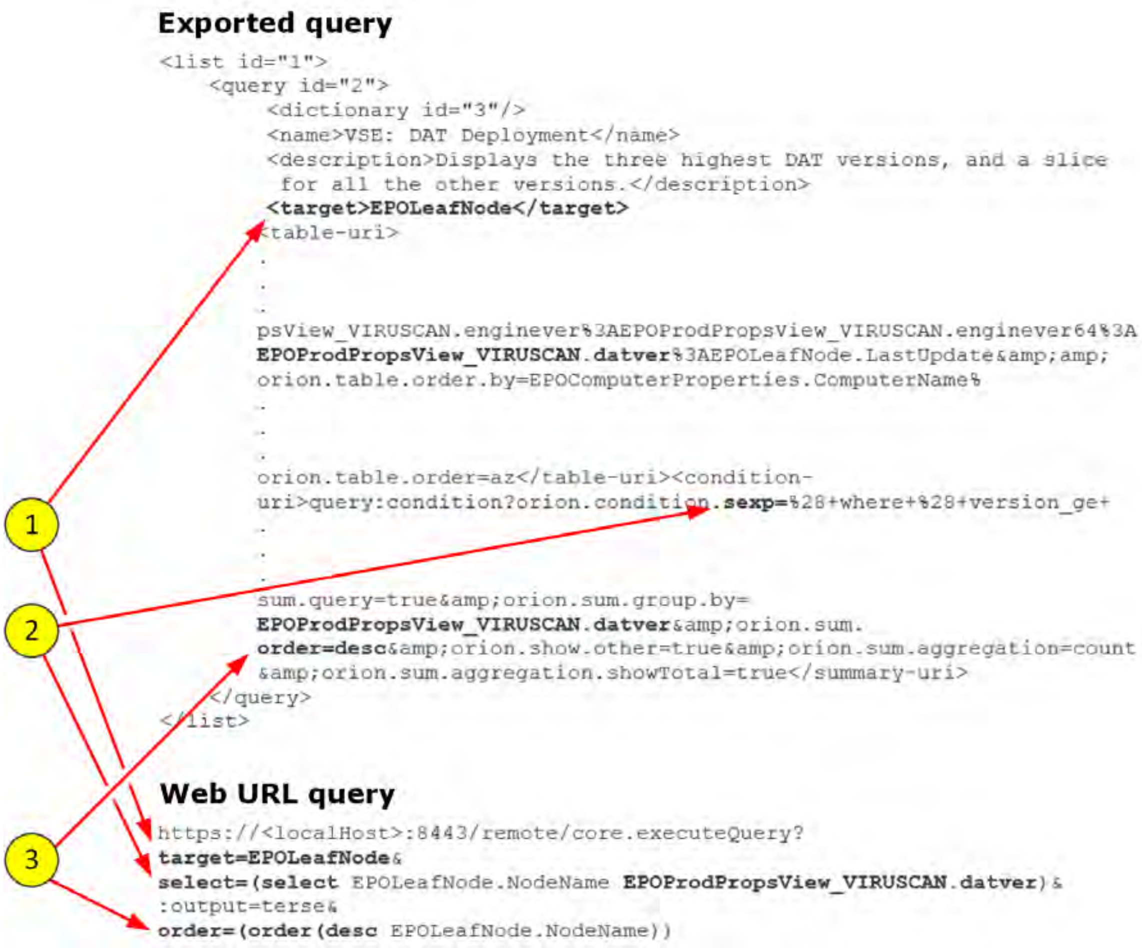
The exported query contains strings that are URL-encoded. Use this table to convert the URL-encoded characters to valid web URL query characters.

**Table 8-2 Convert URL-encoded characters to web URL query characters**

| URL-encoded characters | Web URL query characters |
|---|---|
| %22 | quotation marks ""..."" |
| "+" | space " " |
| %28 | opening parenthesis "(" |
| %29 | closing parenthesis ")" |
| &amp | ampersand "&" |
| az (in an order command) | "asc" = ascending order |
| za (in an order command) | "desc" = descending order |

## XML query data file structure

The XML query export data file is separated into sections of data. Some sections aren't used in your final web URL query, and some sections can be used almost as they appear.



**Exported query**

```
<list id="1">
    <query id="2">
         <dictionary id="3"/>
         <name>VSE: DAT Deployment</name>
         <description>Displays the three highest DAT versions, and a slice
          for all the other versions.</description>
         <target>EPOLeafNode</target>
        <table-uri>
        .
        .
        .
        psView_VIRUSCAN.enginever%3AEPOProdPropsView_VIRUSCAN.enginever64%3A
        EPOProdPropsView_VIRUSCAN.datver%3AEPOLeafNode.LastUpdate&amp;amp;
        orion.table.order.by=EPOComputerProperties.ComputerName%
        .
        .
        .
        orion.table.order=az</table-uri><condition-
        uri>query:condition?orion.condition.sexp=%28+where+%28+version_ge+
        .
        .
        .
        sum.query=true&amp;orion.sum.group.by=
        EPOProdPropsView_VIRUSCAN.datver&amp;orion.sum.
        order=desc&amp;orion.show.other=true&amp;orion.sum.aggregation=count
        &amp;orion.sum.aggregation.showTotal=true</summary-uri>
    </query>
</list>
```

**Web URL query**

```
https://<localHost>:8443/remote/core.executeQuery?
target=EPOLeafNode&
select=(select EPOLeafNode.NodeName EPOProdPropsView_VIRUSCAN.datver)&
:output=terse&
order=(order(desc EPOLeafNode.NodeName))
```

Figure 8-10 Exported query and web URL query data comparison

The commands in the `<summary-uri>query:` code creates the pie chart and are not used to create the web URL query output. The `order=desc` parameter is shown as a sorting and grouping example in the final web URL query

This table lists the numbers shown in the figure, the major sections of the exported query and the final web URL query, and how they are used.

Table 8-3 Convert URL-encoded characters to web URL query characters

| Number | Exported query | Web URL query | Description |
|---|---|---|---|
| 1 | <target>...</target> | target=... | Lists the table parsed in the query. |
| 2 | sexp=... | select=(select... | Lists the S-Expressions command objects, their parameters, and joint tables. |
| 3 | order=... | order=(order(... | Lists the sort order used in the output. |

See the *Convert URL-encoded characters to web URL query characters* table to convert more data to use in your web URL query.

### Web URL query separated into parts

Using the information from the existing query exported XML file, you can create this file, with line breaks for clarity:

```
https://<localHost>8443/remote/core.executeQuery?

target=EPOLeafNode&

select=(select EPOLeafNode.NodeName EPOProdPropsView_VIRUSCAN.datver)&

:output=terse&

order=(order(desc EPOLeafNode.NodeName))
```

The `?` and `&`s indicate the different parts of the web URL query.

When you remove the line breaks, this example is final web URL query.

```
https://<localHost>:8443/remote/core.executeQuery?target=EPOLeafNode&select=(select
EPOLeafNode.NodeName EPOProdPropsView_VIRUSCAN.datver)&:output=terse& order=(order(desc
EPOLeafNode.NodeName))
```

Following is the output of the web URL query.

```
OK:
System Name      DAT Version (VirusScan Enterprise)
---------------- ----------------------------------
DP-W7PIP-3       7465.0000
DP-W7PIP-2       7429.0000
DP-W7PIP-1       7437.0000
DP-EN-W7E1XP-2
DP-2K8ER2EPO510  7465.0000
DP-2K8AGTHDLR    7437.0000
DP-2K12R2S-SRVR
```

# Web URL query examples

You can create simple web URL queries using the existing query ID number, or create complex queries by modifying an existing query.

Use the web URL Help to add commands with complex objects and S-Expressions.

## Query with ID number

The quickest way to run a query using a web URL is to use the preconfigured query ID, then use the output from the web browser in other scripts or in an email.

**Before you begin**

You must have administer permissions to run the query.

Running web API queries is quicker than running a query using the McAfee ePO user interface. Plus, you can use their output in scripts and redirect the output and port it for further processing.

For example, to access this output screen using the McAfee ePO user interface, click **Menu** | **Reports** | **Queries & Reports**, find and select the **New Agents Added to ePO per Week** query, and click **Actions** | **Run**. These steps display this query output in the user interface.

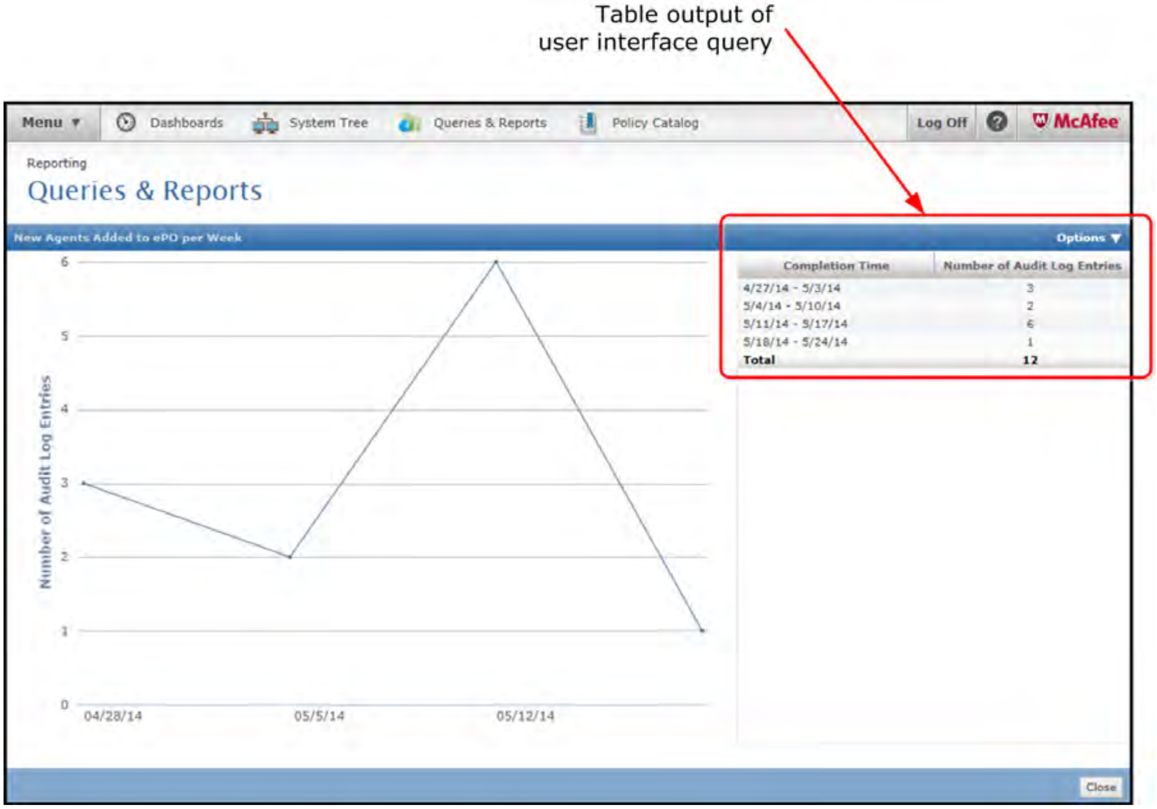


Table output of user interface query

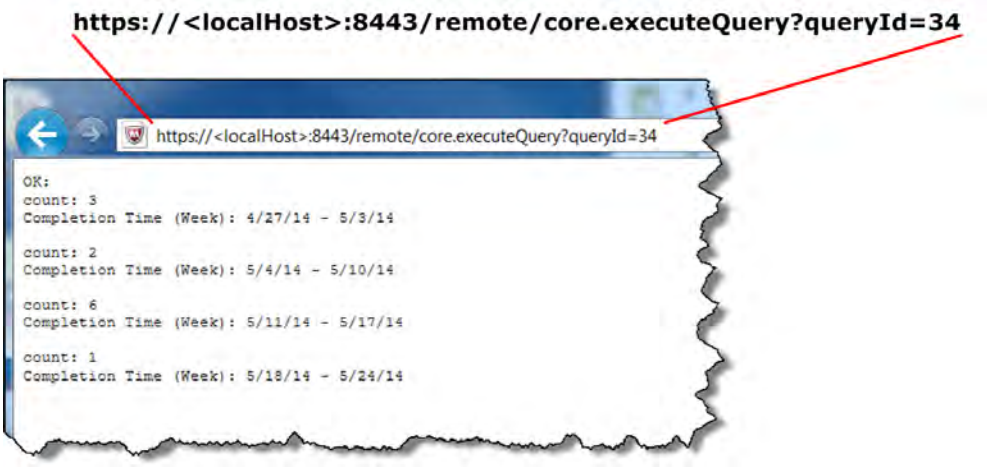
| Completion Time | Number of Audit Log Entries |
|---|---|
| 4/27/14 - 5/3/14 | 3 |
| 5/4/14 - 5/10/14 | 2 |
| 5/11/14 - 5/17/14 | 6 |
| 5/18/14 - 5/24/14 | 1 |
| **Total** | **12** |

Figure 8-11 Query output with the user interface

This web URL output is very similar to the query output with the user interface, plus it allows you to use the output in another script or manipulate it as needed.

### Task

As an alternative, you can paste, `https://<localHost>:8443/remote/core.executeQuery?queryId=34` in a browser address bar to display this URL output.



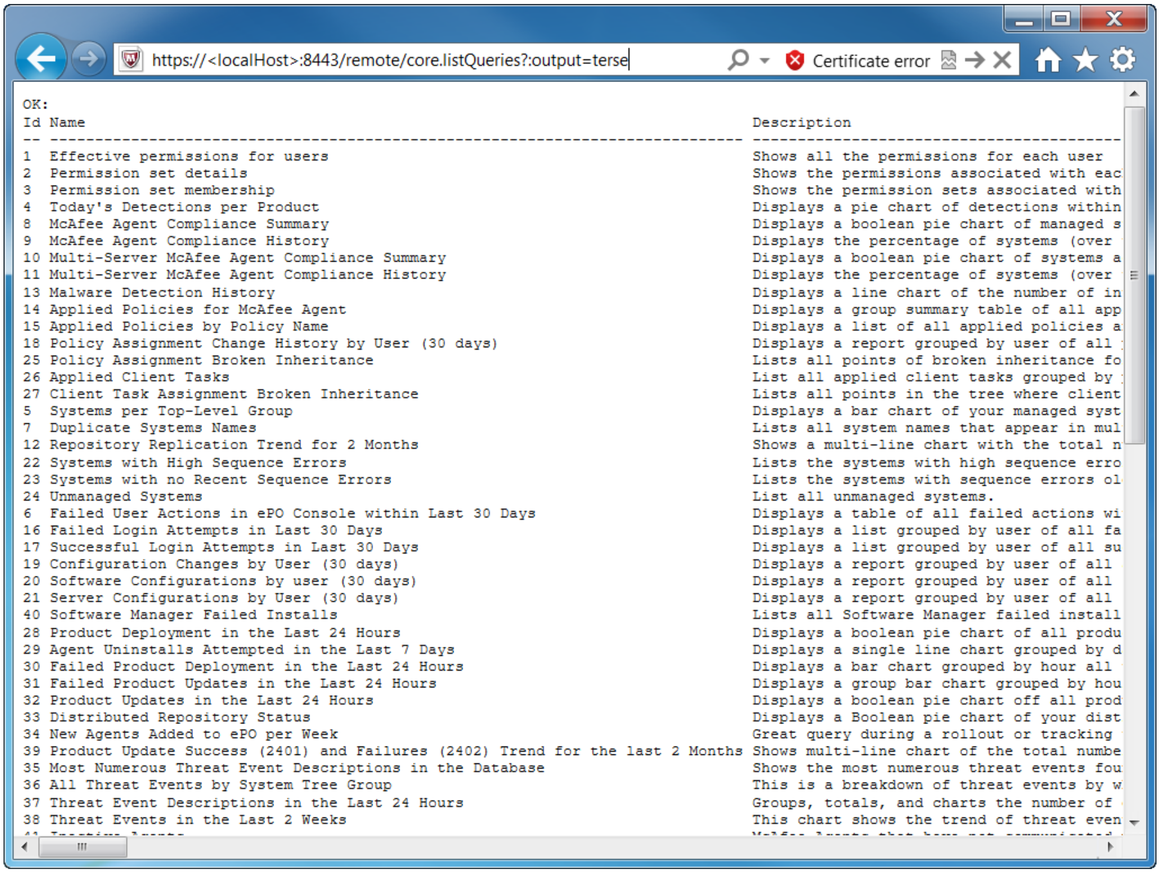
**https://<localHost>:8443/remote/core.executeQuery?queryId=34**

```
OK:
count: 3
Completion Time (Week): 4/27/14 - 5/3/14

count: 2
Completion Time (Week): 5/4/14 - 5/10/14

count: 6
Completion Time (Week): 5/11/14 - 5/17/14

count: 1
Completion Time (Week): 5/18/14 - 5/24/14
```

**Figure 8-12 Web URL output for**

1. Use your browser to log on to your McAfee ePO server.
2. To get a list of the preconfigured queries and their ID numbers, type this URL into the browser address bar, then press **Enter**.

`https://<localHost>:8443/remote/core.listQueries?:output=terse`



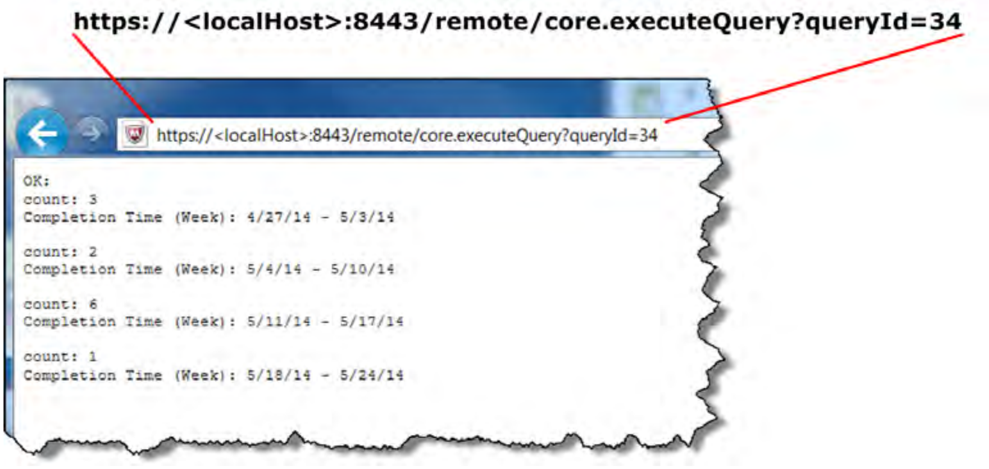
```
OK:
Id Name                                                                          Description
-- ----------------------------------------------------------------------------- -----------------------------------------
1  Effective permissions for users                                               Shows all the permissions for each user
2  Permission set details                                                        Shows the permissions associated with eac
3  Permission set membership                                                     Shows the permission sets associated with
4  Today's Detections per Product                                                Displays a pie chart of detections within
8  McAfee Agent Compliance Summary                                               Displays a boolean pie chart of managed s
9  McAfee Agent Compliance History                                               Displays the percentage of systems (over
10 Multi-Server McAfee Agent Compliance Summary                                  Displays a boolean pie chart of systems a
11 Multi-Server McAfee Agent Compliance History                                  Displays the percentage of systems (over
13 Malware Detection History                                                     Displays a line chart of the number of in
14 Applied Policies for McAfee Agent                                             Displays a group summary table of all app
15 Applied Policies by Policy Name                                               Displays a list of all applied policies a
18 Policy Assignment Change History by User (30 days)                            Displays a report grouped by user of all
25 Policy Assignment Broken Inheritance                                          Lists all points of broken inheritance fo
26 Applied Client Tasks                                                          List all applied client tasks grouped by
27 Client Task Assignment Broken Inheritance                                     Lists all points in the tree where client
5  Systems per Top-Level Group                                                   Displays a bar chart of your managed syst
7  Duplicate Systems Names                                                       Lists all system names that appear in mul
12 Repository Replication Trend for 2 Months                                     Shows a multi-line chart with the total n
22 Systems with High Sequence Errors                                             Lists the systems with high sequence erro
23 Systems with no Recent Sequence Errors                                        Lists the systems with sequence errors ol
24 Unmanaged Systems                                                             List all unmanaged systems.
6  Failed User Actions in ePO Console within Last 30 Days                        Displays a table of all failed actions wi
16 Failed Login Attempts in Last 30 Days                                         Displays a list grouped by user of all fa
17 Successful Login Attempts in Last 30 Days                                     Displays a list grouped by user of all su
19 Configuration Changes by User (30 days)                                       Displays a report grouped by user of all
20 Software Configurations by user (30 days)                                     Displays a report grouped by user of all
21 Server Configurations by User (30 days)                                       Displays a report grouped by user of all
40 Software Manager Failed Installs                                              Lists all Software Manager failed install
28 Product Deployment in the Last 24 Hours                                       Displays a boolean pie chart of all produ
29 Agent Uninstalls Attempted in the Last 7 Days                                 Displays a single line chart grouped by d
30 Failed Product Deployment in the Last 24 Hours                                Displays a bar chart grouped by hour all
31 Failed Product Updates in the Last 24 Hours                                   Displays a group bar chart grouped by hou
32 Product Updates in the Last 24 Hours                                          Displays a boolean pie chart off all prod
33 Distributed Repository Status                                                 Displays a Boolean pie chart of your dist
34 New Agents Added to ePO per Week                                              Great query during a rollout or tracking
39 Product Update Success (2401) and Failures (2402) Trend for the last 2 Months Shows multi-line chart of the total numbe
35 Most Numerous Threat Event Descriptions in the Database                       Shows the most numerous threat events fou
36 All Threat Events by System Tree Group                                        This is a breakdown of threat events by w
37 Threat Event Descriptions in the Last 24 Hours                                Groups, totals, and charts the number of
38 Threat Events in the Last 2 Weeks                                             This chart shows the trend of threat even
```

https://<localHost>:8443/remote/core.listQueries?:output=terse
Certificate error

**Figure 8-13  Web URL listQueries command output**

3 From the `listQueries` command output, find the query to run.

In the following example, the `queryId=34` argument is appended to the web URL `https://<localHost>/remote/core.executeQuery?queryId=<number>` to run the New Agents Added to ePO per Week query.



**https://<localHost>:8443/remote/core.executeQuery?queryId=34**

```
OK:
count: 3
Completion Time (Week): 4/27/14 - 5/3/14

count: 2
Completion Time (Week): 5/4/14 - 5/10/14

count: 6
Completion Time (Week): 5/11/14 - 5/17/14

count: 1
Completion Time (Week): 5/18/14 - 5/24/14
```

**Figure 8-14  Web URL output for queryId=34 query**

## Query with XML data

Exporting existing query XML definitions is a great way to learn how to create web URL queries.

See Parsing query export data to create web URL queries on page 92 for details about how the existing query XML definitions are structured, and how to convert the URL-encoded characters to use in your web URL query.

In this example, export the "VSE: DAT Deployment XML" definition file and use those table objects to create a list of the VirusScan Enterprise DAT file versions for each system in your network.

### Task

1 Export the existing query definition XML file and open it in a text editor. See the McAfee ePolicy Orchestrator Product Guide for details about exporting query definitions.

Your export files should look similar to this VSE: DAT Deployment XML definition file.

```
<list id="1">
  <query id="2">
    <dictionary id="3"/>
    <name>VSE: DAT Deployment</name>
    <description>Displays the three highest DAT versions, and a slice for all the other
versions.</description>
    <target>EPOLeafNode</target>
    <table-uri>query:table?orion.table.columns=EPOComputerProperties.ComputerName
%3AEPOComputerProperties.DomainName%3AEPOLeafNode.os%3AEPOComputerProperties.Description
%3AEPOLeafNode.Tags%3AEPOProdPropsView_VIRUSCAN.productversion
%3AEPOProdPropsView_VIRUSCAN.hotfix%3AEPOProdPropsView_VIRUSCAN.servicepack
%3AEPOProdPropsView_VIRUSCAN.enginever
%3AEPOProdPropsView_VIRUSCAN.enginever64%3AEPOProdPropsView_VIRUSCAN.datver
%3AEPOLeafNode.LastUpdate&amp;orion.table.order.by=EPOComputerProperties.ComputerName
%3AEPOComputerProperties.DomainName%3AEPOLeafNode.os%3AEPOComputerProperties.Description
%3AEPOLeafNode.Tags%3AEPOProdPropsView_VIRUSCAN.productversion
%3AEPOProdPropsView_VIRUSCAN.hotfix%3AEPOProdPropsView_VIRUSCAN.servicepack
%3AEPOProdPropsView_VIRUSCAN.enginever
%3AEPOProdPropsView_VIRUSCAN.enginever64%3AEPOProdPropsView_VIRUSCAN.datver
%3AEPOLeafNode.LastUpdate&amp;orion.table.order=az</table-uri>
    <condition-uri>query:condition?orion.condition.sexp=%28+where+%28+version_ge
+EPOProdPropsView_VIRUSCAN.productversion+%228%22+%29+%29</condition-uri>
    <summary-uri>query:summary?
pie.slice.title=EPOProdPropsView_VIRUSCAN.datver&amp;pie.count.title=EPOLeafNode&amp;orion
.query.type=pie.pie&amp;orion.sum.query=true&amp;orion.sum.group.by=EPOProdPropsView_VIRUS
CAN.datver&amp;orion.sum.order=desc&amp;orion.show.other=true&amp;orion.sum.aggregation=co
unt&amp;orion.sum.aggregation.showTotal=true</summary-uri>
  </query>
</list>
```

2 Open an existing web URL query file to use as a template, then save it with a new name. For example, `URL_template`.

Following is an example of an existing web URL template file.

```
https://<localHost>:8443/remote/core.executeQuery?
target=<tableTarget>&
select=(select <tableObjectNames>)
```

3 From the query definition XML file, find the query target listed between the target tags.

For example, `<target>EPOLeafNode</target>` and paste the target table name in `target=` of your template URL.

This is the template URL with the target table name added.

```
https://<localHost>:8443/remote/core.executeQuery?
target=EPOLeafNode&
select=(select <tableObjectNames>)
```

4. From the query definition XML file, find the S-Expression function, listed between the opening and closing `<condition-uri> ... </condition-uri>` tags, then perform these steps:

   a. In the URL template file, paste the object names in the `select=(select` parameter and the closing parenthesis. This example adds the EPOLeafNode.NodeName (system name) and EPOProdPropsView_VIRUSCAN.datver (VirusScan Enterprise DAT version) from the EPOLeafNode (System Tree) table.

   ```
   https://<localHost>:8443/remote/core.executeQuery?
   target=EPOLeafNode&
   select=(select EPOLeafNode.NodeName EPOProdPropsView_VIRUSCAN.datver)
   ```

   See Parsing query export data to create web URL queries on page 92 for the URL-encoded characters conversion table.

   b. Add the sort order function. For example, to sort the output by system name, add the string "`& order=(order(desc EPOProdPropsView_VIRUSCAN.datver)`" within the existing S-Expression. See Using S-Expressions in web URL queries on page 89 for information about sorting, grouping, and filtering data.

   The following example sorts the output by the VirusScan Enterprise DAT version.

   ```
   https://<localHost>:8443/remote/core.executeQuery?
   target=EPOLeafNode&
   select=(select EPOLeafNode.NodeName EPOProdPropsView_VIRUSCAN.datver&
   order=(order(asc EPOProdPropsView_VIRUSCAN.datver))
   ```

5. Replace the `<localHost>` variable with your McAfee ePO server DNS name, or IP address and paste the URL in your browser address bar. Your output should be similar to this output, but with many entries.

```
OK:
System Name: DP-2K12R2S-SRVR
DAT Version (VirusScan Enterprise):

System Name: DP-EN-W7E1XP-2
DAT Version (VirusScan Enterprise):

System Name: DP-W7PIP-2
DAT Version (VirusScan Enterprise): 7429.0000

System Name: DP-W7PIP-1
DAT Version (VirusScan Enterprise): 7437.0000
.
.
.
```

6 (Optional) To have the information appear in table format, paste the string `:output=terse&` before any ampersand in the URL and rerun the command. This is an example of your template file with `:output=terse&` added.

```
https://<localHost>:8443/remote/core.executeQuery?
target=EPOLeafNode&:output=terse&select=(select EPOLeafNode.NodeName
EPOProdPropsView_VIRUSCAN.datver)&
order=(order(desc EPOLeafNode.NodeName))
```

Confirm that your output is similar to this.

```
OK:
System Name     DAT Version (VirusScan Enterprise)
--------------- ---------------------------------
DP-2K12R2S-SRVR
DP-EN-W7E1XP-2
DP-W7PIP-2      7429.0000
DP-W7PIP-1      7437.0000
DP-2K8AGTHDLR   7437.0000
DP-2K8ER2EPO510 7465.0000
DP-W7PIP-3      7465.0000
.
.
.
```

You have created a web URL query using the information exported from an existing XML query definition.

## Query using table objects, commands, and arguments

You can create web URL queries using a web query template and the web URL Help.

This example describes creating a simple web URL query that displays this information about your managed systems:

- System name
- McAfee Agent version
- When the agent was last updated
- VirusScan Enterprise product family
- VirusScan Enterprise version
- Displays the information as a table

### Task

1 To find the name of the SQL table with most of your information, use this Help command.

`https://<localHost>:8443/remote/core.listTables?:output=terse`

See Using the web URL Help on page 84 for other web URL Help commands.

2 Using your text editor, type this web URL template command.

```
https://<localHost>:8443/remote/core.executeQuery?target=<tableName>&select=(select
<columns>)
```

3 Use the information from this command to find the arguments for the system names, McAfee Agent version, and when it was last updated.

`https://<localHost>:8443/remote/core.listTables?:output=terse&table=EPOLeafNode`

This command displays this information, which you need for your web URL query:

- Query "target" — `EPOLeafNode`
- System name — `EPOLeafNode.NodeName`

- McAfee Agent version — `EPOLeafNode.AgentVersion`
- When the agent was last updated — `EPOLeafNode.LastUpdate`
- Products installed on each system — `EPOProductPropertyProducts`

```
OK:
Name: Managed Systems
Target: EPOLeafNode
Type: target
Database Type:
Description: Retrieves information about systems that have been added to your System Tree.
Columns:
    Name                         Type          Select? Condition? GroupBy? Order? Number?
    ---------------------------- ------------- ------- ---------- -------- ------ -------
    AutoID                       int           False   False      False    True   True
    Tags                         string        True    False      False    True   False
    ExcludedTags                 string        True    False      False    True   False
    AppliedTags                  applied_tags  False   True       False    False  False
    LastUpdate                   timestamp     True    True       True     True   False
    os                           string        True    False      False    False  False
    products                     string        False   False      False    False  False
    NodeName                     string        True    True       True     True   False
    ManagedState                 enum          True    True       False    True   False
    AgentVersion                 string_lookup True    True       True     True   False
    AgentGUID                    string        True    False      False    True   False
    Type                         int           False   False      False    True   False
    ParentID                     int           False   False      False    True   True
    ResortEnabled                boolean       True    True       False    True   False
    ServerKeyHash                string        True    True       False    True   False
    NodePath                     string_lookup False   False      False    True   False
    TransferSiteListsID          isNotNull     True    True       False    True   False
    SequenceErrorCount           int           True    True       False    True   True
    SequenceErrorCountLastUpdate timestamp     True    True       False    True   False
    LastCommSecure               string_enum   True    True       True     True   False
    TenantId                     int           False   False      False    True   True
Related Tables:
    Name
    --------------------------
    EPOProdPropsView_EEFF
    EPOProdPropsView_VIRUSCAN
    EPOProductPropertyProducts
    EPOProdPropsView_PCR
    EPOBranchNode
    EPOProdPropsView_EPOAGENT
    EPOComputerProperties
    EPOComputerLdapProperties
    EPOTagAssignment
    EPOProdPropsView_TELEMETRY
Foreign Keys:
    Source table Source Columns Destination table          Destination columns Allows
inverse? One-to-one? Many-to-one?

 ------------ -------------- -------------------------- ------------------- --------------- --------
    EPOLeafNode  AutoID         EPOComputerProperties      ParentID
False           False       True
    EPOLeafNode  AutoID         EPOTagAssignment           LeafNodeID
False           False       True
    EPOLeafNode  ParentID       EPOBranchNode              AutoID
False           False       True
    EPOLeafNode  AutoID         EPOComputerLdapProperties  LeafNodeId
False           False       True
    EPOLeafNode  AutoID         EPOProductPropertyProducts ParentID
False           False       True
```

4 Add the arguments from step 3 to the web URL template command and test it. Confirm your command looks similar to this example.

```
https://<localHost>:8443/remote/core.executeQuery?target=EPOLeafNode&select=(select
EPOLeafNode.NodeName EPOLeafNode.AgentVersion EPOLeafNode.LastUpdate)
```

Confirm that your output is similar to this example.

```
OK:
System Name: DP-2K8ER2EPO510
Agent Version (deprecated): 4.8.0.887
Last Communication: 6/13/14 9:21:49 AM PDT

System Name: DP-2K12R2S-SRVR
Agent Version (deprecated): 4.8.0.887
Last Communication: 6/13/14 9:55:19 AM PDT

System Name: DP-EN-W7E1XP-2
Agent Version (deprecated): null
Last Communication: null

.
.
.
```

5 Use the `core.listTables` Help command again, but with the `EPOProdPropsView_VIRUSCAN` table, to find the VirusScan Enterprise products installed on each system and product version arguments. Confirm your command looks similar to this example.

```
 https://<localHost>:8443/remote/core.listTables?table=EPOProdPropsView_VIRUSCAN
```

6 Using the output of step 5, add these parameters to your web URL command and test it.

- VirusScan Enterprise product family — `EPOProdPropsView_VIRUSCAN.ProductFamily`
- VirusScan Enterprise version — `EPOProdPropsView_VIRUSCAN.productversion`

Confirm your example looks similar to the following.

```
https://<localHost>:8443/remote/core.executeQuery?target=EPOLeafNode&select=(select
EPOLeafNode.NodeName EPOLeafNode.AgentVersion EPOLeafNode.LastUpdate
EPOProdPropsView_VIRUSCAN.ProductFamily EPOProdPropsView_VIRUSCAN.productversion)
```

Confirm your example output looks similar to the following.

```
OK:
System Name: DP-2K8ER2EPO510
Agent Version (deprecated): 4.8.0.887
Last Communication: 6/13/14 10:21:50 AM PDT
ProdProps.productFamily (VirusScan Enterprise): VIRUSCAN
Product Version (VirusScan Enterprise): 8.8.0.1266

System Name: DP-2K12R2S-SRVR
Agent Version (deprecated): 4.8.0.887
Last Communication: 6/13/14 10:55:19 AM PDT
ProdProps.productFamily (VirusScan Enterprise): VIRUSCAN
Product Version (VirusScan Enterprise):

System Name: DP-EN-W7E1XP-2
Agent Version (deprecated): null
Last Communication: null
ProdProps.productFamily (VirusScan Enterprise): VIRUSCAN
Product Version (VirusScan Enterprise):

.
.
.
```

7 Finally, to show the output as a table, add the command `:output=terse&` after the first ampersand and rerun the command.

Confirm your example example command looks similar to the following.

```
https://<localHost>:8443/remote/core.executeQuery?
target=EPOLeafNode&:output=terse&select=(select EPOLeafNode.NodeName
EPOLeafNode.AgentVersion EPOLeafNode.LastUpdate EPOProdPropsView_VIRUSCAN.ProductFamily
EPOProdPropsView_VIRUSCAN.productversion)
```

Confirm your example output looks similar to the following.

```
OK:
System Name     Agent Version (deprecated) Last Communication
ProdProps.productFamily (VirusScan Enterprise) Product Version (VirusScan Enterprise)
--------------- -------------------------- ----------------------- ---------------------------------
DP-2K8ER2EPO510 4.8.0.887                  6/13/14 10:21:50 AM PDT
VIRUSCAN                                       8.8.0.1266
DP-2K12R2S-SRVR 4.8.0.887                  6/13/14 10:55:19 AM PDT
VIRUSCAN
DP-EN-W7E1XP-2  null                       null
VIRUSCAN
DP-W7PIP-1      4.8.0.887                  6/13/14 10:37:20 AM PDT
VIRUSCAN                                       8.8.0.1266
DP-W7PIP-2      4.8.0.887                  6/13/14 10:36:56 AM PDT
VIRUSCAN                                       8.8.0.1266
DP-W7PIP-3      4.8.0.887                  6/13/14 10:37:00 AM PDT
VIRUSCAN                                       8.8.0.1266
DP-2K8AGTHDLR   4.8.0.887                  6/13/14 10:25:10 AM PDT
VIRUSCAN                                       8.8.0.1266
```

# Scaling your managed network

As your managed network grows, distributed repositories and Agent Handlers can help improve performance and network protection.

9

# Using repositories

Distributed repositories work as file shares that store and distribute security content for your managed client systems.

Repositories play an important role in your McAfee ePO infrastructure. How you configure repositories and deploy them depends on your environment. See Using Agent Handlers on page 4 for details.

**Contents**

## What repositories do

The agents on your managed systems obtain their security content from repositories on the McAfee ePO server. This content keeps your environment up to date.

Repository content can include the following:

- Managed software to deploy to your clients
- Security content such as DATs and signatures
- Patches and any other software needed for client tasks that you create using McAfee ePO

One common misconception is that a repository is created by installing a McAfee ePO server on a system. Unlike your server, repositories *do not* manage policies, collect events, or have code installed on them. A repository is nothing more than a file share located in your environment that your clients can access.

# Repository types

Before you create distributed repositories, it is important to understand which type of repository to use in your managed environment.

The McAfee ePO server always acts as the Master Repository. It keeps the master copy of all the content needed by your agents. The server replicates content to each of the repositories distributed throughout your environment. As a result, your agents can retrieve updated content from an alternate and closer source.

> Your McAfee ePO server does not require configuration to make it the Master Repository. It is the Master Repository by default.

Repository types include:

- FTP repositories
- HTTP repositories
- UNC share repositories
- SuperAgents

Consider the following when planning your distributed repositories:

- The McAfee ePO server requires that you use certain protocols for the repositories, but any server vendor can provide those protocols. For example, if you use an HTTP repository, you can use either Microsoft Internet Information Services (IIS) or Apache server (Apache is the faster option).
- There is no operating system requirement for the systems that host your repository. As long as your McAfee ePO server can access the folders you specify to copy its content to, and as long as the agents can connect to the folder to download their updates, everything works as expected.
- Your agent updates and McAfee ePO replication tasks are only as good as your repositories. If you are already using one of these repositories and your environment works well, then do not change the configuration.

  > If you are starting with a new installation with no repositories, use a SuperAgent because they are easy to configure and are reliable.

**See also**
*SuperAgent repositories* on page 110

## FTP repositories

FTP servers can host a distributed McAfee ePO server repository. You might already have FTP servers in your environment, and you can store McAfee content there as well.

FTP repositories are:

- Fast
- Able to manage extensive loads from the clients pulling data
- Helpful in a DMZ where HTTP might not be optimal and UNC shares can't be used

Using FTP servers, your clients do not need authentication and can use an anonymous logon to pull their content. No authentication reduces the chance that a client fails to pull its content.

## HTTP repositories

HTTP servers can host a distributed McAfee ePO server repository. You might already have HTTP servers in your environment.

HTTP servers can be fast serving out files to large environments. Your HTTP servers allow clients to pull their content without authentication, which reduces the chance that a client might fail to pull its content.

## UNC share repositories

Universal Naming Convention (UNC) shares can host your McAfee ePO server repository.

Because most administrators are familiar with the concept of UNC shares, UNC shares might seem like the easiest method to choose, but that's not always the case.

If you choose to use UNC shares, you must:

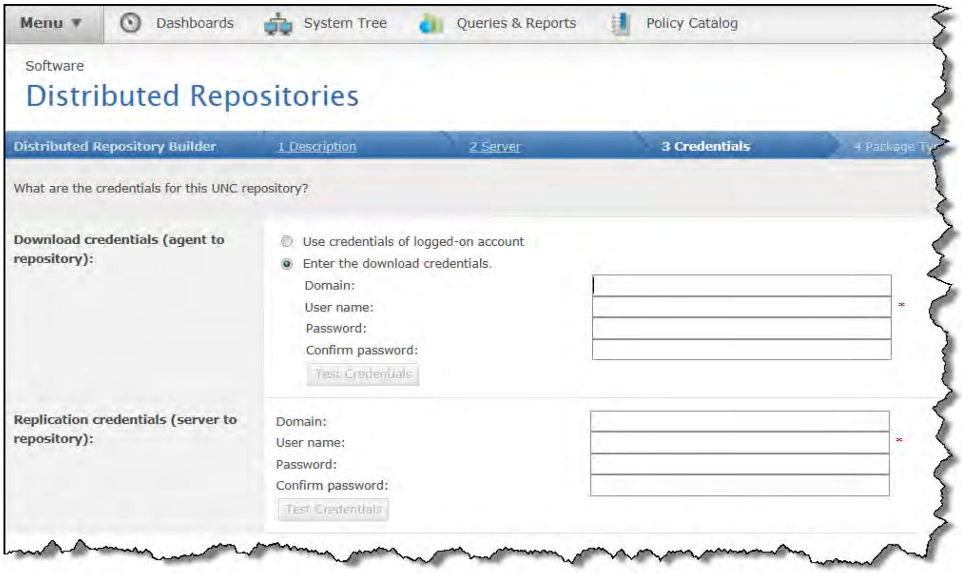
1 Create the folder.

2 Adjust share permissions.

3 Change the NTFS permissions.

4 Create two accounts, one with read access and another with write access.

> If your IT group has password rules, such as changing a password every 30 days even for service accounts, changing those passwords in McAfee ePO can be cumbersome. You would need to change the password for access to each of the distributed repository shares in the Windows OS and within the configuration settings for each of the UNC Distributed Repositories within McAfee ePO. Access the McAfee ePO UNC Distributed Repositories settings using, **Menu | Software | Distributed Repositories**.



What are the credentials for this UNC repository?

**Download credentials (agent to repository):**

○ Use credentials of logged-on account

● Enter the download credentials.

Domain:

User name: *

Password:

Confirm password:

**Replication credentials (server to repository):**

Domain:

User name: *

Password:

Confirm password:

**Figure 9-1 UNC repository credentials page**

All these tasks increase the chance of failure because these processes must be completed manually. Your agents might not properly update if your agents cannot authenticate to your UNC share because they are not part of the domain or the credentials are incorrect.

## SuperAgent repositories

You can create a SuperAgent repository to act as an intermediary between the McAfee ePO server and other agents.

The SuperAgent caches information received from a McAfee ePO server, the Master Repository, or a mirrored Distributed Repository, and distributes it to the nearest agents. The Lazy Caching feature allows **SuperAgents** to retrieve data from McAfee ePO servers only when requested by a local agent node. Creating a hierarchy of SuperAgents along with lazy caching further saves bandwidth and minimizes the wide-area network traffic.

A SuperAgent also broadcasts wake-up calls to other agents using that SuperAgent repository. When the SuperAgent receives a wake-up call from the McAfee ePO server, it wakes up the agents using its repository connection.

> This is an alternative to sending ordinary wake-up calls to each agent in the network or sending an agent wake-up task to each computer.

For detailed information about SuperAgents and how to configure them, see McAfee ePolicy Orchestrator Product Guide and McAfee Agent Product Guide.

### SuperAgent considerations

When you configure systems as SuperAgents, , follow these guidelines.

- Use existing file repositories in your environment, for example Microsoft System Center Configuration Manager (SCCM).
- You don't need a SuperAgent on every subnet.
- Turn off Global Updating to prevent unwanted updates of new engines or patches from the Master Repository. See Global Updating restrictions on page 116.

### SuperAgent and its hierarchy

A hierarchy of SuperAgents can serve agents in the same network with minimum network traffic utilization. A SuperAgent caches the content updates for the McAfee ePO server or distributed repository and distributes content updates to the agents in the network, reducing the wide area network traffic. It is always ideal to have more than one SuperAgent to balance the network load.

You use the Repository policy to create the SuperAgent hierarchy. McAfee recommends that you have a three-level hierarchy of SuperAgents in your network. Refer to the McAfee ePolicy Orchestrator Product Guide for details about creating a hierarchy of SuperAgents.

See McAfee Agent Product Guide for details about SuperAgent caching (lazy caching) and communication interruptions.

### Create a SuperAgent

Creating a SuperAgent requires these tasks.

1. Create a new SuperAgents policy.
2. Create a new group in the System Tree, for example named SuperAgents
3. Assign the new SuperAgent policy to the new SuperAgents group.
4. Drag a system into the new **SuperAgents** group.

Once you have created the new SuperAgents group, you can drag any system into that group and it becomes a SuperAgent the next time it communicates with the McAfee ePO server.

## Create new SuperAgent policy

To convert client systems to SuperAgents, you must assign a SuperAgent policy to those systems.

### Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Policy** | **Policy Catalog** to open the Policy Catalog page.

2 To duplicate the **My Default** policy from the **Product** drop-down menu, select **McAfee Agent**, and from the **Category** drop-down menu, select **General**.

3 In the **My Default** policy row, in the **Actions** column, click **Duplicate**.

> The **McAfee Default** policy cannot be modified.

4 In the **Duplicate Existing Policy** dialog box, modify the policy name, add any notes for reference, and click **OK**.

5 From the Policy Catalog page, click **SuperAgents** tab, select **Convert agents to SuperAgents** to convert the agent to a SuperAgent and update its repository with the latest content.

6 Select **Use systems running SuperAgents as distributed repositories** to use the systems that host SuperAgents as update repositories for the systems in its broadcast segment, then provide the **Repository path**.

7 Select **Enable Lazy caching** to allow the SuperAgents to cache content when it is received from the McAfee ePO server.

8 Click **Save**.

## Create a new group in the System Tree

Adding a SuperAgent group to your System Tree allows you to assign a SuperAgent policy to the group.

### Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Systems Section** | **System Tree**, click **System Tree Actions** | **New Subgroups**, and give it a distinctive name, for example *SuperAgents*.

2 Click **OK**. The new group appears in the System Tree list.

## Assign the new SuperAgents policy to the new SuperAgent group

Assigning the SuperAgent policy to the new group completes the configuration of the SuperAgent group.

### Task

For option definitions, click **?** in the interface.

1 In the **System Tree**, select the SuperAgent group that you created, select the **Assigned Policies** tab, then select **McAfee Agent** from the Product list.

2 From the **Actions** column for the **General** category, click **Edit Assignment**.

3 From the **McAfee Agent : General** page, click **Break inheritance and assign the policy and settings below**. Select the SuperAgent policy that you created from the **Assigned Policy** list, then click **Save**.

## Assign a system to the new SuperAgent group

After the SuperAgent group is configured, you can assign the SuperAgent policies to individual client systems by dragging them into that group. These policies convert the client systems into SuperAgents.

### Task

For option definitions, click **?** in the interface.

1. In the **System Tree**, click the **Systems** tab and find the system that you want to change to a SuperAgent repository.
2. Drag that row with the system name and drop it into the new SuperAgent group you created in the System Tree.

   Once the system communicates with the McAfee ePO server, it changes to a SuperAgent repository.
3. To confirm that the system is now a SuperAgent repository, click **Menu** | **Software** | **Distributed Repositories** and select **SuperAgent** from the **Filter** list. The new SuperAgent repository appears in the list.

   > Before the system appears as a SuperAgent in the group, two agent-server communications must occur. First, the system must receive the policy change and second, the agent must respond back to the McAfee ePO server that is now a SuperAgent. This conversion might take some time depending on your ASCI settings.

# Where to place repositories

You must determine how many repositories are needed in your environment and where they should be located.

To answer these questions, you must look at your McAfee ePO server managed systems and your network geography.

Consider the following factors:

- How many nodes do you manage with the McAfee ePO server?
- Are these nodes located in different geographic locations?
- What connectivity do you have to your repositories?

Remember, the purpose of a repository is to allow clients to download the large amount of data in software updates locally instead of connecting to the McAfee ePO server and downloading the updates across the slower WAN links. At a minimum, your repository is used to update your signature, or DAT files for VirusScan Enterprise on a daily basis. In addition, your repository is used by your agents to download new software, product patches, and other content, for example Host Intrusion Prevention content.

Typically you can create a repository for each large geographic location, but there are several caveats. Plus, you must avoid the most common mistakes of having too many or too few repositories and overloading your network bandwidth. See Calculating bandwidth for repository replication and product updates on page 166, to calculate the bandwidth to update your repositories.

# How many repositories do you need?

How many repositories you need depends on the server hardware, node count, network topology, and where the repositories are installed.

Repositories have no hard technical limit to how many nodes they can handle. With a properly crafted update task for your clients, repositories can update a significant number of nodes. Bandwidth recommendations for repository distribution on page 164 list the suggested number of repositories needed depending on the systems in the LAN, network bandwidth, and randomization interval setting.

The following table is an estimate of the updates a repository can handle and the hardware needed. Many factors can influence these specifications, for example how you update content, products, and patches.

| Server hardware | Nodes updated | Dedicated or shared client hardware |
|---|---|---|
| Single 3-GHz processor with 4 GB of memory | 3,000 | Shared with other applications |
| Single 3-GHz processor with 4 GB of memory | 3,000–7,000 | Dedicated |
| Server class hardware, dual-quad processor, and 8 GB of memory | 5,000–7,000 | Dedicated |

Disk space needed for a repository is rarely a concern with today's storage standards. Even if you checked in several McAfee endpoint products, for example McAfee Endpoint Encryption, SiteAdvisor Enterprise, and Policy Auditor, your repository disk space is in the 1-GB range.

To find the exact size of the product installation files in Windows Explorer, right-click the Install folder and click Properties. The product files are at this default path:

```
C:\Program Files(X86)\McAfee\ePolicy Orchestrator\DB\Software\Current\<ProductName>
\Install\
```

These examples provide three common organization sizes and their repository size.

## Example 1–3,000 node organization with one office

This example describes the repository specifics for an organization with 3,000 nodes in one office. The organization has these characteristics:

- Approximately 3,000 nodes of workstations and servers.
- Uses VirusScan Enterprise, Host Intrusion Prevention, McAfee Endpoint Encryption, and Host Data Loss Prevention.
- Has a small data center in the same building where the devices reside, so there are no WAN links and all clients are on a 100 MB LAN.

In this example, you can use the primary McAfee ePO server to act as the only repository. The McAfee ePO server is always the Master Repository by default. For 3,000 clients, the McAfee ePO server can handle:

- Policy deployment
- Event collection
- Distributing all updates and software

## Example 2–15,000–20,000 node organization with four offices

This example describes the repository specifics for an organization with 15,000–20,000 nodes and four offices. The organization has these characteristics:

- Approximately 15,000–20,000 nodes of workstations and servers.
- Has one data center in New York where all traffic destined for the Internet is routed.
- Four offices in the U.S. located in New York, San Francisco, Dallas, and Orlando.
- Each office has approximately 3,000–4,000 nodes and a T1 connection (1.544 Mb/s) back to the New York office.

The McAfee ePO server, located in New York, manages all 20,000 nodes for policies and events for McAfee Endpoint Encryption, VirusScan Enterprise, Host Intrusion Prevention, and Application Control.

A dedicated SuperAgent repository is placed in each of the three major offices that connect to the data center. These repositories are dedicated SuperAgent repositories that connect to the New York data center with medium hardware class servers, for example a single processor 3 GHz CPU and 4 GB of RAM. The SuperAgents only job is to serve out files to the McAfee Agent at each office. When you have multiple repositories, you can specify the order in which agents access repositories. In this example, you would order the repositories so that the dedicated SuperAgent repositories that connect to the New York data center are accessed first. You can even disable access to other repositories you don't want the agents to use.

## Example 3 – 40,000–60,000 node organization with multiple global offices

This example describes the repository specifics for an organization with 40,000–60,000 node organization with multiple global offices. The organization has these characteristics:

- Approximately 40,000–60,000 nodes of workstations and servers.
- Three major regions of the U.S. offices, with one data center in New York and three additional offices across the country.
- Each office has approximately 5,000–7,000 nodes.
- The one McAfee ePO server in the New York data center runs VirusScan Enterprise, Host Intrusion Prevention, and SiteAdvisor Enterprise.
- The largest office in the U.S., other than the New York Data Center, has an Agent Handler installed. See Introducing Agent Handlers on page 119 for details.

The Europe, Middle East, and Africa (EMEA) offices have another data center in the UK with several other offices across EMEA. These other offices range from 200 nodes 3,000 nodes.

The Asia-Pacific (APAC) offices include two smaller offices.

| Region | Office | Number of nodes | Servers |
|---|---|---|---|
| U.S. | New York, Data Center | 7,000 | McAfee ePO server |
| U.S. | Office 1 | 5,000 | Repository |
| U.S. | Office 2 | 6,000 | Repository and Agent Handler |
| U.S. | Office 3 | 5,000 | Repository |
| EMEA | U.K., Data Center | 3,000 | Repository |
| EMEA | Office 1 | 200 | |
| EMEA | Office 2 | 1,000 | Repository |
| EMEA | Office 3 | 3,000 | Repository |
| APAC | Office 1 | 500 | |
| APAC | Office 2 | 300 | |

### U.S. region servers

Put one server class client, for example dual processor 3 GHz and 8 GB of RAM, at each site in the U.S.

**EMEA region servers**

Use the Systems Management Server (SMS) and install the SuperAgents at each office in the EMEA because they are smaller sites. Your repository does not have to be dedicated to McAfee as long as it's not serving files to several thousand agents.

**APAC region servers**

The small offices in the APAC region use slow WAN links back to the McAfee ePO server in the New York. Plus these WAN links are already saturated with traffic. These links mean replication from the McAfee ePO server to an APAC repository is not feasible unless it is done during off hours. This option is reasonable if you want to put SuperAgents in APAC.

Fortunately, the APAC offices each have their own fast dedicated connections out to the Internet and do not have to route Internet traffic back to the data center in New York. That provides two potential solutions:

- You can adjust the client tasks in APAC to have them go to the next nearest repository, which might be in California.

  > You must completely randomize the agents updating schedule so you spread their updates throughout the day.

- You can put a SuperAgent in the DMZ (publicly accessible on the Internet) at one of the data centers. Then adjust the APAC client tasks forcing them to only update from this SuperAgent in the DMZ. Because the SuperAgent is local to the data center, replication from McAfee ePO is fast. Because the agents don’t have to use a WAN link and can go straight to the Internet and your slow WAN bandwidth concerns are solved.

## Disable server Master Repository

In large environments, you can improve performance of your McAfee ePO server by excluding the Master Repository from providing agent updates.

> **Before you begin**
>
> You must have another repository configured before you can disable the Master Repository on the McAfee ePO server.

In large environments, the McAfee ePO server is already busy distributing policies and collecting events. You can improve performance by changing the agent policy so agents don't pull content from the McAfee ePO server itself, the default Master Repository. Instead, agents access dedicated repositories that are created for local access. This change forces the agents to use only the repositories you created manually. You can specify which repositories agents access when selecting a repository within a policy.

> In smaller environments, where fewer nodes are managed, there is no need for this change. The server can handle all these tasks without impacting performance.

### Task

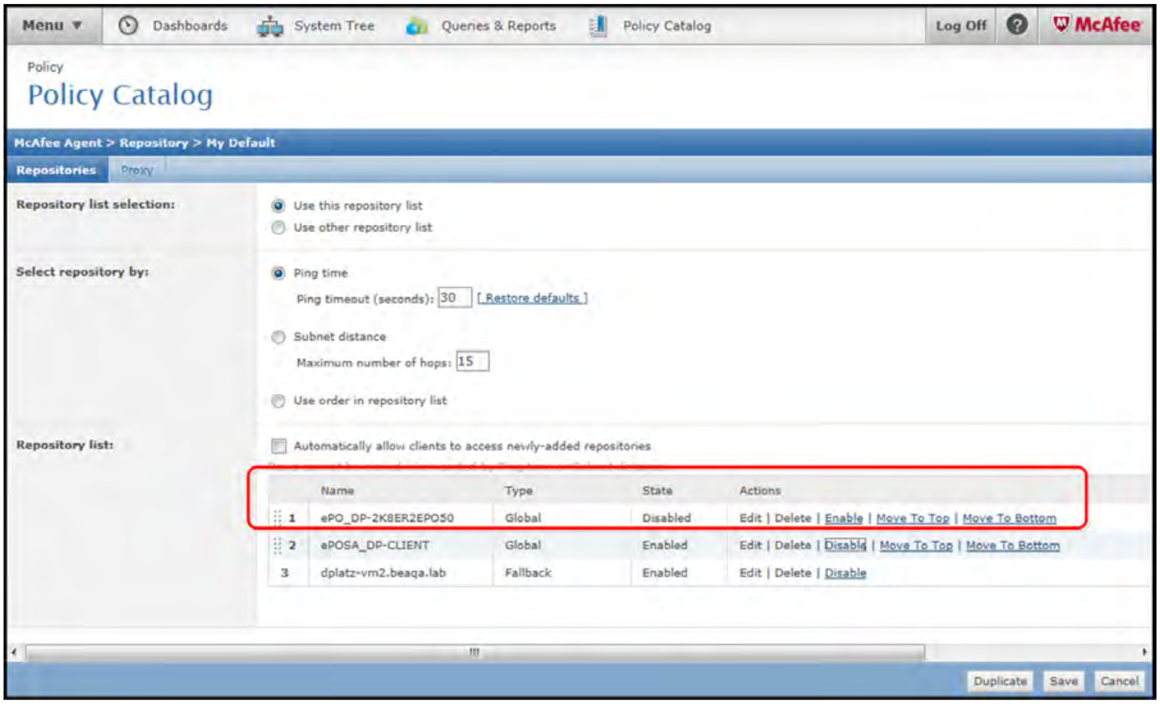
For option definitions, click **?** in the interface.

1 To open the Policy Catalog, click **Menu** | **Policy** | **Policy Catalog**.

2 From the Product list, select **McAfee Agent**, then from the Category list, select **Repository**, and click the policy name to modify.

3. Click the **Repositories** tab.
4. In the Repository list, click **Disable** in the Actions column for the McAfee ePO server.

   This figure shows the McAfee ePO server disabled.



Policy

Policy Catalog

McAfee Agent > Repository > My Default

Repositories | Proxy

Repository list selection:
● Use this repository list
○ Use other repository list

Select repository by:
● Ping time
Ping timeout (seconds): 30 [ Restore defaults ]
○ Subnet distance
Maximum number of hops: 15
○ Use order in repository list

Repository list:
□ Automatically allow clients to access newly-added repositories

| | Name | Type | State | Actions |
|---|---|---|---|---|
| 1 | ePO_DP-2K8ER2EPO50 | Global | Disabled | Edit \| Delete \| Enable \| Move To Top \| Move To Bottom |
| 2 | ePOSA_DP-CLIENT | Global | Enabled | Edit \| Delete \| Disable \| Move To Top \| Move To Bottom |
| 3 | dplatz-vm2.beaqa.lab | Fallback | Enabled | Edit \| Delete \| Disable |

**Figure 9-2 Repositories with McAfee ePO server disabled**

5. Click **Save**.

Now you have improved the McAfee ePO server performance because the agents are no longer accessing it for updates.

## Global Updating restrictions

Global Updating is a powerful feature, but if used incorrectly it can have a negative impact in your environment.

Global Updating is used to update your repositories as quickly as possible whenever the Master Repository changes. Global Updating is great if you have a smaller environment (fewer than 1,000 nodes) with no WAN links. Global Updating generates a huge amount of traffic that could impact your network bandwidth. If your environment is on a LAN, and bandwidth is not a concern, then use Global Updating. If you are managing a larger environment and bandwidth is critical, disable Global Updating. See Bandwidth usage on page 5 for considerations when using Global Updating in an enterprise environment.

> Global Updating is disabled by default when you install McAfee ePO software.
>
> To confirm the Global Updating setting, click **Menu** | **Configuration** | **Server Settings** and select **Global Updating** from the Setting Categories list. Confirm that the status is disabled. If not, click **Edit** and change the status.

If you are a user with a large environment and where bandwidth is critical, you can saturate your WAN links if you have Global Updating enabled. You might think having Global Updating enabled makes you receive their DATs quickly. But eventually, McAfee, for example releases an update to its VirusScan Enterprise engine that can be several megabytes, compared to the 400-KB DAT files. This engine update typically occurs twice a year. When that release occurs the McAfee ePO server pulls the engine from McAfee, starts replicating it to the distributed repositories, and starts waking up agents to receive the new engine immediately. This engine update can saturate your WAN links and roll out an engine that you might prefer to upgrade in a staged release.

> ℹ If you have a large environment, you can still use Global Updating, but you must disable it when a new engine or product patch is released or the updates could saturate your WAN links.

For additional information see these KnowledgeBase articles:

- How to prevent McAfee ePO 5.0 from automatically updating to the latest posted Engine, KB77901
- ePolicy Orchestrator prematurely deploys McAfee product software patch, KB77063

## How Global Updating works

If your McAfee ePO server is scheduled to pull the latest DATs from the McAfee website at 2 p.m. Eastern time (and the scheduled pull changes the contents of your **Master Repository**), your server automatically initiates the Global Update process to replicate the new content to all your distributed repositories.

The Global Updating process follows this sequence of events:

1. Content or packages are checked in to the Master Repository.
2. The McAfee ePO server performs an incremental replication to all distributed repositories.
3. The McAfee ePO server issues a SuperAgent wake-up call to all SuperAgents in the environment.
4. The SuperAgent broadcasts a global update message to all agents within the SuperAgent subnet.
5. Upon receipt of the broadcast, the agent is supplied with a minimum catalog version needed.
6. The agent searches the distributed repositories for a site that has this minimum catalog version.
7. Once a suitable repository is found, the agent runs the update task.

10

# Using Agent Handlers

Agent Handlers distribute agent-server communications by directing managed systems to report to a specific Agent Handler instead of connecting to the McAfee ePO server.

**Contents**

## Introducing Agent Handlers

Agent Handlers allow you to move McAfee Agent requests and added management logic closer to the systems making these requests.

Agent Handlers also allow you to scale your network infrastructure horizontally, reduce the load on your McAfee ePO server, and save bandwidth.

This figure shows some of the typical connections between Agent Handlers, the McAfee ePO server, and the McAfee ePO SQL Server database server.

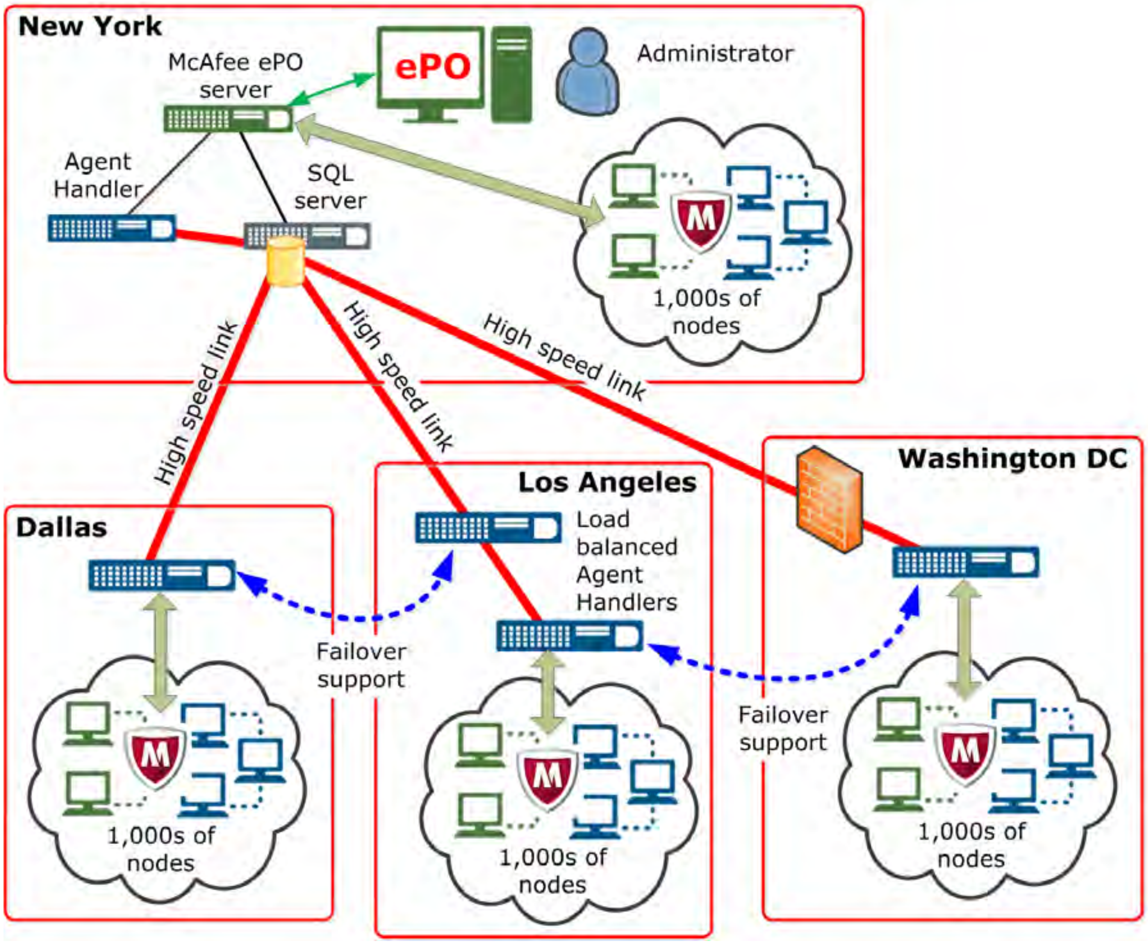


**Figure 10-1 Agent Handlers in an enterprise network**

In this figure, all Agent Handlers:

- Are connected to the McAfee ePO SQL database using low-latency high-speed links
- Are located close to the clients they support
- Have failover configured between Agent Handlers in other cities
- Are managed from the McAfee ePO server

The Agent Handlers in these cities have specific configurations.

- **Dallas** — The Agent Handler is configured with failover support to the Agent Handler in Los Angeles.
- **Los Angeles** — The two Agent Handlers have load balancing configured.
- **Washington DC** — The Agent Handler uses specific ports to connect to the McAfee ePO server from behind a firewall.

# Agent Handler basics

Agent Handlers provide specific features that can help grow your network to include many more managed systems.

## When to use Agent Handlers

There are many reasons to use Agent Handlers in your network.

- **Hardware is cheaper** — The mid-range server hardware used for Agent Handlers is less expensive than the high-end servers used for McAfee ePO servers.
- **Scalability** — As your network grows, Agent Handlers can be added to reduce the load on your McAfee ePO server.

  > We recommend connecting no more than five Agent Handlers to a single McAfee ePO server with a maximum of 50,000 nodes connected to each Agent Handler.

- **Network topology** — Agent Handlers can manage your agent requests behind a firewall or in an external network.
- **Failover** — Agents can failover between Agent Handlers using a configured fallback priority list.
- **Load Balancing** — Multiple Agent Handlers can load balance the McAfee Agent requests in a large remote network.

## When *not* to use Agent Handlers

There are some instances not to use Agent Handlers.

- **As distributed repositories** — Repositories, for example **SuperAgents**, distribute large files throughout an organization. Repositories do not contain any logic. Agent Handlers use logic to communicate events back to the database. These events tell the McAfee Agent when to download new products from the distributed repositories. Agent Handlers can cache files from the distributed repositories, but should not be used to replace distributed repositories. Agent Handlers are used to reduce the event management load on the McAfee ePO server.
- **Through a slow or irregular connection** — Agent Handlers require a relatively high speed, low latency connection to the database to deliver events sent by the agents.

## How Agent Handlers work

Agent Handlers use a work queue in the McAfee ePO database as their primary communication mechanism.

Agent Handlers check the server work queue every10 seconds and perform the requested action. Typical actions include agent wake-up calls, requests for product deployment, and data channel messages. These frequent communications to the database require relatively high speed, low latency connection between the Agent Handler and the McAfee ePO database.

Agent Handlers also communicate with each other and are used for load balancing and failover.

Three services run in any McAfee ePO installation. You can access these services from the Windows software at **Start** | **Run** | **Services.msc**:

- **McAfee ePolicy Orchestrator 5.1.0 Application Server (MCAFEETOMCATSRV510)** — The Application Server (Tomcat) hosts the McAfee ePO user interface and server task scheduler.
- **McAfee ePolicy Orchestrator 5.1.0 Event Parser (MCAFEEEVENTPARSERSRV)** — Event Parser service
- **McAfee ePolicy Orchestrator 5.1.0 Server (MCAFEEAPACHESRV)** — Apache/2.2.22 (Win32) mod_ssl/2.2.22 OpenSSL/1.0.1

> The Apache Server and Event Parser communicate with the McAfee Agent. These two services work together to receive updated events and properties from the agents. Then they send updated policies and tasks as assigned by administrators in the McAfee ePO console.

An Agent Handler installation includes only the Apache Server and Event Parser services. You can deploy Agent Handlers on separate hardware, or virtual machines, that coexist within a single logical McAfee ePO infrastructure.

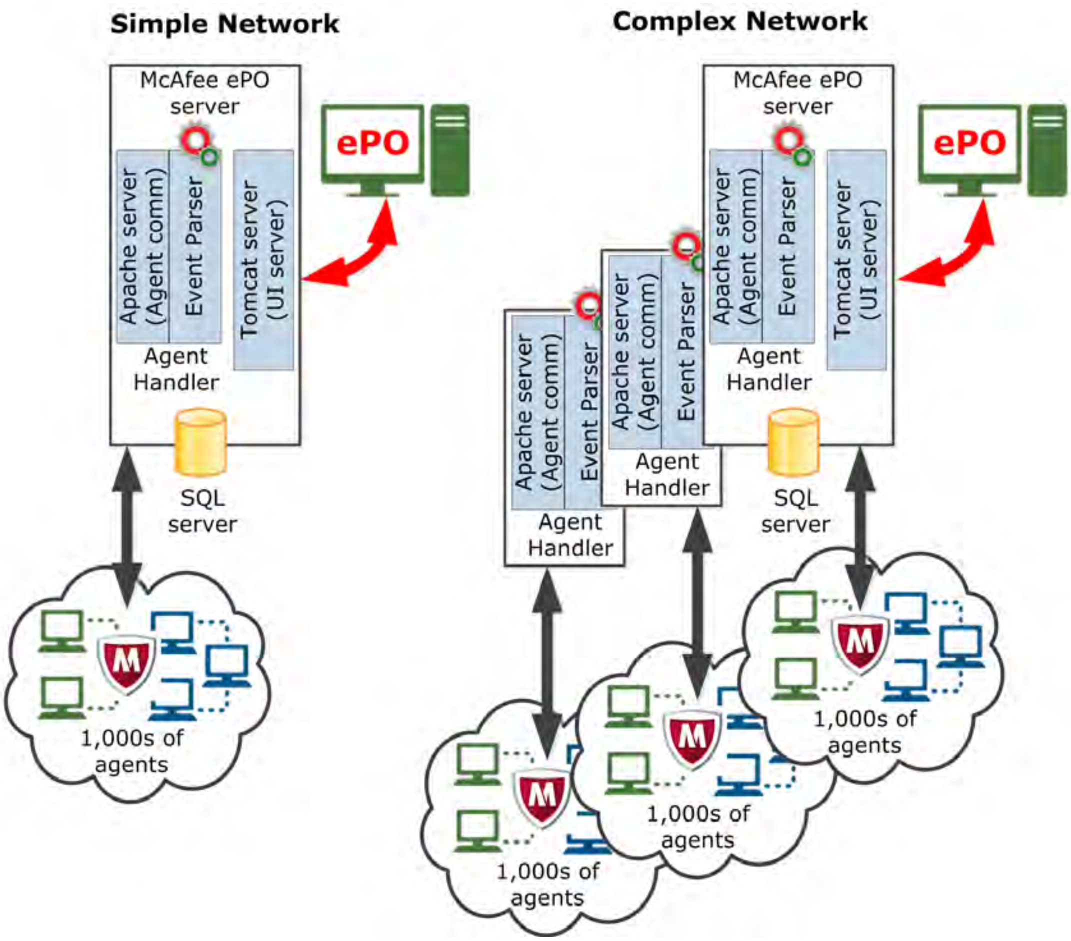


**Figure 10-2 Agent Handler functional diagram**

This figure shows two different network configurations and their Agent Handlers.

- **Simple network** — The primary Agent Handler is installed as a part of the McAfee ePO server. This is sufficient for many small McAfee ePO installations; typically additional Agent Handlers are not required.
- **Complex network** — Multiple remote Agent Handlers are installed on separate servers connected to the McAfee ePO server. Once installed, the additional Agent Handlers are automatically configured to work with the McAfee ePO server to distribute the incoming agent requests. The McAfee ePO console is also used to configure Agent Handler Assignment rules to support more complex scenarios. For example, an Agent Handler behind the DMZ, firewall, or using network address translation (NAT).

Administrators can override the Agent Handler default behavior by creating rules specific to their environment. See Agent Handler configuration overview on page 129.

## Agent Handlers eliminate multiple McAfee ePO servers

Use Agent Handlers in different geographic regions instead of multiple McAfee ePO servers.

> Multiple McAfee ePO servers cause management, database duplication, and maintenance problems.

Use Agent Handlers to:

- Expand the existing McAfee ePO infrastructure to handle more agents, more products, or a higher load due to more frequent agent-server communication.
- Ensure that agents continue to connect and receive policy, task, and product updates even if the McAfee ePO server is unavailable.
- Expand McAfee ePO management into disconnected network segments with high-bandwidth links to the McAfee ePO database.

In most cases, it is more efficient and less expensive to add an Agent Handler rather than a McAfee ePO server.

> Use a separate McAfee ePO server for *separate* IT infrastructures, *separate* administrative groups, or *test* environments.

# Agent Handler functionality

Agent Handlers provide horizontal network scalability, failover protection, load balancing, and allow you to manage clients behind a DMZ, firewall, or using network address translation (NAT).

## Providing scalability

Agent Handlers can provide scalability for McAfee ePO managed networks as the number of clients and managed products grow.

A single McAfee ePO server can easily manage up to 200,000 systems with only the VirusScan Enterprise product installed. But, as the systems managed and the number of products integrated with your McAfee ePO server increase the attempts to receive policies or send events to your server increase. This load increase also decreases the maximum number of systems manageable with the same McAfee ePO server hardware. The McAfee Security Innovation Alliance (SIA) program and the integration of SDKs to third-party partners also increases the number of products your McAfee ePO server can manage.

Agent Handlers allow you to scale your McAfee ePO infrastructure to manage more clients and products. You do this by adding Agent Handlers to manage an equivalent or larger number of agents with a single logical McAfee ePO deployment. By default, when you install the Agent Handlers software on a server, all Agent Handlers are used at the same order level unless custom assignment rules are created.

## Failover protection with Agent Handlers

Agent Handlers allow any McAfee Agent to receive policy and task updates and report events and property changes if the McAfee ePO server is unavailable. For example, an upgrade or network problem.

Once multiple Agent Handler are deployed, they are available to agents as failover candidates. As long as the Agent Handler is connected to the database, it can continue serving agents. This includes any policy or task modifications resulting from agent properties or from administrator modifications before the McAfee ePO server goes offline.

The configuration file shared with the McAfee Agent contains a configurable fallback list of Agent Handlers. If needed, the McAfee Agent tries to connect through the list of Agent Handlers until the list ends or it is able to contact a valid, enabled Agent Handler.

Failover between Agent Handlers is configured in one of two ways.

## Simple deployment failover

In the simple deployment failover, two Agent Handlers can be deployed as primary and secondary. All agents initiate communications with the primary Agent Handler, and only use the secondaryAgent Handler if the primary is unavailable. This deployment makes sense if the primary Agent Handler has better hardware, and is capable of handling the entire load of the infrastructure.

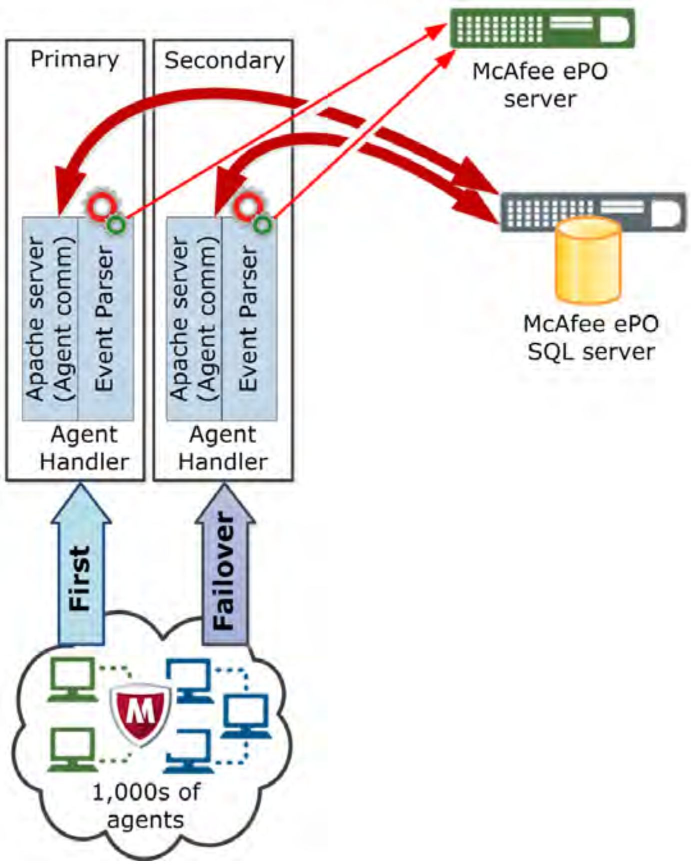


Figure 10-3 Simple Agent Handler failover

### Failover with load balancing

The second deployment combines failover with load balancing. Multiple Agent Handlers are configured into the same Agent Handler group. The McAfee ePO server inserts each Agent Handler in the group into the list of Agent Handlers at the same order level. The McAfee Agent randomizes Agent Handlers at the same order level, which results in an equal load across all Agent Handlers in a particular group.

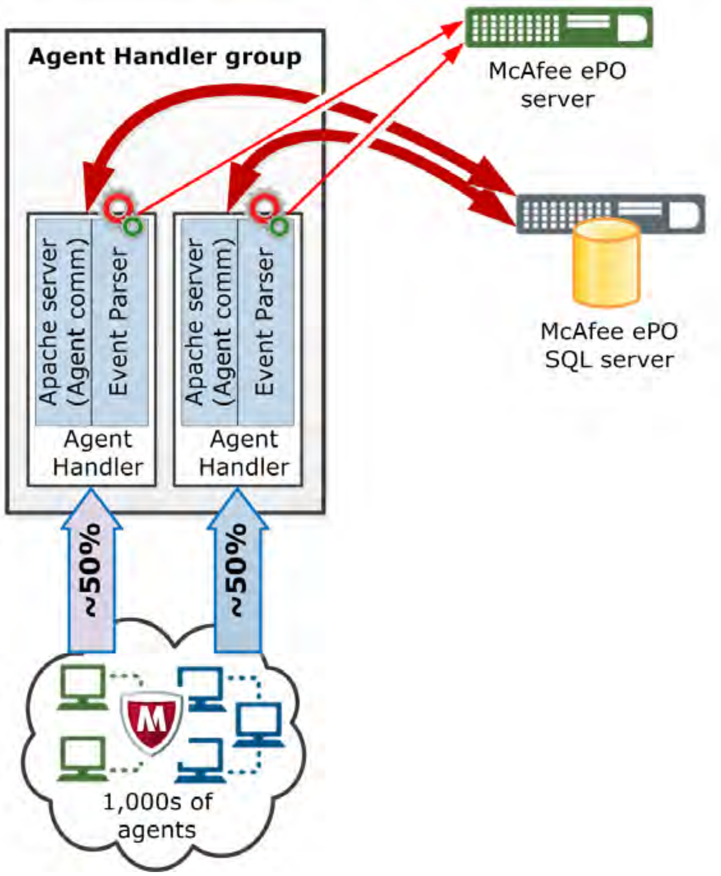


Figure 10-4  Failover with Agent Handler load balancing

Agents fail over between all Agent Handlers in a group before failing through to the next Agent Handler in the assignment list. Using Agent Handler groups results in both load balancing and failover benefits.

## Network topology and deployment considerations

Agent Handlers allow flexibility in your network configuration, but additional planning can improve your network performance.

### Using Agent Handlers behind a DMZ, firewall, or in NAT networks

Without Agent Handlers, any McAfee Agent behind a DMZ, firewall, or in a NAT network can be viewed with the McAfee ePO server. But you can't manage or directly manipulate those systems in the NAT network.

With an Agent Handler behind the DMZ, you can address systems within the NAT region for wake-up calls, data channel access, and more.

This Agent Handler connection requires access to both the SQL database and the McAfee ePO server. Some firewall rules are necessary for this configuration.

This figure shows an Agent Handler with managed systems behind the DMZ and these connections:

- Data Channel connection to the McAfee ePO server
- Low-latency high-speed connection to the SQL database
- Failover connection between the Agent Handlers

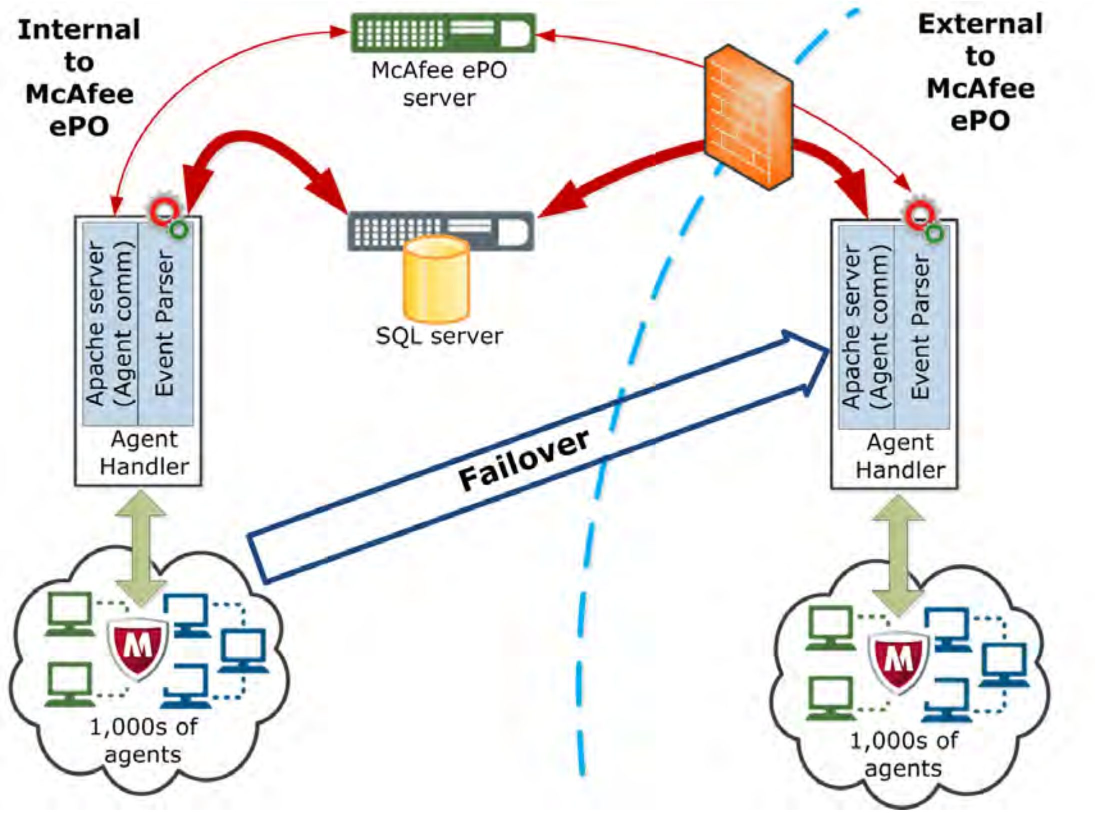


**Figure 10-5 Agent Handler behind the DMZ**

This table lists all ports used by the McAfee ePO server and the other network components.

The ports connecting the Agent Handler to the McAfee ePO server and SQL database must be open to connect to the Agent Handler through a firewall.

**Table 10-1 Default ports used**

| Server | Direction | Connection | Port |
|---|---|---|---|
| McAfee ePO | To | Web browser | HTTPS 8443 |
| McAfee ePO | To | SQL database | JDBC/SSL 1433 |
| Agent Handler | From | McAfee ePO | HTTPS 8443 (install), HTTPS 8444 |
| Agent Handler | Both | McAfee ePO | HTTP 80 |
| Agent Handler | To | SQL database | ADO/SSL 1433 |
| Agent Handler | To | Clients | HTTP 8081 |
| Agent Handler | From | Clients | HTTP 80, HTTPS 443 |

## Roaming with Agent Handlers

Agent Handlers allow users who roam between enterprise network sites to connect to the nearest Agent Handler.

Roaming is possible only if the Agent Handlers from all locations are configured in the McAfee Agent failover list. You can modify policy and system sorting so that roaming systems can receive a different policy in each location.

## Repository cache and how it works

Agent Handlers automatically cache content and product updates if a McAfee Agent can't access the content directly from the Master Repository on the McAfee ePO server.

The McAfee Agent, by default, uses the primary McAfee ePO server (same server as Tomcat) as the Master Repository. Agents fail back to the Agent Handler if they are unable to communicate with their configured remote repository to pull content and product updates. Since the Agent Handler might not be running on the same server as the true Master Repository (on the McAfee ePO server), the Agent Handler manages these requests. Agent Handlers transparently handle requests for software and cache the required files after downloading them from the Master Repository. No configuration is necessary.

This figure shows how Agent Handlers cache product update content if the configured remote repository is unavailable to remote systems.

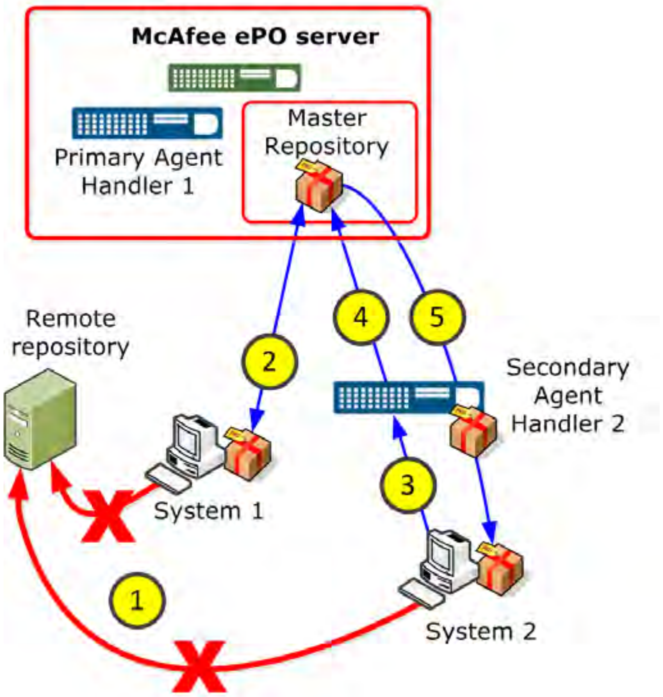


**Figure 10-6 Agent Handler repository caching**

These steps describe the numbers shown in the previous figure.

1 Systems 1 and 2 attempt to pull content or product updates from their configured remote repository and the attempt fails.

2 For System 1, the McAfee Agent is configured, by default, to use Primary Agent Handler 1 that is part of the McAfee ePO server. If the connection to the remote repository fails, System 1 requests the content or product updates directly from the Master Repository on the McAfee ePO server.

3 For System 2, the McAfee Agent is configured to use Secondary Agent Handler 2, unless the connection to the remote repository fails.

4 Secondary Agent Handler 2 requests the content or product updates from the Master Repository.

5 Secondary Agent Handler 2 caches those updates, for any subsequent requests, and delivers them to System 2.

# Agent Handler installation and configuration

You can configure mid-range servers, located within your network, as Agent Handlers by simply installing the Agent Handler software and assigning systems for management.

You can also group Agent Handlers, set their failover priority, and create virtual Agent Handlers behind a DMZ, firewall, or in NAT networks.

> Whenever you change a policy, configuration, client or server task, automatic response, or report, export the settings before and after the change. For detailed instructions about exporting objects, see the McAfee ePolicy Orchestrator Product Guide.

## Deployment considerations

Before you deploy Agent Handlers in your extended network, consider the health of your existing McAfee ePO server and database hardware. If this hardware is already overloaded, adding Agent Handlers actually decreases McAfee ePO performance.

A fully configured Agent Handler has about the same hardware and database requirements as a McAfee ePO server. When determining how many Agent Handlers you need, first examine the database usage. If the database serving your McAfee ePO server is under a heavy load, adding Agent Handlers does not improve your performance. You need to upgrade your SQL Server hardware to take advantage of multiple Agent Handlers. If the database is currently running at a moderate to low load, then additional Agent Handlers can help you expand your logical McAfee ePO infrastructure.

McAfee testing shows that adding Agent Handlers improves performance until your McAfee ePO database CPU load exceeds 70 percent. Since each Agent Handler adds some overhead, for example database connections and management queries to the database, adding Agent Handlers beyond 70 percent database CPU load does not help performance. See Finding and using Performance Monitor on page 145 to check your Windows server CPU load.

## Agent Handler configuration overview

Agent Handlers can be configured to load balance in groups and as virtual Agent Handlers.

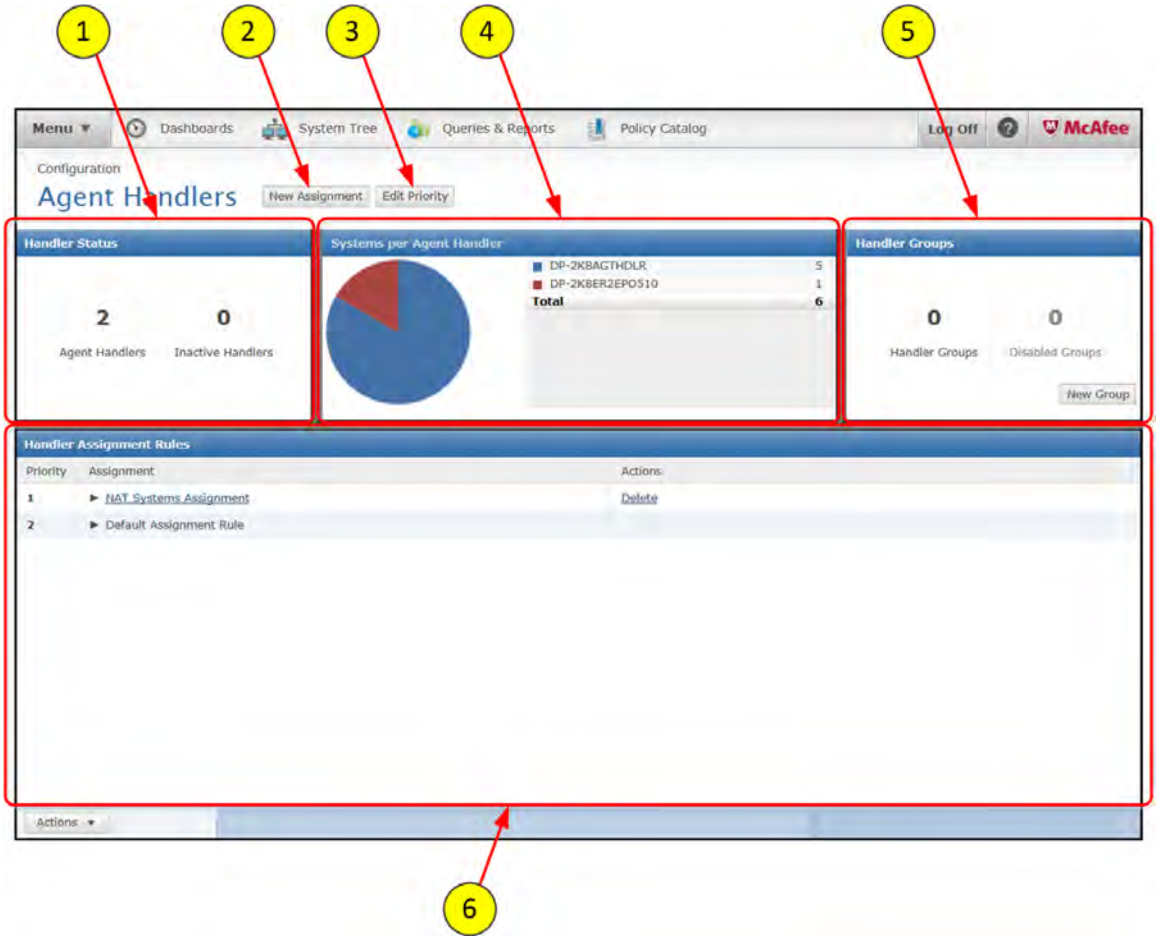
Virtual Agent Handlers allow clients to find them using different IP addresses on more than one network segment using priority assignment rules.

These documents include detailed Agent Handler instructions.

- McAfee ePolicy Orchestrator 5.1.0 Installation Guide — Provides instructions for installing remote Agent Handler software
- McAfee ePolicy Orchestrator 5.1.0 Product Guide — Provides information for configuring remote Agent Handlers

## Agent Handlers configuration page

To configure all Agent Handler management tasks, click **Menu** | **Configuration** | **Agent Handlers**.



| | | |
|---|---|---|
| ■ | DP-2K8AGTHDLR | 5 |
| ■ | DP-2K8ER2EPO510 | 1 |
| | Total | 6 |

| Priority | Assignment | Actions |
|---|---|---|
| 1 | ► NAT Systems Assignment | Delete |
| 2 | ► Default Assignment Rule | |

**Figure 10-7 Agent Handlers configuration page**

The Agent Handlers configuration page includes:

1 **Handler Status** — Provides the number of installed Agent Handlers and if they are active.

2 **New Assignment** — Opens the Agent Handler Assignment page to create an Agent Handler assignment.

3 **Edit Priority** — Opens the Edit Priority page to change priority of the Agent Handler assignments.

4 **Systems per Agent Handler** — Specifies the number of agents assigned to each Agent Handler.

> To see a detailed list of the agents assigned to an Agent Handler, click the Agent Handler name in the list or the color associated with the Agent Handler segment in the pie chart.

5 **Handler Groups** — Specifies the number of Agent Handler groups that the McAfee ePO server manages.

6 **Handler Assignment Rules** — Displays the list of Agent Handler Assignments in your environment, their priority, and details about rule settings.

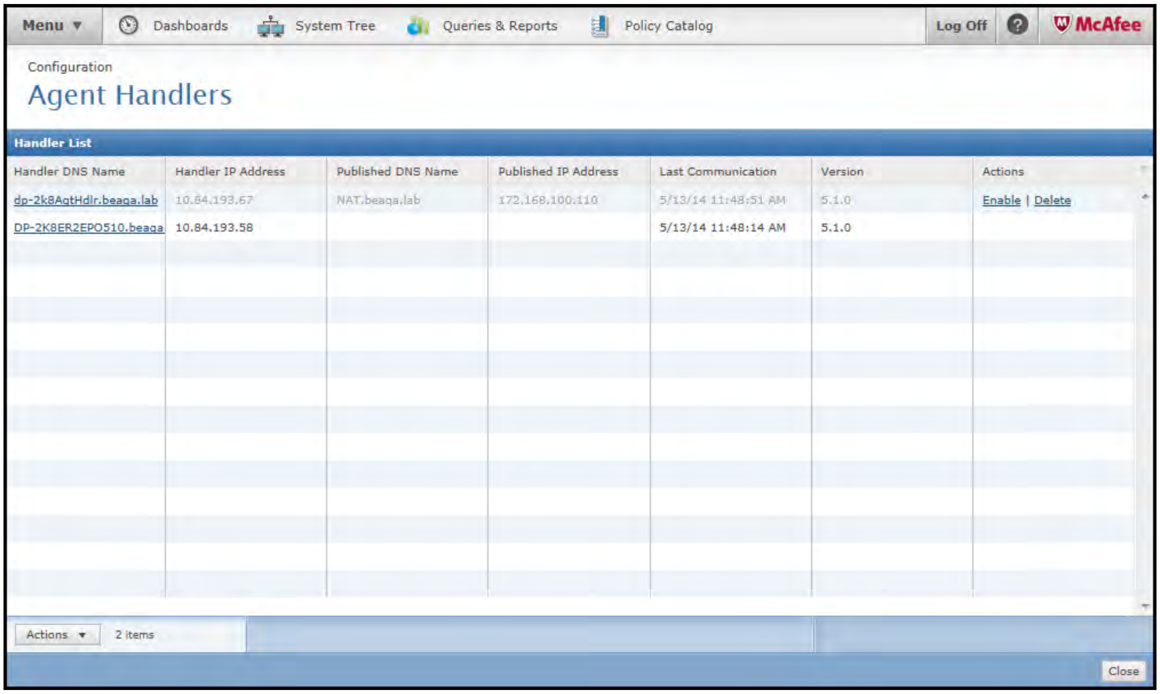
## Configure Agent Handlers list

To see a list of your Agent Handlers and their detailed information, use the Handlers List accessed through the dashboard.

### Task

For option definitions, click **?** in the interface.

1. Click **Menu** | **Configuration** | **Agent Handlers**, to configure an Agent Handler.
2. Click the Agent Handlers number in the **Handler Status** of the dashboard, to see a list of your Agent Handlers and their detailed information.



Configuration

Agent Handlers

Handler List

| Handler DNS Name | Handler IP Address | Published DNS Name | Published IP Address | Last Communication | Version | Actions |
|---|---|---|---|---|---|---|
| dp-2k8AgtHdlr.beaga.lab | 10.84.193.67 | NAT.beaqa.lab | 172.168.100.110 | 5/13/14 11:48:51 AM | 5.1.0 | Enable \| Delete |
| DP-2K8ER2EPO510.beaga | 10.84.193.58 | | | 5/13/14 11:48:14 AM | 5.1.0 | |

**Figure 10-8 Agent Handlers list page**

3. Click the setting in the **Actions** column, to disable, enable, and delete Agent Handlers, c.
4. Click the Agent Handler name in the **Handler DNS Name** column to configure Agent Handler Settings.
5. From the Agent Handler Settings page, configure these properties.
   - **Published DNS Name**
   - **Published IP Address**
6. Click **Save**

## Configure Agent Handlers groups and virtual groups

You can configure your Agent Handlers into groups and create virtual handlers to use behind a DMZ, firewall, or in NAT networks.

### Task

For option definitions, click **?** in the interface.

1. Click **Menu** | **Configuration** | **Agent Handlers** and, in the **Handler Group** dashboard, click **New Group** to create Agent Handler groups.
2. From the Agent Handlers Add/Edit Group page, configure these group settings:
   - **Group Name** — Type a name for the Agent Handler group.
   - **Included Handlers** — Allows you to:
     - Click **Use load balancer** to use a third-party load balancer, then type the **Virtual DNS Name** and **Virtual IP address** in the fields (both are required).
     - Click **Use custom handler list** and use **+** and **–** to add and remove additional Agent Handlers. Use the drag and drop handle to change the priority of Agent Handlers.
3. Click **Save**

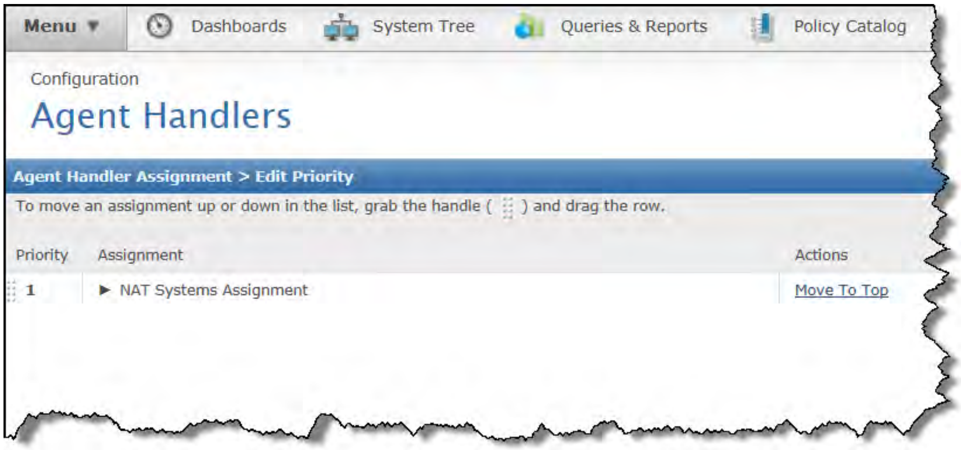
## Configure Agent Handlers priority

You can configure the failover priority of your Agent Handlers by setting their failover priorities.

### Task

For option definitions, click **?** in the interface.

1. Click **Menu** | **Configuration** | **Agent Handlers**, then click **Edit Priority** to create Agent Handler groups.
2. Click and drag the Agent Handlers to create the priority list you need for your network.



Configuration

Agent Handlers

Agent Handler Assignment > Edit Priority

To move an assignment up or down in the list, grab the handle ( ⋮ ) and drag the row.

| Priority | Assignment | Actions |
|---|---|---|
| 1 | ▶ NAT Systems Assignment | Move To Top |

**Figure 10-9 Agent Handlers priority settings**

3. Click **Save**.

## Configure assignments for Agent Handlers

You can assign agents to use Agent Handlers individually or as groups.

> When assigning systems to Agent Handlers, consider geographic proximity to reduce unnecessary network traffic.

### Task

For option definitions, click **?** in the interface.

1. Click **Menu | Configuration | Agent Handlers**, then click **New Assignment** to modify the assignments for Agent Handlers.
2. From the Agent Handler Assignment page, configure these settings:
   - **Assignment Name** — Type a name for the assignment.
   - **Agent Criteria** — Choose one of these methods to assign agents to Agent Handlers:
     - **System Tree location** — Click **System Tree**, select the System Tree Group from the dialog box, then click **OK**.
     - **Agent Subnet** — Type the IPv4/IPv6 address, IPv4/IPv6 address ranges, subnet masks, or subnet masks range.
   - **Handler Priority** — To configure the priority used by the McAfee Agent, select:
     - **Use all agent handlers** — Agents randomly select which handler to communicate with.
     - **Use custom handler list** — Use **+** and **–** to add more or remove Agent Handlers. Use the drag and drop handle to change the priority of handlers.
3. Click **Save**.

## Adding an Agent Handler in the DMZ

Agent Handlers in the DMZ allow you to directly manage systems with a McAfee Agent installed. Without an Agent Handler installed in the DMZ, you can only view those systems with your McAfee ePO server.

The Agent Handler you install in the DMZ has specific hardware and software requirements. These requirements are similar to the McAfee ePO server requirements. See this information before you begin:

- See Server hardware requirements on page 18 for Agent Handler hardware and operating system requirements.
- See Using Agent Handlers behind a DMZ, firewall, or in NAT networks on page 126 for an overview of this configuration and the default ports used.

These are the major steps to configure an Agent Handlers in the DMZ.

1. Install the Windows Server hardware and software in the DMZ between your networks that are internal and external to McAfee ePO.
2. Configure all ports on your firewall between your McAfee ePO server and SQL database and the Agent Handler.
3. Install the McAfee ePO remote Agent Handler software using the information in the McAfee ePolicy Orchestrator Installation Guide.
4. If needed, create a subgroup of systems to communicate with the McAfee ePO server through the Agent Handler.
5. Create an Agent Handlers assignment.
6. Configure the Agent Handlers priority list and enable the Agent Handler in the DMZ.

## Configure hardware, operating system, and ports

Installing the Agent Handler server hardware, software, and configuring the firewall ports are the first steps before using McAfee ePO to manage systems behind a DMZ.

> **Before you begin**
>
> See these topics for Agent Handler server hardware and software requirements:
>
> - Server hardware requirements on page 18
> - McAfee ePolicy Orchestrator Installation Guide, operating system requirements

### Task

1. In the DMZ of your firewall protected network, install the Agent Handler server hardware and Microsoft Windows server operating system.

   Confirm all the latest operating system security patches are installed.

2. Configure your Domain Name System (DNS) server to host the Agent Handler server to the internal McAfee ePO network.

3. Configure these ports on the *internal-facing* firewall to communicate between the McAfee ePO server and the Agent Handler in DMZ:

   - Port 80 — Bidirectional
   - Port 8443 — Bidirectional
   - Port 8444 — Bidirectional
   - Port 443 — Bidirectional

4. **Optional** — If your SQL database is installed on a different server than your McAfee ePO server, configure these two ports on the *internal-facing* firewall for that connection to the Agent Handler:

   - Port 1433 TCP — Bidirectional
   - Port 1434 UDP — Bidirectional

5. Configure these ports on the *public-facing* firewall to communicate between the McAfee ePO server and the Agent Handler in the DMZ:

   - Port 80 TCP — Inbound
   - Port 443 TCP — Inbound
   - Port 8081 TCP — Inbound
   - Port 8082 UDP — Inbound

Now you have installed your Agent Handler hardware and server operating system in the DMZ. Plus, you configured all ports to connect through the firewall between the McAfee ePO server and database to the Agent Handler server.

## Install software and configure the Agent Handler

When you complete the McAfee ePO Agent Handler software installation and configuration, your Agent Handler allows you to directly manage systems behind the DMZ.

> **Before you begin**
>
> You must have installed the Agent Handler hardware and operating system in the DMZ of your external network. See Agent Handler configuration overview on page 129 for details.

### Task

For option definitions, click **?** in the interface.

1. To install the McAfee ePO remote Agent Handlers software, see the McAfee ePolicy Orchestrator Installation Guide.

   These instructions assume that you have access to the McAfee ePO executable files located in the downloaded ePolicy Orchestrator installation files.

2. Create a subgroup of systems to communicate through the Agent Handler to the McAfee ePO server.

   There are many ways to create this subgroup. In this example, there is a subgroup, named **NAT Systems** in the System Tree behind the DMZ.

   > Alternately, in Agent Subnet you can type IP addresses, IP address ranges, or subnet masks, separated by commas, spaces, or new lines.

3. To start the **Agent Handler** configuration, click **Menu** | **Configuration** | **Agent Handlers**.

   You use this McAfee ePO page to configure all Agent Handler settings. See Agent Handler configuration overview on page 129.

4. To create the Agent Handler assignment settings, click **New Assignment** and configure these settings:

   a. Type an **Assignment Name**. For example, `NAT Systems Assignment`.

   b. Next to Agent Criteria, click **Add Tree Locations** and the "..." to select a System Tree group and click **OK**.

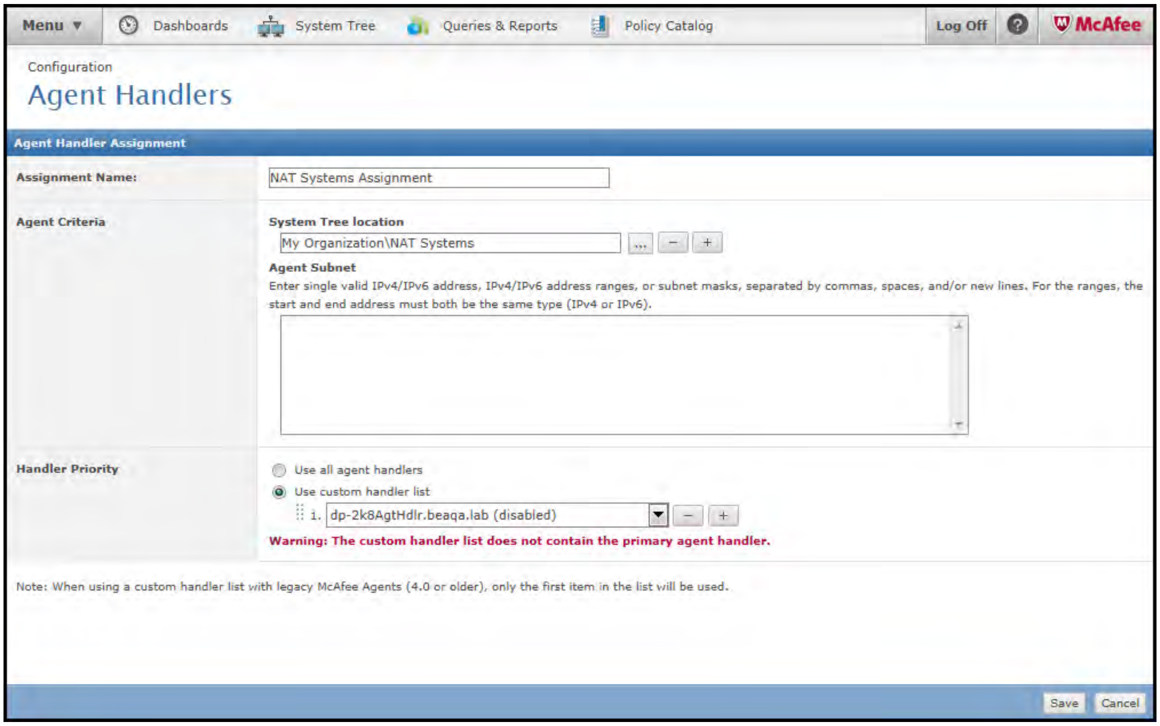
      For example, select the NAT Systems group.

   c. Next to Handler Priority, click **Use custom handler list** and **Add Handlers**.

d From the list, select the Agent Handler to handle these selected systems.

Disregard the warning that appears.

e Click **Save**.



Configuration

Agent Handlers

Agent Handler Assignment

Assignment Name: NAT Systems Assignment

Agent Criteria

System Tree location: My Organization\NAT Systems

Agent Subnet

Enter single valid IPv4/IPv6 address, IPv4/IPv6 address ranges, or subnet masks, separated by commas, spaces, and/or new lines. For the ranges, the start and end address must both be the same type (IPv4 or IPv6).

Handler Priority

○ Use all agent handlers

● Use custom handler list

1. dp-2k8AgtHdlr.beaqa.lab (disabled)

Warning: The custom handler list does not contain the primary agent handler.

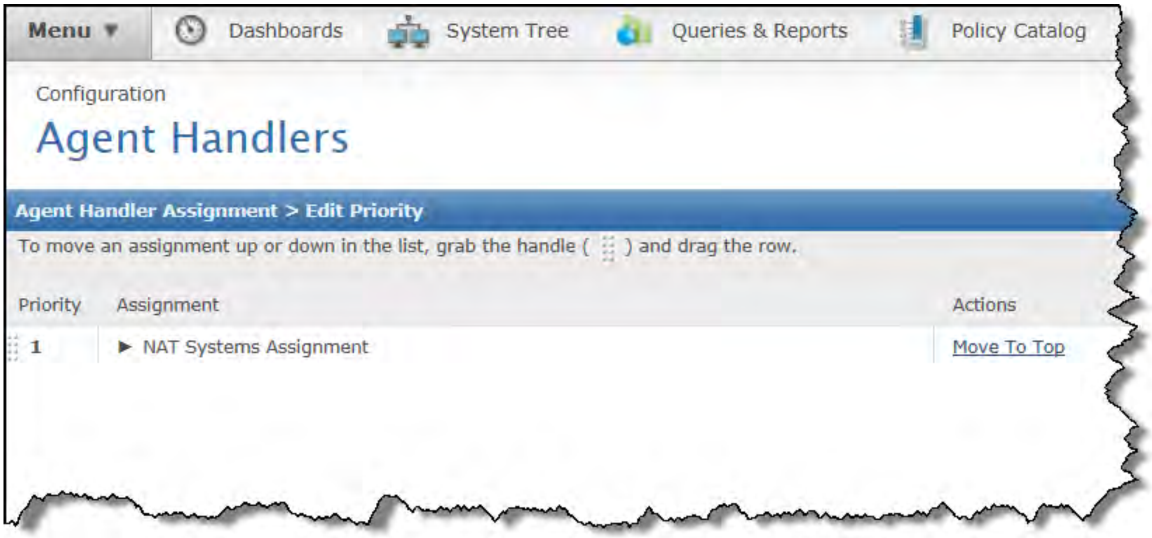
Note: When using a custom handler list with legacy McAfee Agents (4.0 or older), only the first item in the list will be used.

**Figure 10-10 Agent Handler Assignment page**

5 To configure the Agent Handler as the highest priority for the systems behind the DMZ, click **Edit Priority** and configure these settings, from the Agent Handler Configuration page:

a Move the Agent Handler to the top of the priority list by moving the Agent Handler names.

b Click **Save**.



Configuration

Agent Handlers

Agent Handler Assignment > Edit Priority

To move an assignment up or down in the list, grab the handle ( ⋮⋮ ) and drag the row.

| Priority | Assignment | Actions |
|---|---|---|
| 1 | ▶ NAT Systems Assignment | Move To Top |

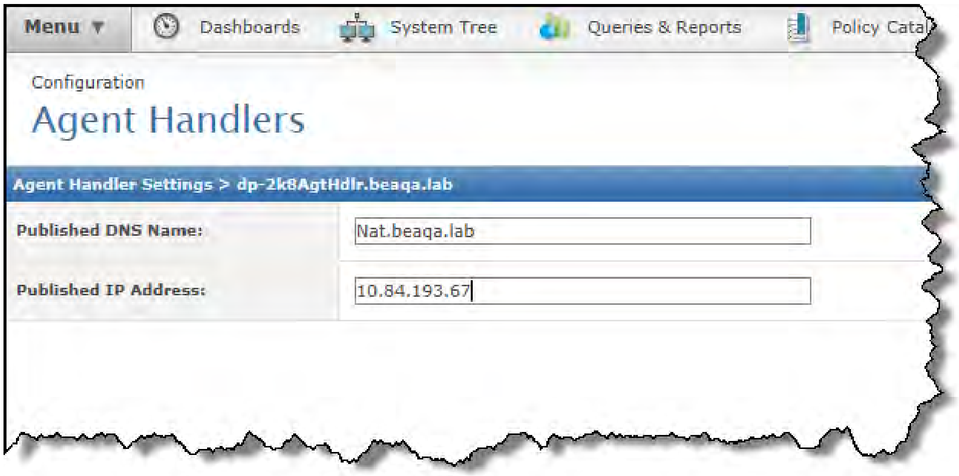
**Figure 10-11 Agent Handler Assignment page**

6 From the **Agent Handler** configuration page, in the **Handler Status** dashboard, click the number of the **Agent Handlers** to open the **Agent Handlers List** page.

7 From the Agent Handler Settings page, configure these settings and click **Save**:

a Type the Published DNS Name configured for the Agent Handler.

b Type the Published IP Address configured for the Agent Handler.



Configuration

Agent Handlers

Agent Handler Settings > dp-2k8AgtHdlr.beaqa.lab

Published DNS Name: Nat.beaqa.lab

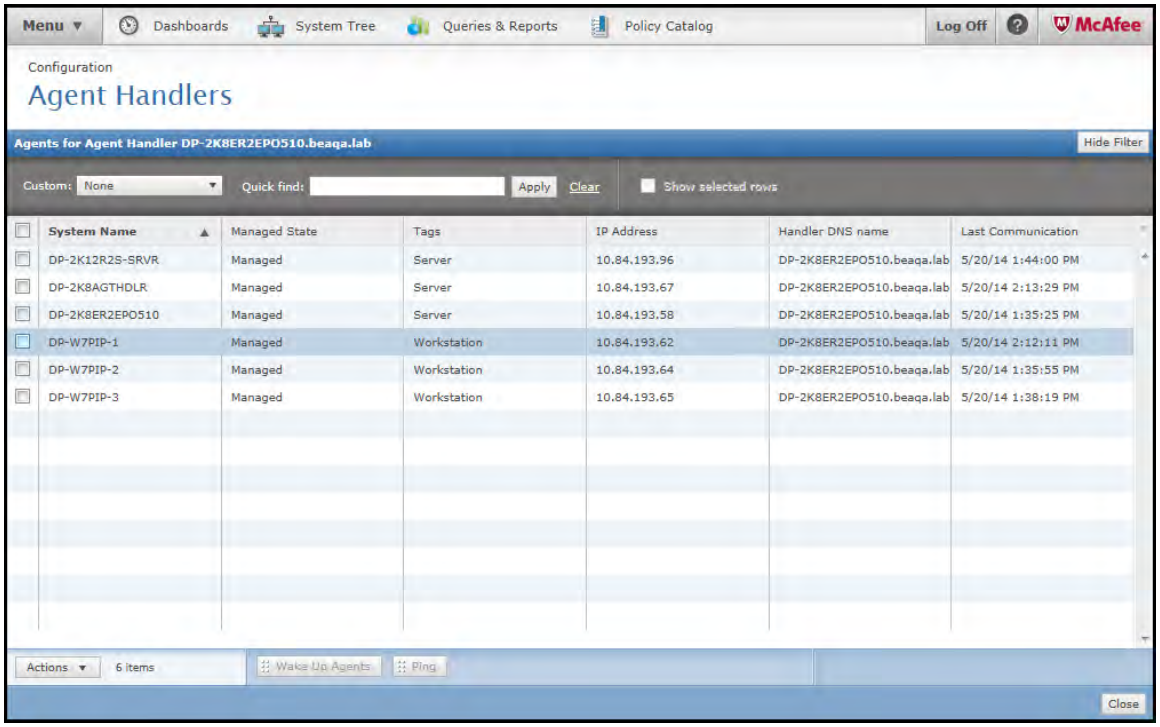
Published IP Address: 10.84.193.67

**Figure 10-12 Agent Handlers settings page**

8 From the Handlers List page, in the row for the Agent Handler in the DMZ, click **Enable** in the Actions column.

9. To confirm that the Agent Handler in the DMZ is managing the systems behind the DMZ, perform these steps:
   a. From the Agent Handlers Configuration page, in the **Systems per Agent Handler** dashboard, click either the Agent Handler name in the list or the corresponding color for the Agent Handler in the pie chart.
   b. From the Agents for Agent Handler page, confirm that the correct systems appear in the list.

   > It might take multiple instances of the agent-server communication before all systems appear in the list.



Configuration

Agent Handlers

Agents for Agent Handler DP-2K8ER2EPO510.beaqa.lab

Custom: None ▼ Quick find: Apply Clear □ Show selected rows

| □ | System Name ▲ | Managed State | Tags | IP Address | Handler DNS name | Last Communication |
|---|---|---|---|---|---|---|
| □ | DP-2K12R2S-SRVR | Managed | Server | 10.84.193.96 | DP-2K8ER2EPO510.beaqa.lab | 5/20/14 1:44:00 PM |
| □ | DP-2K8AGTHDLR | Managed | Server | 10.84.193.67 | DP-2K8ER2EPO510.beaqa.lab | 5/20/14 2:13:29 PM |
| □ | DP-2K8ER2EPO510 | Managed | Server | 10.84.193.58 | DP-2K8ER2EPO510.beaqa.lab | 5/20/14 1:35:25 PM |
| □ | DP-W7PIP-1 | Managed | Workstation | 10.84.193.62 | DP-2K8ER2EPO510.beaqa.lab | 5/20/14 2:12:11 PM |
| □ | DP-W7PIP-2 | Managed | Workstation | 10.84.193.64 | DP-2K8ER2EPO510.beaqa.lab | 5/20/14 1:35:55 PM |
| □ | DP-W7PIP-3 | Managed | Workstation | 10.84.193.65 | DP-2K8ER2EPO510.beaqa.lab | 5/20/14 1:38:19 PM |

Actions ▼ 6 items

**Figure 10-13 Agent Handler systems page**

Now with the Agent Handlers in the DMZ and configured with the McAfee ePO server, you can directly manage systems with a McAfee Agent installed behind the DMZ.

# Frequently Asked Questions

Here are answers to frequently asked questions.

### What ports do I open in my firewall to allow the Agent Handler?

See Using Agent Handlers behind a DMZ, firewall, or in NAT networks on page 126 for a table of default ports used.

### What data is sent to the McAfee ePO server and what is sent to the database?

A data channel is a mechanism for McAfee products to exchange messages between their endpoint plug-ins and their management extensions. The data channel provides the majority of data sent from the Agent Handler to the application server. It is used internally by the McAfee ePO server for agent deployment and wake-up progress messaging. Other functions such as agent properties, tagging, and policy comparisons are performed directly against the McAfee ePO database.

### If the McAfee ePO server is not defined in my repository list, does replication still occur?

Yes, if the agent contacts the Agent Handler for software packages, the Agent Handler retrieves them from the McAfee ePO server Master Repository. See Repository cache and how it works on page 128.

### How much bandwidth is used for communication between the database and the Agent Handler?

Bandwidth between the Agent Handler and the database varies based on the number of agents connecting to that Agent Handler. However, each Agent Handler places a fixed load on the database server for:

- Heartbeat (updated every minute)
- Work queue (checked every 10 seconds)
- Database connections held open to the database (2 connections per CPU for EventParser plus 4 connections per CPU for Apache)

### How many agents can one Agent Handler support?

Agent Handlers for scalability are not required until a deployment reaches 100,000 nodes. Agent Handlers for topology or failover might be required at any stage. A good rule is one Agent Handler per 50, 000 nodes.

### What hardware and operating system should I use for an Agent Handler?

Use the Microsoft Server Operating System (2008 SP2+ server or 2012 64-bit server). See Server hardware requirements on page 18.

> Non-server Operating System versions have severe (~10) limits set on the number of incoming network connections.

# Maintaining and optimizing your McAfee ePO software

The McAfee ePO server requires little maintenance, but some optimization and automation can help you perform everyday tasks while protecting your network.

11

# Maintaining your McAfee ePO server

Generally your McAfee ePO server does not require periodic maintenance, but if your server performance changes, take these steps before calling technical support.

> The SQL database used by the McAfee ePO server requires regular maintenance and back ups to ensure that McAfee ePO functions correctly.

### Contents

## Monitoring server performance

You should periodically check how hard your McAfee ePO server is working so that you can create benchmarks and avoid performance problems.

If you suspect your McAfee ePO server is having performance problems, use Windows Task Manager and Windows Server Reliability and Performance Monitor to check the performance.

### Using Windows Task Manager

The first steps to take if your McAfee ePO server is having performance problems are to start Windows Task Manager on the server and check McAfee ePO server performance.

- Is there excessive paging?
- Is the physical memory over-utilized?
- Is the CPU over-utilized?

See the How to use and troubleshoot issues with Windows Task Manager website for details.

## Using the Windows Reliability and Performance Monitor

When you install McAfee ePO server, custom counters are added to the built-in Windows Reliability and Performance Monitor. Those counters are informative and can give you an idea of how hard the McAfee ePO server is working.

> You must use the 32-bit version of the Reliability and Performance Monitor found at `C:\Windows\SysWOW64\perfmon.exe`. The default 64-bit version of Reliability and Performance Monitor does not have the custom McAfee ePO counters added.

See these links for Microsoft Windows Performance Monitor information:

- Configure the Performance Monitor Display
- Working with Performance Logs

**See also**

*Finding and using Performance Monitor* on page 145

# Finding and using Performance Monitor

To use the custom McAfee ePO counters with the Windows Performance Monitor, you must use the 32-bit version of the tool.

## Task

1 To find the 32-bit version of the Windows Performance Monitor, use Windows Explorer and navigate to `C:\Windows\SysWOW64`, then find and double-click **perfmon.exe**.

2 To confirm that you opened the 32-bit version of Performance Monitor, click **Monitoring Tools** | **Performance Monitor**, **Add Counters**, then click the **+** sign to open the Add Counters dialog box.

3 To find the McAfee ePO server counters, scroll down the list of counters, find **ePolicy Orchestrator Server**, and expand the list.

This screen is an example of the McAfee ePO Server counters.

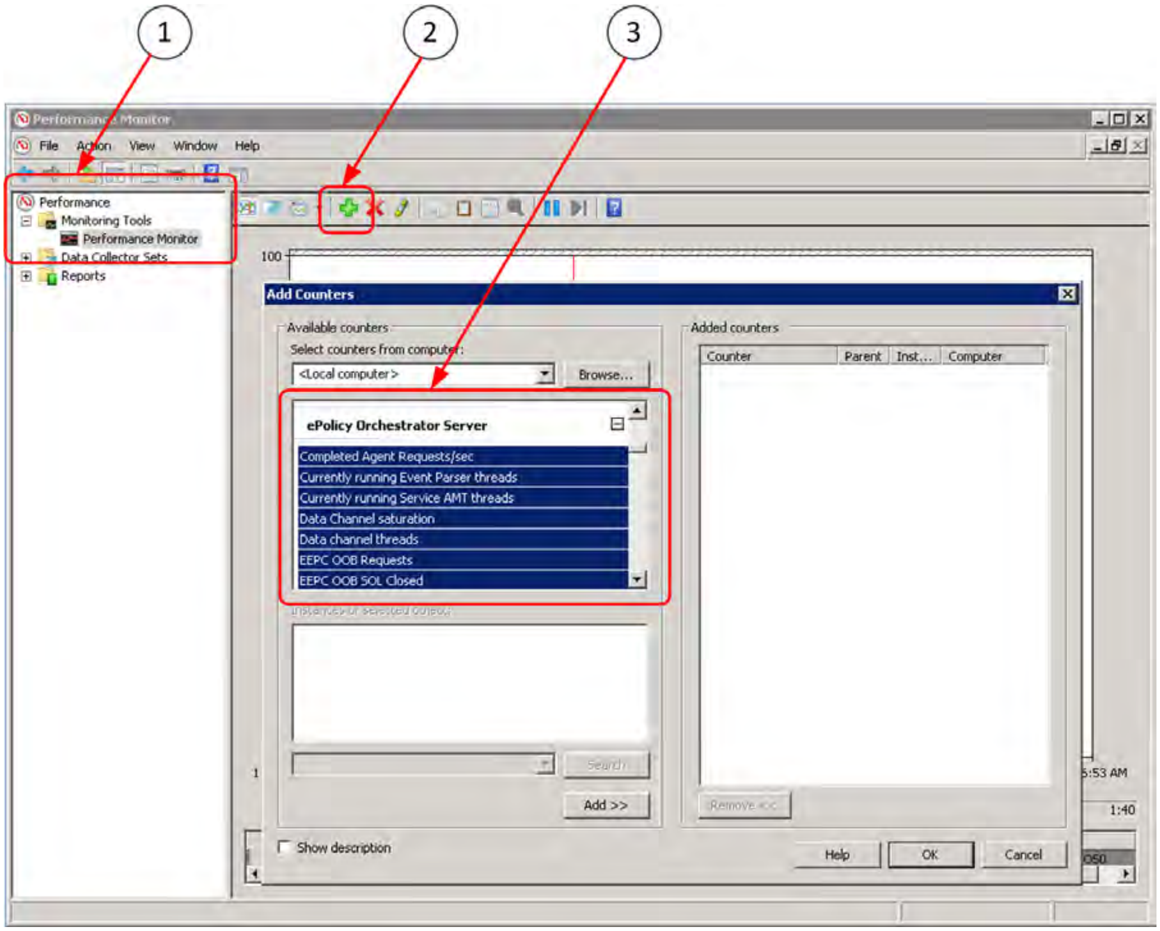


**Figure 11-1 Windows Performance Monitor showing the ePolicy Orchestrator Server counters**

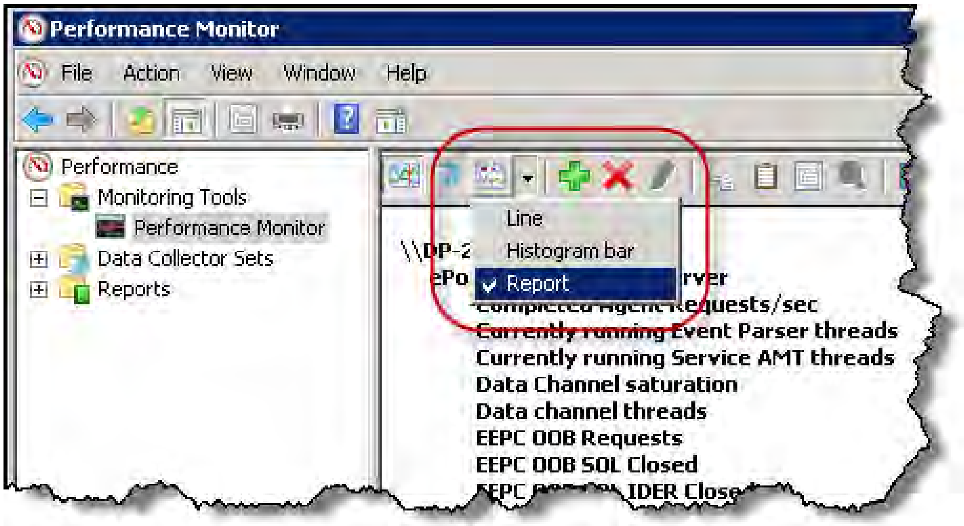
Now you can start using the counters to test and create benchmarks for your McAfee ePO server performance.

## Use "perfmon" with ePolicy Orchestrator

The 32-bit Windows Reliability and Performance Monitor is a tool to develop server benchmarks, which can help you manage your server performance.

### Task

1. Start the Windows 32-bit Performance Monitor.
2. In the **Add Counters** list, browse or scroll down to the **ePolicy Orchestrator Server** counters selection, then click **+** to expand the list of counters.
3. To view the output as a report, click the **Change Graph Type** icon and select **Report** from the list.



equests/sec
Currently running Event Parser threads
Currently running Service AMT threads
Data Channel saturation
Data channel threads
EEPC OOB Requests
EEPC OOB SOL Closed
EEPC IDER Close

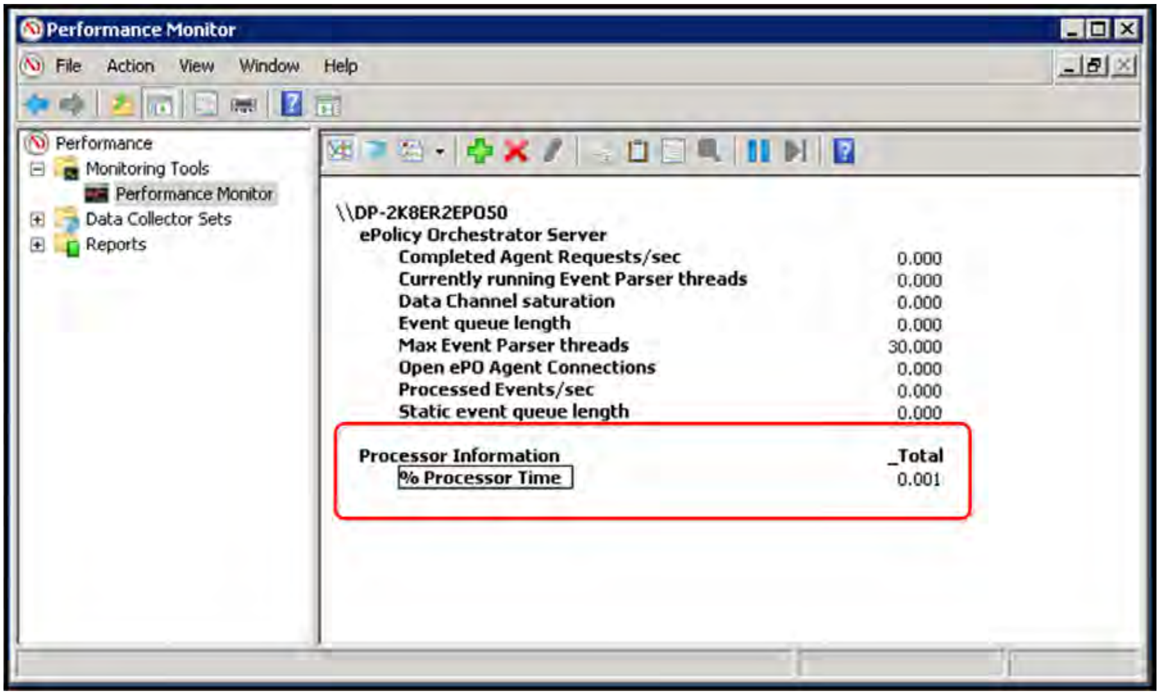
**Figure 11-2 Windows Performance Monitor Reports menu**

For example, the **Open ePO Agent Connections** counter tells you how many agents are communicating with the McAfee ePO server simultaneously. A healthy McAfee ePO server keeps this number fairly low, usually under 20. For a McAfee ePO server that is struggling, this number is over 200 (the maximum is 250) and stays high, and rarely drops below 20.

4. Click **Add** to move the selected counter into the Added counters list, then click **OK**.
5. To determine the stress on your McAfee ePO server and how quickly it can process events from all your agents, add the following counters, then click **OK**.

   - **Completed Agent Requests/sec**
   - **Currently Running Event Parser Threads**
   - **Data Channel saturation**
   - **Data channel threads**
   - **Event Queue Length**
   - **Max Event Parser Threads**
   - **Open ePO Agent Connections**
   - **Processor Events/sec**
   - **Static even queue length**

This example shows the output of the McAfee ePO counters.



```
\\DP-2K8ER2EPO50
   ePolicy Orchestrator Server
         Completed Agent Requests/sec                    0.000
         Currently running Event Parser threads          0.000
         Data Channel saturation                         0.000
         Event queue length                              0.000
         Max Event Parser threads                       30.000
         Open ePO Agent Connections                      0.000
         Processed Events/sec                            0.000
         Static event queue length                       0.000

   Processor Information                                _Total
         % Processor Time                                0.001
```

**Figure 11-3 Windows Performance Monitor showing McAfee ePO processor time**

The tests listed here are just a few that you can perform with the McAfee ePO server using the Windows 32-bit Performance Monitor. For additional Windows Performance Monitor information, see these websites:

- Configure the Performance Monitor Display
- Working with Performance Logs

**See also**

*Send a policy change immediately* on page 53
*Finding and using Performance Monitor* on page 145

## Check event processing

The number of events appearing in the ePolicy Orchestrator database events folder can indicate the performance of your McAfee ePO server.

### Task

1 Using Windows Explorer, navigate to this folder:

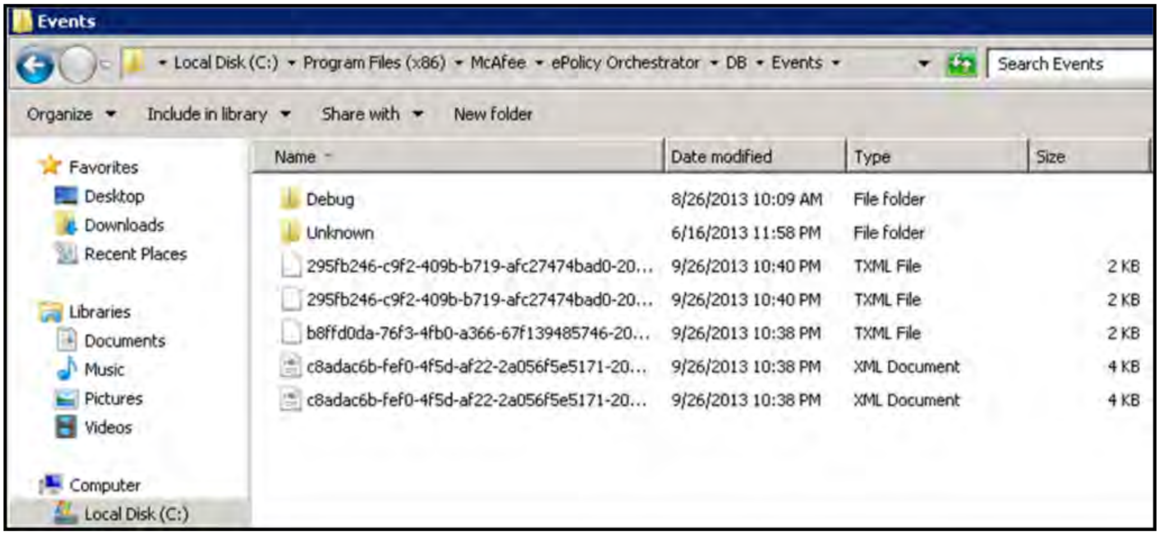
```
C:\Program Files (x86)\McAfee\ePolicy Orchestrator\DB\Events
```

At any time, this folder might display a few dozen or a few hundred events.

> In larger environments, this folder is constantly processing thousands of events per minute.

2 Click the **Refresh** icon multiple times, then look at the status bar to see the number of files in this folder changing quickly.

This screen is an example of the ePolicy Orchestrator Events folder.



| Name | Date modified | Type | Size |
|---|---|---|---|
| Debug | 8/26/2013 10:09 AM | File folder | |
| Unknown | 6/16/2013 11:58 PM | File folder | |
| 295fb246-c9f2-409b-b719-afc27474bad0-20... | 9/26/2013 10:40 PM | TXML File | 2 KB |
| 295fb246-c9f2-409b-b719-afc27474bad0-20... | 9/26/2013 10:40 PM | TXML File | 2 KB |
| b8ffd0da-76f3-4fb0-a366-67f139485746-20... | 9/26/2013 10:38 PM | TXML File | 2 KB |
| c8adac6b-fef0-4f5d-af22-2a056f5e5171-20... | 9/26/2013 10:38 PM | XML Document | 4 KB |
| c8adac6b-fef0-4f5d-af22-2a056f5e5171-20... | 9/26/2013 10:38 PM | XML Document | 4 KB |

**Figure 11-4 ePolicy Orchestrator Events folder**

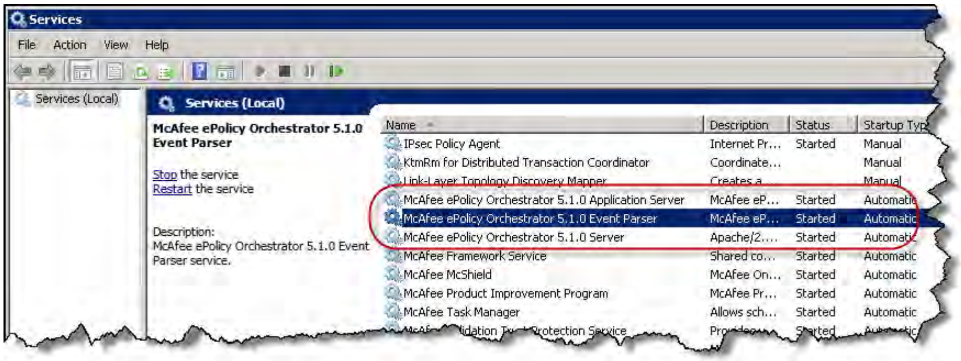
If there are thousands of files in this folder and McAfee ePO is unable to process them, the server is probably struggling to process the events at a reasonable rate.

> It is normal for this Events folder to fluctuate depending on the time of day. But, if there are thousands of files in this folder and it is constantly increasing then that probably indicates a performance issue.

3 Confirm that the events are not occurring faster than the event parser can process them. This causes this folder to grow quickly. Use these steps to confirm the event parser is running.

a To open the Windows Services Manager and confirm that the event parser is running, click **Start**, **Run**, type `services.msc` and click **OK**.

b In the Services Manager list, find **McAfee ePolicy Orchestrator 5.1.0 Event Parser** and confirm it is **Started**.



**McAfee ePolicy Orchestrator 5.1.0 Event Parser**

Stop the service
Restart the service

Description:
McAfee ePolicy Orchestrator 5.1.0 Event Parser service.

| Name | Description | Status | Startup Typ |
|---|---|---|---|
| IPsec Policy Agent | Internet Pr... | Started | Manual |
| KtmRm for Distributed Transaction Coordinator | Coordinate... | | Manual |
| Link-Layer Topology Discovery Mapper | Creates a ... | | Manual |
| McAfee ePolicy Orchestrator 5.1.0 Application Server | McAfee eP... | Started | Automatic |
| McAfee ePolicy Orchestrator 5.1.0 Event Parser | McAfee eP... | Started | Automatic |
| McAfee ePolicy Orchestrator 5.1.0 Server | Apache/2.... | Started | Automatic |
| McAfee Framework Service | Shared co... | Started | Automatic |
| McAfee McShield | McAfee On... | Started | Automatic |
| McAfee Product Improvement Program | McAfee Pr... | Started | Automatic |
| McAfee Task Manager | Allows sch... | Started | Automatic |
| McAfee Validation Trust Protection Service | Provides ... | Started | Automatic |

**Figure 11-5 Windows Serviced running**

4 Check the event parser log file for any errors, using these steps.

a Go to the log file folder at this path:

```
C:\Program Files (x86)\McAfee\ePolicy Orchestrator\DB\Logs
```

b Open this log file and check for errors:

**eventparser_<serverName>.log**

5 Use these steps if the events are still occurring faster than the event parser can process them.

a Open the Services Managers list again and *temporarily* stop all three of these McAfee ePO services:

- McAfee ePolicy Orchestrator 5.1.0 Application Server
- McAfee ePolicy Orchestrator 5.1.0 Event Parser
- McAfee ePolicy Orchestrator 5.1.0 Server

b Move the contents of the `C:\Program Files (x86)\McAfee\ePolicy Orchestrator\DB\Events\` folder to another location, or delete the events, if you're not worried about losing the data.

# Estimating and adjusting the ASCI

You might need to estimate and adjust the agent-server communication interval (ASCI) on your network, depending on the number of systems in your managed environment.

## Estimating the best ASCI

To improve the McAfee ePO server performance, you might need to adjust the ASCI setting for your managed network.

To determine whether you should change your ASCI, ask how often changes occur to endpoint policies on your McAfee ePO server. For most organizations, once your policies are in place, they don't often change. Some organizations change an endpoint policy less frequently than once every few months. That means a system calling in every 60 minutes looking for a policy change, about eight times in a typical work day, might be excessive. If the agent does not find any new policies to download, it waits until the next agent-server commnication, then checks again at its next scheduled check-in time.

To estimate the ASCI, your concern is not wasting bandwidth because agent-server communications are only a few kilobytes per communication. The concern is the strain put on the McAfee ePO server with every communication from every agent in larger environments. All of your agents need at least two communications a day with the McAfee ePO server. This requires a 180–240 minute ASCI in most organizations.

For organizations with fewer than 10,000 nodes, the default ASCI setting is not a concern at 60 minutes. But for organizations with more than 10,000 nodes, you should change the default setting of 60 minutes setting to about 3–4 hours.

For organizations with more than 60,000 nodes, the ASCI setting is much more important. If your McAfee ePO server is not having performance issues, you can use the 4-hour ASCI interval. If there are any performance issues, consider increasing your ASCI to 6 hours; possibly even longer. This significantly reduces the number of agents that are simultaneously connecting to the McAfee ePO server and improves the server performance.

> ℹ You can determine how many connections are being made to your McAfee ePO server by using the ePolicy Orchestrator Performance Counters.

This table lists basic ASCI guidelines.

| Node count | Recommended ASCI |
|---|---|
| 100–10,000 | 60–120 minutes |
| 10,000–50,000 | 120–240 minutes |
| 50,000 or more | 240–360 minutes |

**See also**

*Monitoring server performance* on page 143

## Configure the ASCI setting

After you estimate the best ASCI setting, reconfigure the setting in the McAfee ePO server.

The ASCI is set to 60 minutes by default. If that interval is too frequent for your organization, change it.

### Task

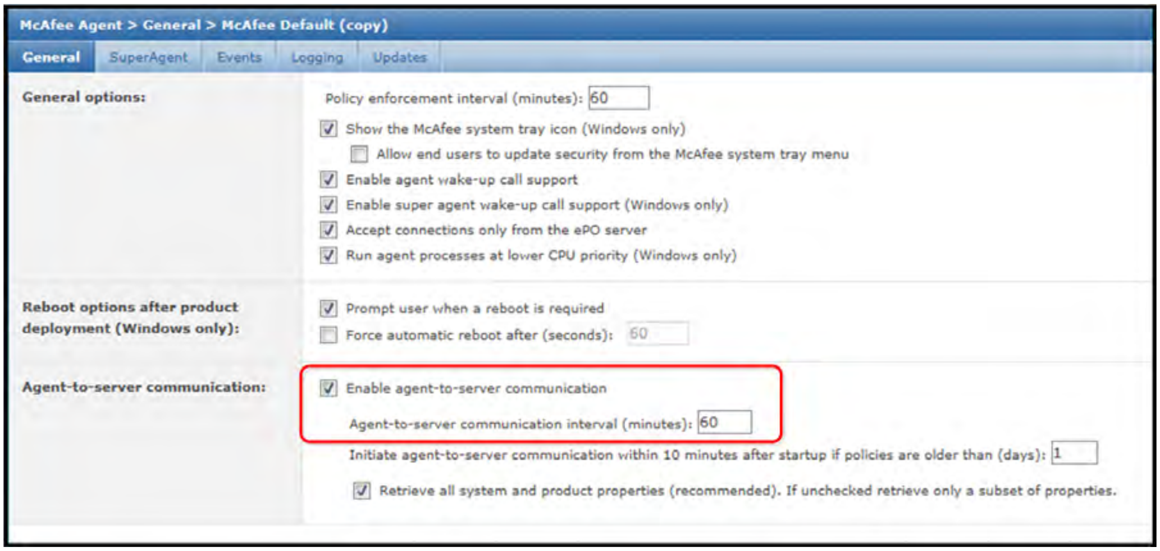
For option definitions, click **?** in the interface.

1 Click **Menu** | **Policy** | **Policy Catalog**, then select **McAfee Agent** from the **Product** list and **General** from the **Category** list.

2 Click the name of the policy you want to change and the **General** tab.

3 Next to **Agent-to-server communication interval**, type the number of minutes between updates.

This example shows the interval set to 60 minutes.



McAfee Agent > General > McAfee Default (copy)

General options:

Policy enforcement interval (minutes): 60

☑ Show the McAfee system tray icon (Windows only)

□ Allow end users to update security from the McAfee system tray menu

☑ Enable agent wake-up call support

☑ Enable super agent wake-up call support (Windows only)

☑ Accept connections only from the ePO server

☑ Run agent processes at lower CPU priority (Windows only)

Reboot options after product deployment (Windows only):

☑ Prompt user when a reboot is required

□ Force automatic reboot after (seconds): 60

Agent-to-server communication:

☑ Enable agent-to-server communication

Agent-to-server communication interval (minutes): 60

Initiate agent-to-server communication within 10 minutes after startup if policies are older than (days): 1

☑ Retrieve all system and product properties (recommended). If unchecked retrieve only a subset of properties.

**Figure 11-6 Policy Catalog Agent-to-server communication interval configuration**

4 Click **Save**.

If you send a policy change or add a client task immediately, you can execute an agent wake-up call.

**See also**

*Send a policy change immediately* on page 53

# Maintaining your SQL database

To help the McAfee ePO server function correctly, you must have a well performing SQL database. It is the central storage place for all the data your McAfee ePO server uses, and it requires maintenance.

## Maintaining the McAfee ePO SQL database

The SQL database requires regular maintenance and back ups to ensure that McAfee ePO functions correctly.

The McAfee ePO SQL database houses everything that McAfee ePO uses to function; your System Tree structure, policies, administrators, client tasks, and configuration settings.

Perform these tasks regularly to maintain your SQL Server:

- Regularly back up the McAfee ePO SQL database and its transaction log.
- Reindex your database regularly.
- Rebuild your database regularly.
- Purge older events using server tasks as described in Purging events automatically on page 170.

Back up your SQL database regularly, in case your SQL database or your McAfee ePO server environment fails. If the McAfee ePO server must be rebuilt or restored, current back ups ensure that a safe copy is available. In addition, if you are using the information in the website Microsoft Full Recovery Model for SQL, your transaction log can continue to grow indefinitely until a full back up is performed.

### Table data fragmentation

One of the most significant performance problems found in databases is table data fragmentation. For example, table fragmentation can be compared to an index at the end of a large book. A single index entry in this book might select several pages scattered throughout the book. You must then scan each page for the specific information you are looking for.

This fragmented index is different from the index of the telephone book that stores its data in sorted order. A typical query for the name "Jones" might span multiple consecutive pages, but they are always in a sorted order.

For of a database, you start with the data looking like a telephone book and, over time, end up with the data looking more like a large book index. You must occasionally resort the data to re-create the phone book order. This is where reindexing and rebuilding your McAfee ePO SQL database is critical. Over time your database becomes more fragmented, especially if it manages a larger environment where thousands of events are written to it daily.

Setting up a maintenance task to automatically re-index and rebuild your McAfee ePO SQL database takes only a few minutes and is essential to maintain proper performance on the McAfee ePO server. You can include the reindexing as part of your regular back up schedule to combine everything in one task.

Do **not** shrink your database. Data file shrink causes serious index fragmentation. Shrinking the database is a common mistake that many administrators make when building their maintenance task.

### Learn more

For details about creating your maintenance task, see KnowledgeBase article Recommended maintenance plan for McAfee ePO database using SQL Server Management Studio, KB67184.

To learn more about database fragmentation and how to determine the fragmentation of your database, use the DBCC command found in the Understanding SQL Server's DBCC SHOWCONTIG at the link: http://www.sql-server-performance.com/articles/dba/dt_dbcc_showcontig_p1.aspx.

To learn more about maintaining and optimizing your SQL database, see these documents:

- Improving McAfee ePO Performance by Optimizing SQL at the link: https://community.mcafee.com/docs/DOC-2926
- McAfee ePO Maintenance Utility at the link: https://community.mcafee.com/docs/DOC-4021

# Recommended tasks

McAfee recommends that you perform certain tasks daily, weekly, and monthly to ensure that your managed systems are protected and your McAfee ePO server is working efficiently.

Because all networks are different, your environment might require more detailed steps, or only some of the steps, described in this section.

> These are suggested best practices and do not guarantee 100-percent protection against security risks.

The processes outlined share these features:

- Once you learn the processes, they don't take too long to perform.
- They are repeatable, manageable, and effective practices.
- They are based on input from McAfee experts and IT managers.

## Recommended daily tasks

Perform these McAfee recommended tasks at least once a day to ensure that your server-managed network systems are safe from threats and your server is functioning normally.

Before you make any major changes to policies or tasks, McAfee recommends that you back up the database or create a snapshot of the records in the McAfee ePO database.

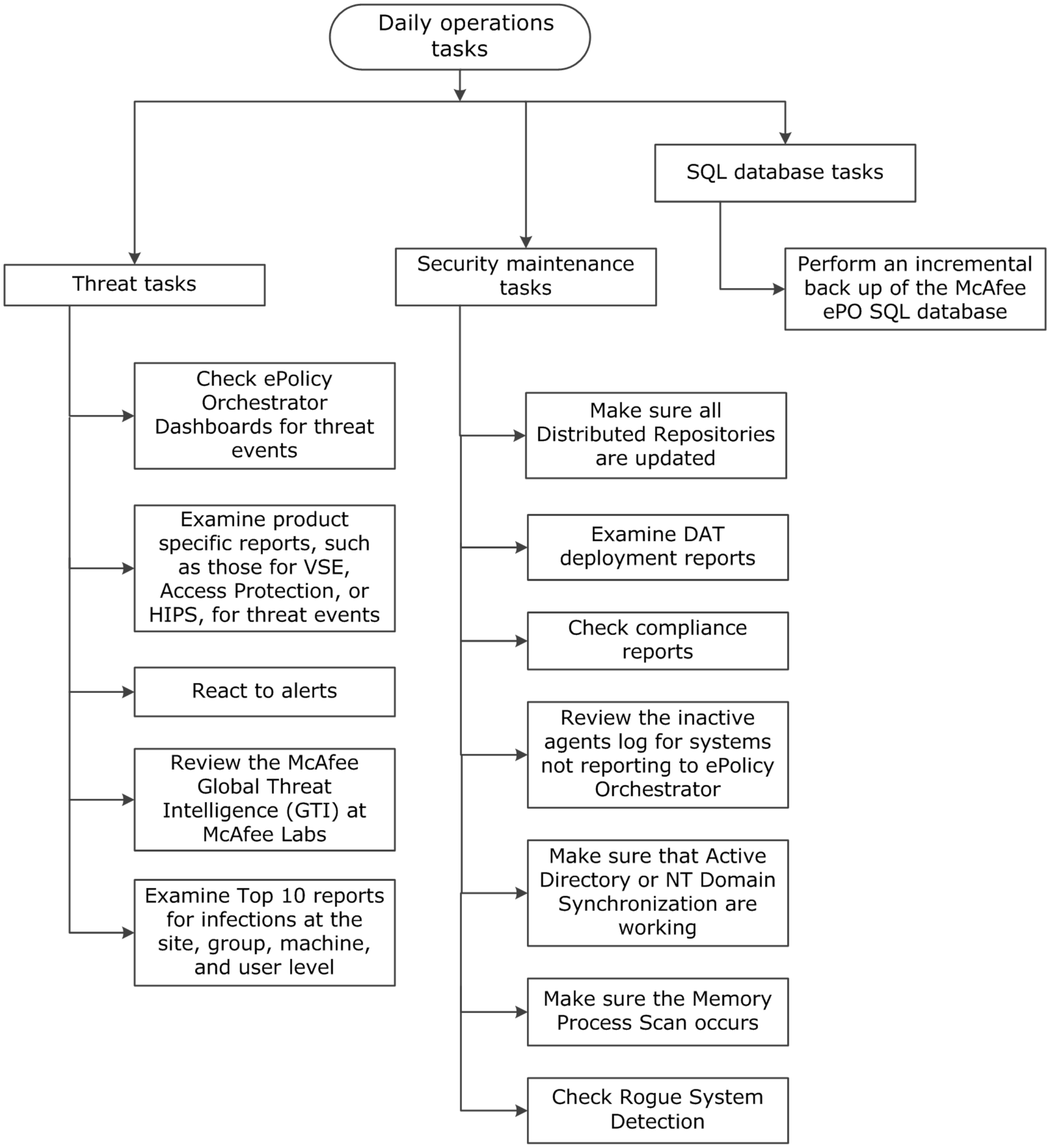

Daily operations tasks
Threat tasks
Security maintenance tasks
SQL database tasks
Perform an incremental back up of the McAfee ePO SQL database
Check ePolicy Orchestrator Dashboards for threat events
Examine product specific reports, such as those for VSE, Access Protection, or HIPS, for threat events
React to alerts
Review the McAfee Global Threat Intelligence (GTI) at McAfee Labs
Examine Top 10 reports for infections at the site, group, machine, and user level
Make sure all Distributed Repositories are updated
Examine DAT deployment reports
Check compliance reports
Review the inactive agents log for systems not reporting to ePolicy Orchestrator
Make sure that Active Directory or NT Domain Synchronization are working
Make sure the Memory Process Scan occurs
Check Rogue System Detection

**Figure 11-7 Suggested McAfee ePO daily tasks**

Each of the recommended daily tasks is described in more detail in the following table.

Where indicated, some of these tasks can be automated. Those instructions are included in this guide.

**Table 11-1 Recommended McAfee ePO daily tasks details**

| Task | Description |
|---|---|
| **Daily threat tasks** | |
| Periodically check McAfee ePO Dashboards for threat events. | Throughout the day, review your dashboards for threats, detections, and trends.<br>ⓘ Set up automated responses to send emails to administrators when threat activity thresholds are met. |
| Examine product-specific reports for threat events, such as VirusScan Enterprise or Host Intrusion Prevention. | Examine reports for any events that might indicate a new vulnerability in the environment. Schedule queries to run using a server task with the resulting report sent to select individuals. Using this data, you might create new policies or edit existing policies. |
| React to alerts. | If new alerts are found, follow your company's internal procedure for handling malware. Collect and send samples to McAfee and work toward cleaning up the environment. Ensure that signature files are updated and run on-demand scans as needed. See Troubleshooting procedure for finding possible infected files.<br>Run queries or review dashboards periodically to check for alerts collected from your managed devices. Also watch for these threat signs:<br>• High CPU usage on undetermined processes<br>• Unusually high increases in network traffic<br>• Services added or deleted by someone other than you<br>• Inability to access network or administrative shares<br>• Applications or files that stop functioning<br>• Unknown registry keys added to launch an application<br>• Any browser homepage that changed outside your control<br>• Examine the VSE: Trending Data Dashboard and look at the VSE: DAT Deployment information to determine whether your signature files are up-to-date. |
| Review the McAfee Global Threat Intelligence (GTI) at McAfee Labs Threat site at least once a day. | To access the McAfee Labs Threat site, select **Menu** \| **Reporting** \| **McAfee Labs**. |
| Examine Top 10 reports for infections at the site, group, system, and user level. | McAfee ePO provides preconfigured Top 10 reports that display statistics on infections in your environment. Determine which users, systems, and parts of the network have the most infections or vulnerability. These reports might reveal weaknesses in the network, where policies must be adjusted. |
| **Daily security maintenance tasks** | |
| Examine the DAT deployment reports. | It is important to have 100 percent deployment of the most recent DAT file to all managed systems. Make sure that clients have an update task configured to run multiple times a day to keep the DAT file current.<br>Run the VSE: DAT Adoption, VSE: DAT Adoption Over the Last 24 Hours, queries or the VSE: DAT Deployment query frequently throughout the day to ensure that systems are running the latest DATs. |

**Table 11-1 Recommended McAfee ePO daily tasks details** *(continued)*

| Task | Description |
|---|---|
| Check compliance queries and reports. | In Queries & Reports, find the compliance queries that identify systems that have not updated a managed product version with an engine, hotfix, or patch.<br>Create a process to make sure that systems are up to date. For example, run an update or deployment task to ensure compliance.<br>Out-of-compliance system numbers drop until all systems have checked in and updated their software. |
| Review the inactive agents log to determine that systems are reporting to McAfee ePO. | In Server Tasks, run the Inactive Agent Cleanup Task. This task identifies systems that have not connected to the McAfee ePO server for a specific number of days, weeks, or months. You can use this task to move inactive systems to a new group in the System Tree, tag the systems, delete the systems, or email a report.<br>If the systems are on the network but having difficulty checking into the McAfee ePO server, you might perform one of these actions:<br>• Use a **Ping Agent** or **Agent Wake-Up Call** to check if a system is online and able to perform an agent-server communication with the McAfee ePO server.<br>• Reinstall the McAfee Agent to ensure that the system is communicating with the McAfee ePO server. |
| Ensure that Active Directory or NT Synchronization is working. | Active Directory or NT Domain synchronization pulls in a list of new systems and containers that must be managed by McAfee ePO. If they are used, confirm that the Sync task can be configured to run at least once a day and is working.<br>If the synchronization fails, systems are vulnerable on the network and pose a major risk for infection. |
| Confirm that a Memory Process Scan occurs at least daily. | Using the Threats Dashboard, confirm that the results of these scans don't indicate an increase in threats.<br>Run memory process scans frequently, because they are quick and unobtrusive. |
| Check Rogue System Detection | Rogue System Detection tells you which devices are attached to the network. It reports unmanaged systems, so they can be quickly found and removed from the network. |
| **Daily SQL database tasks** | |
| Perform an incremental backup of the McAfee ePO database. | Use the Microsoft SQL Enterprise Manager to back up the McAfee ePO database. Verify that the back up was successful after it has completed.<br>You can use the McAfee ePO Disaster Recovery feature to create a snapshot of the records in the McAfee ePO database to quickly recover or reinstall your software, if needed.<br>See these documents for additional information:<br>• McAfee ePolicy Orchestrator Product Guide for Disaster Recovery details.<br>• How to back up and restore the ePO database using SQL Server Management Studio, KB52126<br>• McAfee ePO server backup and disaster recovery procedure, KB66616 |

**See also**

*Configure an Automatic Response for malware detection* on page 190
*Finding inactive systems* on page 178

## Recommended weekly tasks

Perform the McAfee suggested tasks at least once a week to ensure that your McAfee ePO server-managed network systems are safe from threats and your server is functioning normally.

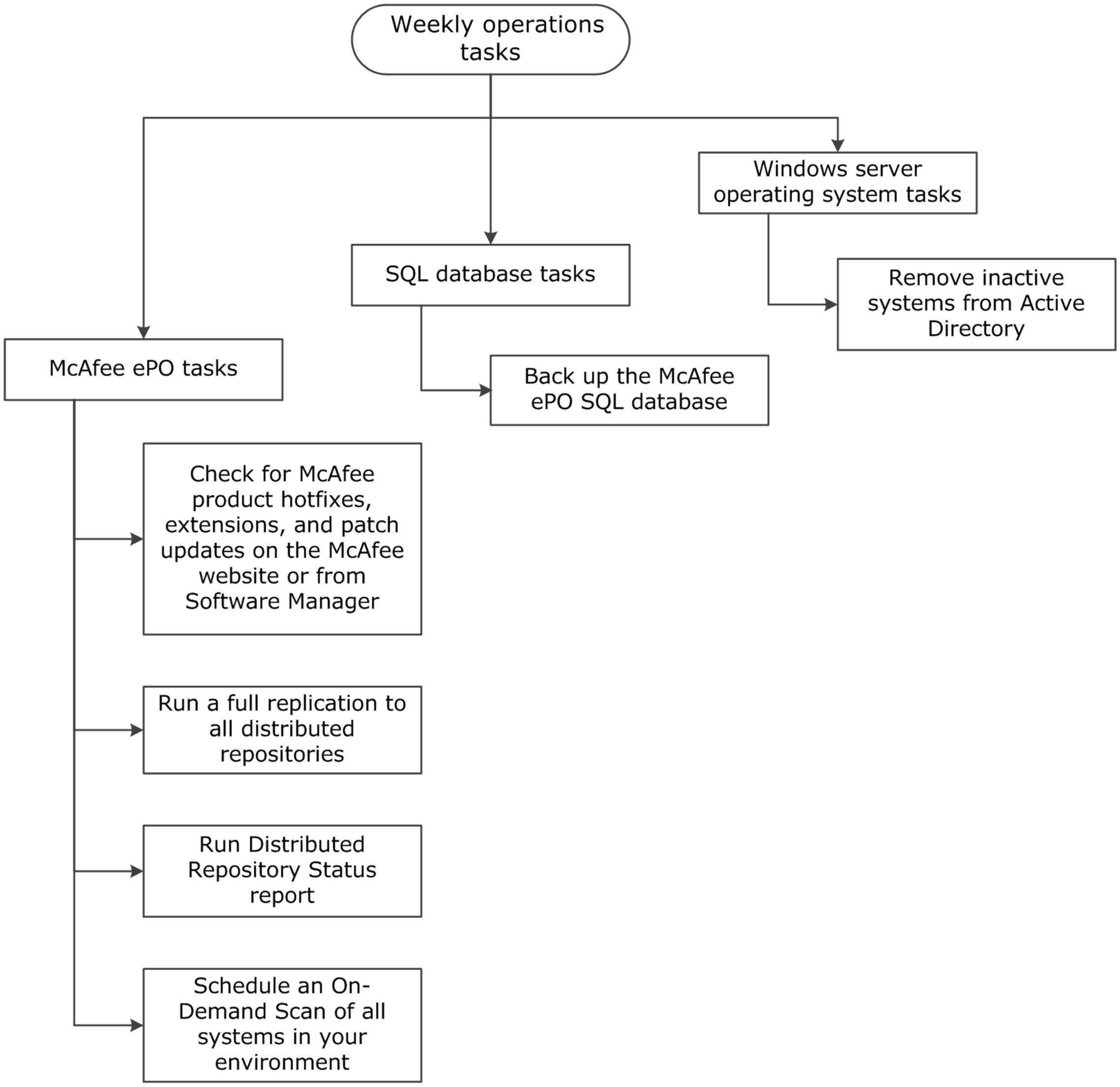

Weekly operations tasks
McAfee ePO tasks
SQL database tasks
Windows server operating system tasks
Remove inactive systems from Active Directory
Back up the McAfee ePO SQL database
Check for McAfee product hotfixes, extensions, and patch updates on the McAfee website or from Software Manager
Run a full replication to all distributed repositories
Run Distributed Repository Status report
Schedule an On-Demand Scan of all systems in your environment

**Figure 11-8 Suggested McAfee ePO weekly tasks**

Each of the recommended weekly tasks is described in more detail in the following table.

Where indicated, some of these tasks can be automated. Those instructions are included in this guide.

**Table 11-2 Recommended McAfee ePO weekly tasks details**

| Task | Description |
|---|---|
| **Weekly McAfee ePO tasks** | |
| Check for McAfee product hotfixes, extensions, and patch updates on the McAfee website or from the Software Manager. | McAfee periodically releases patches and hotfixes, as well as DATs and Engine updates. Check the McAfee website and McAfee ePO Software Manager frequently for new updates to check in to the McAfee ePO console for local environment testing. You can also use the Software Manager to download and check in these updates.<br>DAT and Engine files are not updated with the Software Manager.<br>See the McAfee ePolicy Orchestrator Product Guide for Software Manager details. |
| Run a full replication to all distributed repositories. | Distributed repositories can become corrupt because of an incomplete replication task. Remove corrupt files in the repositories by running a full replication to all distributed repositories once a week. Full replication tasks delete the existing repository contents and replace them with new files.<br>Incremental replication tasks only copy new or non-existent files and can't fix any corrupt files.<br>See the McAfee ePolicy Orchestrator Product Guide for replication details. |
| Run Distributed Repository Status. | Click **Menu** \| **Reports** \| **Reports and Queries**. Locate and Run the **Distributed Repository Status** report to determine whether there have been any failures to update distributed repositories. If there are failures, run the replication again and ensure that it does not fail again. |
| Schedule an On-Demand Scan of all systems in your environment. | Schedule an On-Demand Scan of all systems in your environment that runs during off-hours.<br>See these documents for additional information:<br>• Best Practices for On-Demand Scans in VirusScan Enterprise 8.8, KB74059<br>• Best Practices for On-Demand Scans in VirusScan Enterprise 8.8, TU30280 — Tutorial.<br>• VirusScan Enterprise 8.8 Product Guide for details about configuring On-Demand Scans<br>• How to create a McAfee ePO validation report for the event '1203, KB69428. |
| **Weekly SQL database tasks** | |
| Back up the McAfee ePO SQL database. | Use the Microsoft SQL Enterprise Manager to back up the McAfee ePO database. Verify that the back up was successful after it has completed.<br>You can use the McAfee ePO Disaster Recovery feature to create a snapshot of the records in the McAfee ePO database to quickly recover, or reinstall your software, if needed.<br>See these documents for additional information:<br>• McAfee ePolicy Orchestrator Product Guide for Disaster Recovery details.<br>• How to back up and restore the ePO database using SQL Server Management Studio, KB52126<br>• McAfee ePO server backup and disaster recovery procedure, KB66616 |

**Table 11-2 Recommended McAfee ePO weekly tasks details** *(continued)*

| Task | Description |
|---|---|
| **Weekly Windows Server operating system tasks** | |
| Remove inactive systems from Active Directory. | Active Directory pulls in a list of new systems and containers that must be managed by McAfee ePO. If it's used, confirm that the Sync task can be configured to run at least once a day and is working.<br>If the synchronization fails, systems are vulnerable on the network and pose a major risk for infection. |

**See also**

*Finding inactive systems* on page 178

## Recommended monthly tasks

Perform the McAfee suggested tasks at least once a month to ensure that your McAfee ePO server managed network systems are safe from threats and your server is functioning normally.

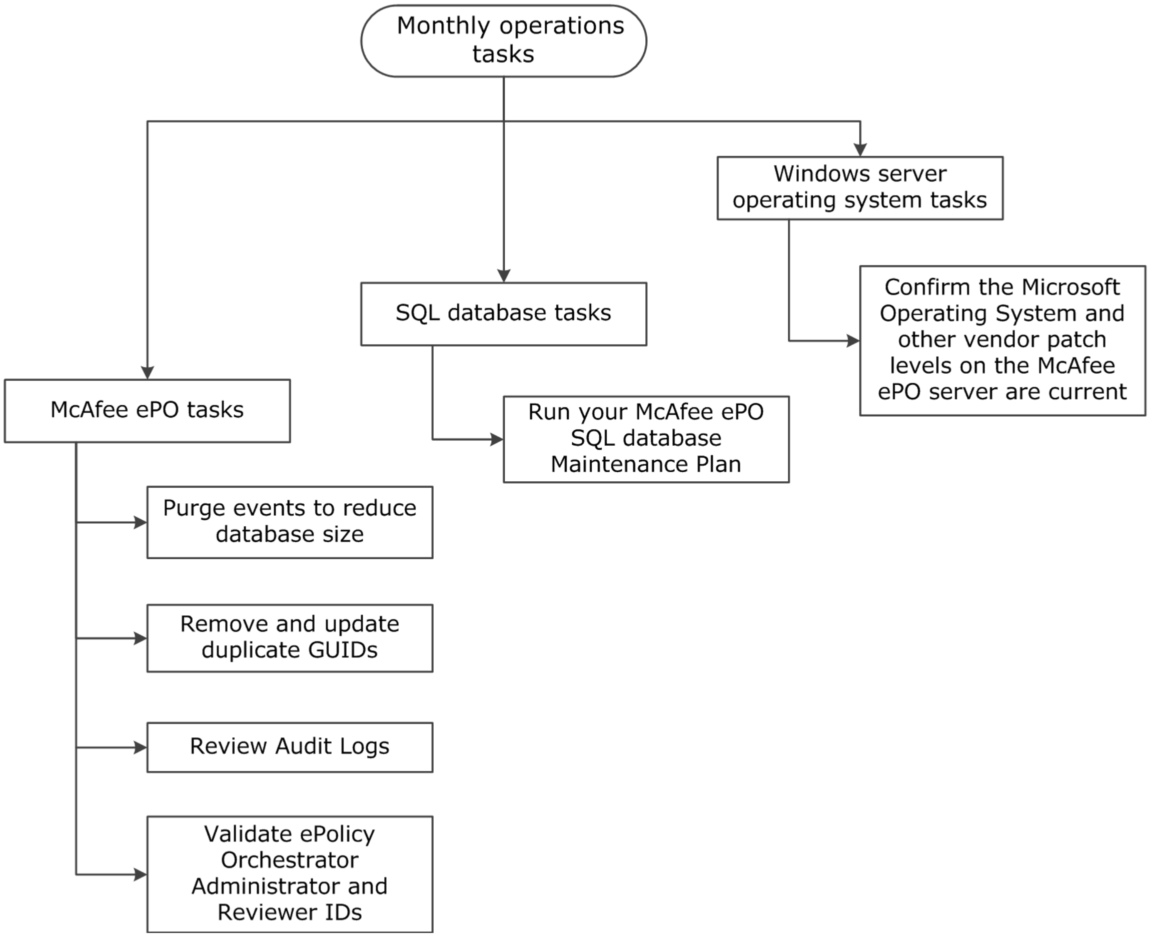

Monthly operations tasks
Windows server operating system tasks
Confirm the Microsoft Operating System and other vendor patch levels on the McAfee ePO server are current
SQL database tasks
Run your McAfee ePO SQL database Maintenance Plan
McAfee ePO tasks
Purge events to reduce database size
Remove and update duplicate GUIDs
Review Audit Logs
Validate ePolicy Orchestrator Administrator and Reviewer IDs

**Figure 11-9 Suggested McAfee ePO monthly tasks**

Each of the recommended monthly tasks is described in more detail in the following table.

Where indicated, some of these tasks can be automated. Those instructions are included in this guide.

**Table 11-3 Recommended McAfee ePO monthly tasks details**

| Task | Description |
|---|---|
| **Monthly McAfee ePO tasks** | |
| Purge events to reduce database size. | Purge events automatically. See Purging events automatically on page 170 and Purge events by query on page 171. |
| Remove and update duplicate GUIDs. | Run the Duplicate Agent GUID server tasks to find and fix any duplicate GUIDs in your environment. See Find systems with the same GUID on page 169.<br>Also, run these server tasks:<br>• **Duplicate Agent GUID - clear Error Count**<br>• **Duplicate Agent GUID - remove systems with potentially duplicated GUIDs** |
| Review Audit Logs. | Review the McAfee ePO Audit Logs to ensure that individuals with administrative privileges are making only approved changes to system configurations, tasks, and policies. See the McAfee ePolicy Orchestrator Product Guide for details. |
| Validate McAfee ePO Administrator and Reviewer IDs | Confirm that only employees authorized to have administrative access have properly configured IDs, with the proper permission sets in the McAfee ePO system. |
| **SQL database tasks** | |
| Run your McAfee ePO SQL database Maintenance Plan. | Set up and run your SQL Monthly Maintenance Plan. See Recommended maintenance plan for McAfee ePO database using SQL Server Management Studio for details. |
| **Monthly Windows Server operating system tasks** | |
| Confirm that the Microsoft Operating System and other vendor patch levels on the McAfee ePO server are current. | Review and implement all Microsoft patches to eliminate vulnerabilities and mitigate risk.<br>Other vendor patches might also be released and need updating to reduce vulnerabilities in the environment. |

**See also**

*Find systems with the same GUID* on page 169

## Periodic tasks

Performing periodic maintenance is important to ensure proper McAfee ePO server operations. Performing every task daily, weekly, or monthly, is not required. But periodic tasks are important to ensure overall site health, security, and disaster recovery plans are up to date.

> Create a periodic maintenance log to document dates that maintenance was conducted, by whom, and any maintenance-related comments about the task conducted.

| Task | Description |
|---|---|
| Assess your environment, policies, and policy assignments periodically to confirm that they are still applicable. | Organizational needs can change. Periodically review both existing policies and policy assignments to ensure that they still make sense in the environment. Fewer policies simplify server administration. |
| Review existing client tasks and task assignments periodically to confirm that they are still needed. | Client tasks run scans, deploy product updates, point products, product patches, and more to systems managed by McAfee ePO. Clean out unused tasks to reduce system complexity which can ultimately affect database size. |

| Task | Description |
|---|---|
| Review existing tags and tag criteria to ensure that they are still relevant to your environment. | Use tags as an alternative to System Tree groups to combine, or select a group of systems to operate upon. For example, to send updates, deploy point products, or run scans. Tagging is useful, but you must monitor tags to ensure that they are useful and have the impact needed. |
| Review product exclusions (for example, VirusScan Enterprise) and includes/excludes (for example, Access Protection rules) periodically to validate relevancy. | You must keep exclusions as specific as possible in your environment.<br>Products changes can affect the exclusions that you have configured. Periodically review exclusions to ensure that they still accomplish what is needed. Plus, you can use High and Low Risk OnAccess scanning configurations to augment exclusions.<br>Structure the System Tree, or use tags as another method to control exclusions. |
| Make any hardware changes or remove any repositories that you want to decommission. | As your network and organization changes, you might find that modifying the location and type of repositories you use provides more efficient and effective coverage. |
| Validate that you have the required software, such as the latest version of the McAfee Agent. | Always use the most current version of point products to ensure that you have technical support for those products. Plus, you have the latest features and fixes available. |
| Remove any unsupported software or software for products you aren't using from the master and distributed repositories. | Keeping disk space to a minimum and removes clutter from the McAfee ePO server and distributed repositories. Only keep those products currently in use in your environment in the Master Repository. |
| Validate your System Tree and remove any agents that have not communicated with the McAfee ePO server in 30 days or that are de-commissioned. | Keep the System Tree organized and delete systems that are no longer in use, or reporting to McAfee ePO. A clean System Tree ensures that reports do not contain extraneous information. Set up a server task to delete inactive systems. |
| Remove server tasks that are no longer used. | Keeping only those server tasks that you intend to use in the task listing. You can always disable an unused task that you want to keep, but don't use regularly. Keeping a minimum list of tasks that you use regularly reduces McAfee ePO complexity. |
| Remove Automated Responses that are no longer relevant. | Automated responses are configured to alert individuals, particularly system administrators when malware event threats, client treats, or compliance issues need to be resolved. |
| Delete shell systems using a McAfee ePO server task. | Delete systems with incomplete or missing system and product properties from the **System Tree**. Those systems skew reports and queries, and waste space in the McAfee ePO database. |

12

# Bandwidth usage

The McAfee ePO server uses your LAN and WAN bandwidth to receive events from your managed clients and download software to your managed clients. It's important to understand these requirements to configure your McAfee ePO server to use the bandwidth efficiently.

### Contents

## Agent deployment and bandwidth

When installing a McAfee ePO server in your environment, you must distribute agents, components, and security products to manage and protect the systems on the network.

During the initial setup of your managed environment, deploying the McAfee Agent generates enough network traffic that we recommend planning the deployment. Although the installation package for the McAfee Agent is smaller than other products (such as VirusScan Enterprise), the agent must be deployed to each client system that you want to manage.

McAfee Agent deployment traffic occurs directly between the McAfee ePO server and the client systems where the agent is deployed.

This table shows the total bandwidth used on an McAfee Agent server, client system, and McAfee Agent SQL database server for McAfee Agent 4.8 deployment.

**Table 12-1 McAfee Agent bandwidth usage**

| Agent deployment | Total (MB) | Transmit (MB) | Receive (MB) |
|---|---|---|---|
| McAfee ePO server | 5.04 | 4.83 | 0.21 |
| SQL database server | 4.64 | 0.04 | 4.60 |
| Client system | 0.42 | 0.18 | 0.24 |

### Actual deployment

The first and most extensive use of bandwidth occurs when the McAfee Agent installation package is deployed to client systems. You can deploy the McAfee Agent installation package from the McAfee ePO server console to sites, groups, or selected systems in the System Tree. Regardless of the method you use, deploying the agent installation package over the network generates traffic to each system.

How you deploy the McAfee Agent depends on three variables.

- The number of client systems to manage
- Their location in the network topology
- The bandwidth available between the McAfee ePO server and those systems

McAfee recommends deploying agents:

- **In stages** — Do not push network utilization over 80% at any time for a given segment of resources.
- **To individual sites or groups** — This is important if you have more bandwidth-limiting factors such as slower connections between geographic locations.

## Calculating client updates bandwidth

New product updates use additional bandwidth. Calculate the requirements before you update your products.

You can calculate the bandwidth if you know the size of the patch or product being downloaded. To find the exact size of the product installation files in Windows Explorer, right-click the Install folder and click Properties. The product files are at this default path:

```
C:\Program Files(X86)\McAfee\ePolicy Orchestrator\DB\Software\Current\<ProductName>
\Install\
```

At a minimum, each of your clients must download, on average, 400 KB a day for DAT files. The following examples show how to calculate the bandwidth used for the client updates using this formula:

**(*Size of update file*) x (*Number of nodes*) = Amount of data pulled a day**

The following examples use this formula to calculate the amount of data pulled a day and describe if creating a local repository reduces the bandwidth.

### Example 1 — A small office in India

The small office in India must download the 400 KB a day for DAT files to its 200 nodes. Using the formula:

**(400 KB) x (200 nodes) = approximately 80 MB of data randomly pulled a day to India**

In the small office in India, you can add a repository, but you must replicate the DAT file from the McAfee ePO server to the repository. This file replication uses approximately 70 MB of bandwidth a day over a slow WAN link that can negatively affect the WAN link to India because it occurs all at once.

Instead, have the agents connect across the WAN link to the next closest repository to download their DAT file updates. The next repository might be in a larger office, for example Tokyo. The agents can randomly pull their DAT files throughout the day, and their total bandwidth use is only 80 MB.

In this case, do not use a repository in India.

### Example 2 — A large office in Tokyo

The large office in Tokyo must download 400 KB a day for DAT files to its 4,000 nodes. Use the formula:

**(400 KB) x (4,000 nodes) = approximately 1.6 GB of data randomly pulled a day to Tokyo**

In the large office in Tokyo with 4,000 nodes uses 1.6 GB of bandwidth a day just to update the DAT files alone. Because replication of the DAT file to Tokyo only uses 70 MB of bandwidth a day, it is much more efficient to have a repository in the Tokyo office. Now all DATs are pulled across the LAN instead of across the slower WAN link.

### Example 3 — A large office in New York City

The large office in New York City must download a 23-MB patch update for VirusScan Enterprise to its 1,000 nodes. Use the formula:

**(23 MB) x (1,000 nodes) = approximately 23 GB of data pulled to the New York City office**

This 23-MB patch is significantly larger than the 400 KB daily DAT files. You probably have a repository in New York depending on the speed of the WAN link to New York and how quickly the patch must be pushed out. You might find a balance if you carefully craft your client tasks to pull updates and patches at a gradual pace instead of deploying the patch to all nodes in one day.

### Conclusions

Some McAfee ePO users put a repository at geographic sites that have only a few dozen nodes. If your site does not have at least 200–300 nodes, it cannot benefit from the bandwidth saved using a repository. If there is no local repository, the agents go to the next nearest repository for their updates. This repository might be connecting to the server across a WAN link, but it still uses less bandwidth because you don’t have to replicate the entire repository across the WAN.

The exception to this rule is if you are deploying a larger software package. For example, the VirusScan Enterprise client software is 56 MB. In this case, it is more efficient to place a repository temporarily at a smaller site so that the client's software can download the 56-MB file locally. Then disable this repository once the client is rolled out.

**See also**

*How client tasks deploy products* on page 55
*Product deployment workflows* on page 56

## Bandwidth required to deploy managed products

Deploying security products, such as VirusScan Enterprise, to client systems is the most bandwidth-intensive part of setting up a managed environment. Like the McAfee Agent, security software must be installed on each system you plan to manage.

This table shows the total bandwidth (in megabytes) used to deploy specific managed products, as well as the data transmitted and received by the McAfee ePO server, a client system, and the database server.

**Table 12-2 McAfee product deployment**

| Product deploym | McAfee ePO server | | | SQL Server | | | Client system | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Total (MB) | Tx (MB) | Rx (MB) | Total (MB) | Tx (MB) | Rx (MB) | Total (MB) | Tx (MB) | Rx (MB) | Disk space (MB) |
| Agent 4.8.0 | 5.04 | 4.83 | 0.21 | 0.42 | 0.18 | 0.24 | 4.64 | 0.04 | 4.60 | 33.90 |
| Endpoint Encryption for Files and Folders 4.2.0 | 9.91 | 5.21 | 4.70 | 6.14 | 4.61 | 1.53 | 3.77 | 0.09 | 3.67 | 22.92 |
| Endpoint Encryption for PC 7.1.0 | 174.79 | 17.04 | 0.44 | 0.50 | 0.29 | 0.22 | 16.98 | 0.15 | 16.83 | 11.29 |
| Host Data Loss Prevention 9.3.0 | 31.47 | 16.85 | 14.62 | 18.75 | 14.38 | 4.38 | 12.71 | 0.24 | 12.47 | 126.78 |
| Host Intrusion Prevention 8.0.0 Patch 4 | 13.67 | 13.29 | 0.38 | 0.57 | 0.25 | 0.32 | 13.10 | 0.13 | 12.97 | 43.02 |
| MOVE-AV 3.0 | 8.88 | 8.54 | 0.34 | 0.63 | 0.27 | 0.36 | 8.25 | 0.07 | 8.18 | 6.00 |
| Security for Microsoft SharePoint 2.5.0 | 191.04 | 155.07 | 35.98 | 45.58 | 34.39 | 11.19 | 145.47 | 1.59 | 143.88 | 610.94 |
| Policy Auditor 6.2 | 24.41 | 23.82 | 0.60 | 0.94 | 0.39 | 0.55 | 23.47 | 0.21 | 23.26 | 46.31 |
| Rogue System Detection 4.7.1 | 5.74 | 5.53 | 0.21 | 0.31 | 0.15 | 0.16 | 5.44 | 0.06 | 5.37 | 5.46 |
| Site Advisor Enterprise 3.5.0 | 5.25 | 5.01 | 0.23 | 0.75 | 0.47 | 0.06 | 4.78 | 0.05 | 4.73 | 15.43 |
| VirusScan Enterprise 8.8.0 Patch 4 | 97.19 | 95.48 | 1.72 | 2.52 | 1.01 | 1.51 | 94.67 | 0.71 | 93.96 | 320.55 |

# Bandwidth recommendations for repository distribution

If the McAfee ePO server is managing systems across a Wide Area Network (WAN), we recommend that you create at least one distributed repository per Local Area Network (LAN) for client updates.

You must configure when these actions occur, after you install the distributed repository.

- When the repositories are updated from the McAfee ePO server Master Repository.
- When the managed systems pull the updates from the distributed repository.

These tasks need randomization intervals configured to avoid network bandwidth saturation.

## Number of repositories needed per LAN

This table lists the suggested number of repositories needed depending on the systems in the LAN and the network bandwidth.

**Table 12-3 Number of distributed repositories**

| Systems in LAN | Network bandwidth (LAN) | |
|---|---|---|
| | 100 Mbps | 1 Gbps |
| 1,000 | 1 repository | 1 repository |
| 2,000 | 2 repositories | 1 repository |
| 3,000 | 3 repositories | 1 repository |
| 4,000 | 4 repositories | 1 repository |
| 5,000 | 5 repositories | 1 repository |
| 10,000 | 10 repositories | 2 repositories |
| 20,000 | 20 repositories | 2 repositories |
| 30,000 | 30 repositories | 3 repositories |

## Repository replication randomization interval setting by WAN bandwidth

You must consider WAN bandwidth before you set a randomization interval to automate repository replication.

Use these steps in this information to automate repository replication in your network.

1 Create an incremental replication task for each distributed repository in each LAN.

2 According to WAN bandwidth in Mbps, set each task to run sequentially at the minimum of the minutes of the corresponding randomization interval, to avoid overlap.

**Table 12-4 McAfee ePO server randomization interval setting (minutes)**

| WAN bandwidth Mbps | Randomization interval (minutes) |
|---|---|
| 6 Mbps | 1 |
| 5 Mbps | 2 |
| 4 Mbps | 3 |
| 3 Mbps | 4 |
| 2 Mbps | 5 |
| 1 Mbps | 6 |

See the McAfee ePolicy Orchestrator Product Guide configuration details for global updates.

## Randomization interval for client update task

The client update task you create ensures that systems are current with the latest DAT and engine files. This task requires a randomization interval, which is determined by these variables:

- Network bandwidth
- Systems in the LAN
- Distributed repositories in LAN

To create the client update task, see the McAfee ePolicy Orchestrator Product Guide and perform these steps.

1. Add the local distributed repository to the repository list in the agent policy.

2. Select the closest repository using **Ping Time**.

3. Create an agent update task with a randomization interval set according to these tables.

**Table 12-5 Recommended interval (minutes) for network bandwidth of 1 Gbps**

| Systems in LAN | Distributed repositories in LAN | | |
|---|---|---|---|
| | 1 | 2 | 3 |
| | Recommended randomization interval (minutes) | | |
| 1,000 | 5 | 0 | 0 |
| 2,000 | 10 | 5 | 0 |
| 3,000 | 15 | 10 | 0 |
| 4,000 | 20 | 15 | 5 |
| 5,000 | 30 | 20 | 10 |
| 10,000 | 60 | 40 | 20 |
| 20,000 | 120 | 80 | 40 |
| 30,000 | 180 | 120 | 60 |

**Table 12-6 Recommended interval (minutes) for network bandwidth of 100 Mbps**

| Systems in LAN | Distributed repositories in LAN | | | | |
|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 |
| | Recommended randomization interval (minutes) | | | | |
| 1,000 | 60 | 30 | 20 | 15 | 10 |
| 2,000 | 120 | 60 | 40 | 30 | 20 |
| 3,000 | 180 | 90 | 60 | 45 | 30 |
| 4,000 | 240 | 120 | 80 | 60 | 40 |
| 5,000 | 300 | 150 | 100 | 75 | 50 |

## Calculating bandwidth for repository replication and product updates

Repository replication consumes valuable bandwidth in all environments. Before you install repositories, calculate the bandwidth required for their replication.

If your enterprise network has geographically diverse networks and WAN network connection speeds that vary, you must calculate the update bandwidth needed from your McAfee ePO server to your managed systems. There are two system update requirements.

- Relatively small, daily, DAT file updates
- Large, infrequent, product software updates

### Calculating DAT file bandwidth usage

If you are replicating only DAT files, the bandwidth used is approximately 70 MB of replication per day. Agents don't use all DAT files that are copied to the repository, but there are 35 incremental DAT files that must be available to all agents in case they are behind on DATs. When determining if you need a repository in a specific location, determine what is more costly in terms of bandwidth usage. You can replicate 70 MB worth of data to a repository, or tell the agents to go to the next nearest repository that might not be located near the agents.

The following example uses updating the DAT files for VirusScan Enterprise, that are released daily. The numbers used to determine if a repository is needed at a site are:

- **400 KB** — The average size of the daily DAT file to download
- **100** — The number of system agents that must download those daily DAT files

**Example 1: Downloading directly from the central McAfee ePO server**

To download the daily DAT file randomly from the central McAfee ePO server to the system agents takes the following bandwidth: 100 agents * 400 KB file = **40 MB of bandwidth approximately**

**Example 2: Downloading the DAT file to the local repository**

For the McAfee ePO server to replicate the DAT file to each repository every day takes at least **70 MB of bandwidth**.

In the previous examples, it is a waste to use 70 MB of bandwidth to download a DAT file to a repository for only 100 system agents. Those 100 system agents can download the same file using only 40 MB of bandwidth.

## Calculating product update bandwidth usage

Always calculate how much bandwidth the deployment needs by taking the size of the deployment package, multiplied by the number of nodes targeted, divided by the number of repositories used. For example, VirusScan Enterprise 8.8, which is 56 MB, deployed to 1,000 nodes, pulled across three repositories, equals about 56 GB of data. That 56 GB of data is being pulled across three repositories which equal about 19 GB per repository.

> Randomization is critical to any client task that uses bandwidth. See Scheduling product deployment with randomization on page 56 to confirm that randomization is enabled.

**56 MB (VSE) * 1,000 (nodes) = 56 GB (total) / 3 (repositories) = approximately 19 GB per repository**

The following formula calculates the bandwidth to move the 19 GB of data per repository randomly over a 9-hour workday. The total equals about 2.1 GB of data per hour pulled from each repository.

**19 GB (per repository) / 9 (hours) = approximately 2.1 GB per hour**

13

# Automating and optimizing McAfee ePO workflow

You can create queries and tasks to automatically run for improved server performance, easier maintenance, and to monitor threats.

> Whenever you change a policy, configuration, client or server task, automatic response, or report, export the settings before and after the change. For detailed instructions about exporting objects, see the McAfee ePolicy Orchestrator Product Guide.

### Contents

## Find systems with the same GUID

You can use preconfigured server tasks that runs queries and targets systems that might have the same GUIDs.

This task tells the agent to regenerate the GUID and fix the problem. See the McAfee ePolicy Orchestrator Product Guide for details.

### Task

For option definitions, click **?** in the interface.

1. Click **Menu** | **Automation** | **Server Tasks** to open the Server Tasks Builder.
2. Click **Edit** in the Actions column for one of the following preconfigured server tasks.
   - **Duplicate Agent GUID - Clear error count**
   - **Duplicate Agent GUID - Remove systems that potentially use the same GUID**
3. On the Description page, select **Enabled**, then click:
   - **Save** — Enable the server task and run it from the Server Task page.
   - **Next** — Schedule the server task to run at a specific time and perform the task.

This clears the error count and removes any systems with the same GUID, and assigns the systems a new GUID.

# Purging events automatically

Periodically purge the events that are sent daily to your McAfee ePO server. These events can eventually reduce performance of the McAfee ePO server and SQL Servers.

Events can be anything from a threat being detected, to an update completing successfully. In environments with a few hundred nodes, you can purge these events on a nightly basis. But in environments with thousands of nodes reporting to your McAfee ePO server, it is critical to delete these events as they become old. In these large environments, your database size directly impacts the performance of your McAfee ePO server, and you must have a clean database.

You must determine your event data retention rate. The retention rate can be from one month to an entire year. The retention rate for most organizations is about six months. For example, six months after your events occur, on schedule, they are deleted from your database.

> McAfee ePO does not come with a preconfigured server task to purge task events. This means that many users never create a task to purge these events and, over time, the McAfee ePO server SQL database starts growing exponentially and is never cleaned.

**See also**
*Reporting features* on page 63

## Create a purge events server task

Create an automated server task to delete all events in the database that are older and no longer needed.

> Some organizations have specific event retention policies or reporting requirements. Make sure that your purge event settings conform to those policies.

### Task

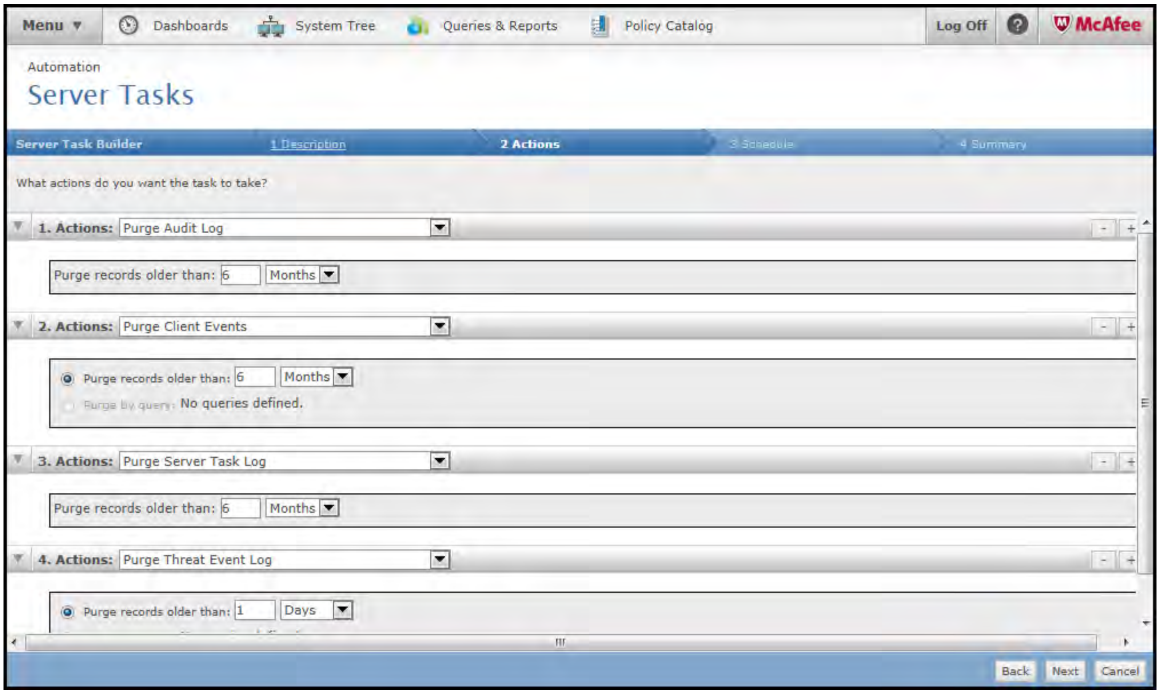
For option definitions, click **?** in the interface.

1. To open the Server Task Builder dialog box, click **Menu** | **Automation** | **Server Tasks**, then click **Actions** | **New Task**.
2. Type a name for the task, for example `Delete client events`, add a description, then click **Next**.

3 On the Actions tab, configure these actions from the list:

- **Purge Audit Log** — Purge after 6 months.
- **Purge Client Events** — Purge after 6 months.
- **Purge Server Task Log** — Purge after 6 months.
- **Purge Threat Event Log** — Purge every day.
- **Purge SiteAdvisor Enterprise Events** — Purge after 10 days.

  This is an example of the Actions list configuration.



Automation

Server Tasks

Server Task Builder — 1 Description — 2 Actions — 3 Schedule — 4 Summary

What actions do you want the task to take?

1. Actions: Purge Audit Log
Purge records older than: 6 Months

2. Actions: Purge Client Events
● Purge records older than: 6 Months
○ Purge by query: No queries defined.

3. Actions: Purge Server Task Log
Purge records older than: 6 Months

4. Actions: Purge Threat Event Log
● Purge records older than: 1 Days

**Figure 13-1 Server Task Builder with multiple Actions configured**

You can chain the actions all in one task so that you don't have to create multiple tasks.

This example purges SiteAdvisor Enterprise events because they are not included in the normal events table and require their own purge task. The SiteAdvisor Enterprise events are retained for only 10 days because they collect all URLs visited by managed systems. These events can save a large amount of data in environments with more than 10,000 systems. Therefore, this data is saved for a much shorter time compared to other event types.

4 Click **Next** and schedule the task to run every day during non-business hours.

5 Click the **Summary** tab, confirm that the server task settings are correct, then click **Save**.

## Purge events by query

You can use a custom configured query as a base to delete client events.

**Before you begin**

You must have created a query to find the events you want purged before you start this task.

There are reasons why you might need to purge data or events based on a query. For example, there can be many specific events overwhelming your database. In this example, you might not want to wait for the event to age out if you are keeping your events for six months. Instead you want that specific event deleted immediately or nightly.

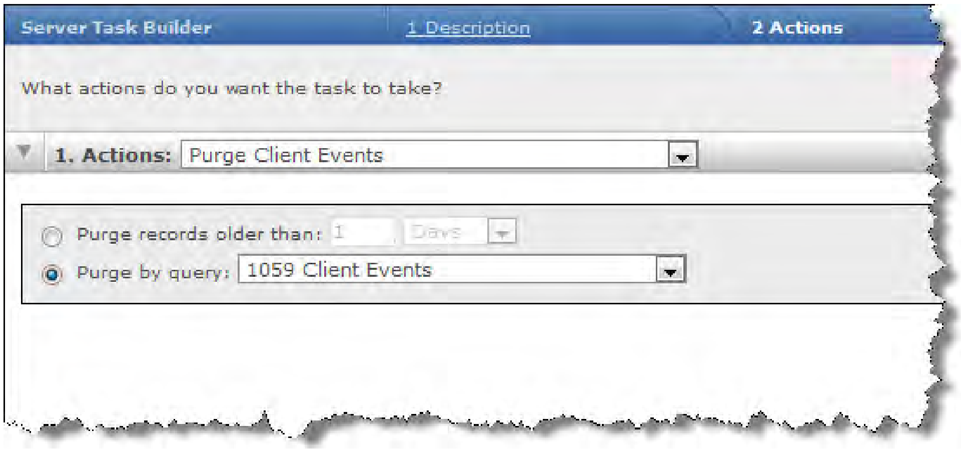
Purging these events can significantly improve the performance of your McAfee ePO server and database.

Configure purging data based on the results of a query.

### Task

For option definitions, click **?** in the interface.

1. Click **Menu** | **Automation** | **Server Tasks**, then click **Action** | **New Task** to open the Server Task Builder.
2. Type a name for the task, for example `Delete 1059 client events`, then on the Actions tab, click **Purge Client Events** from the Actions list.
3. Click **Purge by Query**, then select the custom query that you created.



What actions do you want the task to take?

1. Actions: Purge Client Events

○ Purge records older than: 1 Days
● Purge by query: 1059 Client Events

**Figure 13-2 Server Task Builder with Purge Client Events action configured**

This menu is automatically populated when table queries are created for client events.

4. Schedule the task to run every day during non-business hours, then click **Save**.

**See also**

*Create custom event queries* on page 65
*Create custom table queries* on page 76

## Creating an automatic content pull and replication

Pulling content daily from the public McAfee servers is a primary functions of your McAfee ePO server. Regularly pulling content keeps your protection signatures up to date for McAfee products.

Pulling the latest DAT and content files keeps your protection signatures up to date for McAfee products like VirusScan Enterprise and Host Intrusion Prevention.

The primary steps are:

1 Pull content from McAfee into your Master Repository, which is always the McAfee ePO server.

2 Replicate that content to your distributed repositories. This ensures that multiple copies of the content are available and remain synchronized. This also allows clients to update their content from their nearest repository.

The most important content are the DAT files for VirusScan Enterprise, released daily at approximately 11 a.m. Eastern Time.

Optionally, many users with larger environments choose to test their DAT files in their environment before deployment to all their systems.

**See also**
*Automating DAT file testing* on page 183

## Pull content automatically

Pull the McAfee content from the public McAfee servers. This pull task keeps your protection signatures up to date.

You must schedule your pull tasks to run at least once a day after 11 a.m. Eastern Time. In the following example, the pull is scheduled for twice daily, and if there is a network problem at 2 p.m., the task occurs again at 3 p.m. Some users like to pull their updates more frequently, as often as every 15 minutes. Pulling DATs this often is aggressive and unnecessary because DAT files are typically released only once a day. Pulling two or three times a day is adequate.

Testing your DAT files before deployment requires a predictable pull schedule.

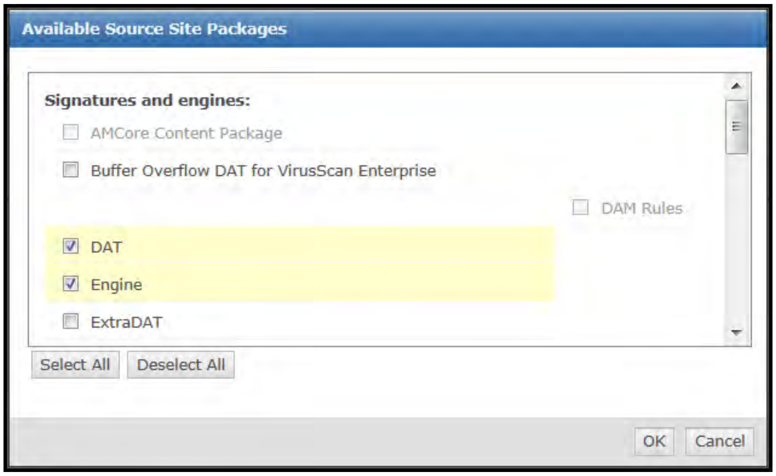
### Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Automation** | **Server Tasks**, then click **Actions** | **New task**.

2 In the Server Task Builder dialog box, type a task name and click **Next**.

3 In the Actions dialog box, from the Actions list, select **Repository Pull**, then click **Selected packages**.


Available Source Site Packages

Signatures and engines:

☐ AMCore Content Package

☐ Buffer Overflow DAT for VirusScan Enterprise

☐ DAM Rules

☑ DAT

☑ Engine

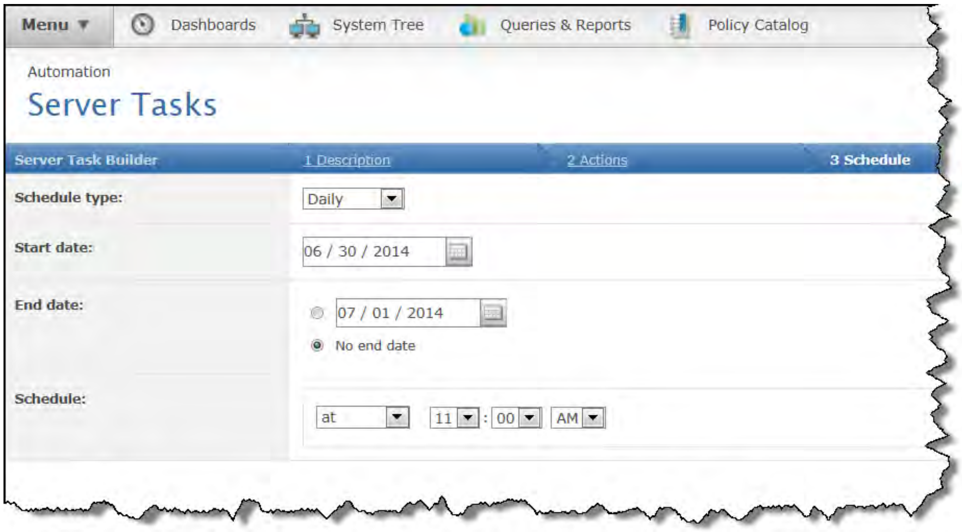
☐ ExtraDAT

Figure 13-3 Available Server Task Builder dialog box with packages selected

When you create a pull task for content, select only the packages that apply to your environment instead of selecting **All packages**. This keeps the size of your Master Repository as small as possible. This selection also reduces the bandwidth used during the pull from the McAfee website and, more importantly, reduces bandwidth used during replication to your distributed repositories.

4 Click **Next**.

5 Schedule your pull task to run at least once a day after 11 a.m. Eastern Time, then click **Next**.



Schedule type: Daily

Start date: 06 / 30 / 2014

End date: ○ 07 / 01 / 2014 ● No end date

Schedule: at 11 : 00 AM

**Figure 13-4 Server Task Builder Schedule configured**

6 Click the **Summary** tab, confirm that the server task settings are correct, then click **Save**.

Now you have created a server task that automatically pulls the McAfee DAT files and content from the public McAfee servers.

**See also**
*Automating DAT file testing* on page 183

# Filtering 1051 and 1059 events

1051 and 1059 events can make up 80 percent of the events stored in your database. If enabled, make sure that you periodically purge these events.

If you have not looked at Event Filtering on your McAfee ePO server in a long time, run the custom **Event Summary Query** and check the output.

The two most common events seen in customer environments are:

- 1051 — Unable to scan password-protected file
- 1059 — Scan timed out

These two events can be enabled on the McAfee ePO server. If you never disabled them, you might find a significant number of these events when you run the **Event Summary Query**. These two events can, for some users, make up 80 percent of the events in the database, use a tremendous amount of space, and impact the performance of the database.

> The 1059 events indicate that a file was not scanned, but the user was given access. Disabling the 1059 event means that you lose visibility of a security risk.

So why are these events in there? These events have historic significance and go back several years and are meant to tell you that a file was not scanned by VirusScan Enterprise. This failure to scan the file might be due to one of two reasons:

- The scan timed out due to the size of the file, which is a 1059 event.
- It was inaccessible due to password protection or encryption on the file, which is a 1051 event.

Disable these two events under event filtering, to prevent a flood of these events into your database. By disabling these events, you are effectively telling the agent to stop sending these events to McAfee ePO.

> VirusScan Enterprise still logs these events in the On-access scanner log file for reference on the local client.

Optionally, you can disable additional events, but this is not typically necessary because most of the other events are important and are generated in manageable numbers. You can also enable additional events, as long as you monitor your event summary query to make sure that the new event you enabled does not overwhelm your database.

**See also**
*How event summary queries work* on page 70

## Filter 1051 and 1059 events

Disable the 1051 and 1059 events if you find a significant number of them when you run the Event Summary Query.

### Task

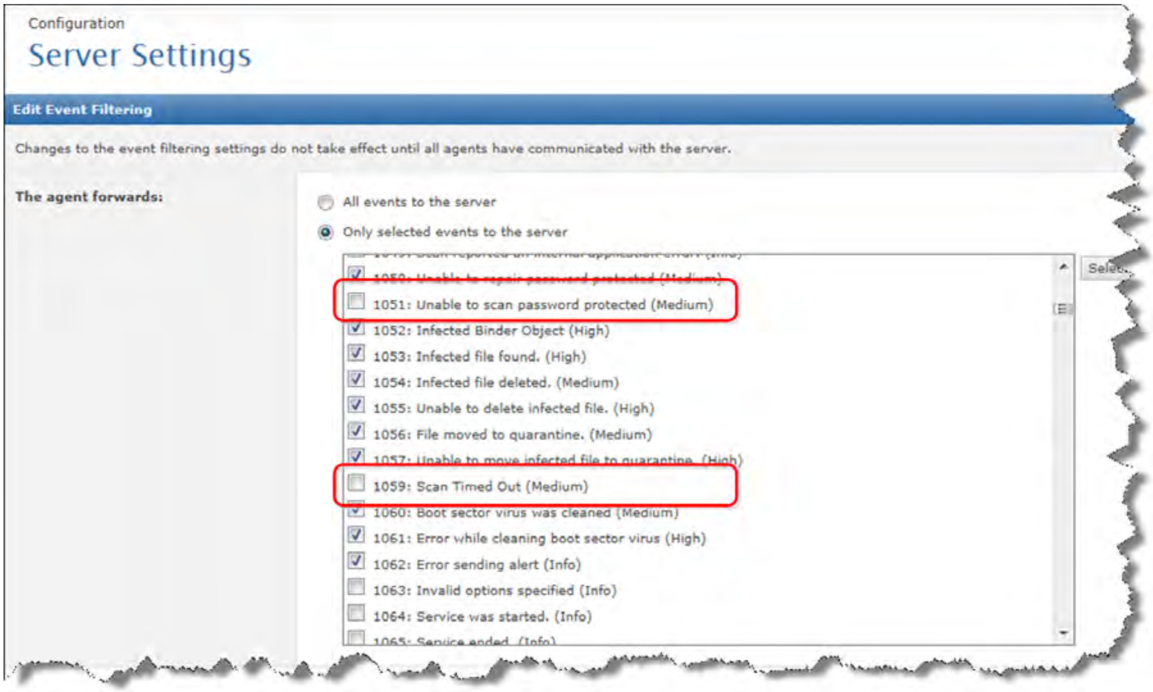
For option definitions, click **?** in the interface.

1 Click **Menu** | **Configuration** | **Server Settings**, in the Setting Categories list select **Event Filtering**, then click **Edit**.

2 In **The agents forwards** list on the Edit Event Filtering page, scroll down until you see these events, then deselect them:

- **1051: Unable to scan password protected (Medium)**
- **1059: Scan Timed Out (Medium)**

  This figure shows the 1051 and 1059 events deselected on the **Server Settings** page.



Configuration

Server Settings

Edit Event Filtering

Changes to the event filtering settings do not take effect until all agents have communicated with the server.

The agent forwards:

○ All events to the server

● Only selected events to the server

☑ 1050: Unable to repair password protected (Medium)
□ 1051: Unable to scan password protected (Medium)
☑ 1052: Infected Binder Object (High)
☑ 1053: Infected file found. (High)
☑ 1054: Infected file deleted. (Medium)
☑ 1055: Unable to delete infected file. (High)
☑ 1056: File moved to quarantine. (Medium)
☑ 1057: Unable to move infected file to quarantine. (High)
□ 1059: Scan Timed Out (Medium)
☑ 1060: Boot sector virus was cleaned (Medium)
☑ 1061: Error while cleaning boot sector virus (High)
☑ 1062: Error sending alert (Info)
□ 1063: Invalid options specified (Info)
□ 1064: Service was started. (Info)
□ 1065: Service ended. (Info)

**Figure 13-5 1051 and 1059 events deselected**

3 Click **Save**.

Now these two events are no longer saved to the McAfee ePO server database when they are forwarded from the agents.

# Finding systems that need a new agent

If you suspect some of your managed systems might not have the same McAfee Agent installed, perform these tasks to find the systems with the older agent versions, then select those systems for a McAfee Agent upgrade.

## Create a new Agent Version Summary query

Find systems with old McAfee Agent versions using a query to generate a list of all agent versions that are older than the current version.

### Task

For option definitions, click **?** in the interface.

1. To duplicate the Agent Versions Summary query, click **Menu** | **Reporting** | **Queries & Reports**, then find the **Agent Versions Summary** query in the list.
2. In the Actions column of the Agent Versions Summary query, click **Duplicate**. In the Duplicate dialog box, change the name, select a group to receive the copy of the query, then click **OK**.
3. Navigate to the duplicate query that you created, then click **Edit** in the Actions column to display the preconfigured Query Builder.
4. In the Chart tab, in the **Display Results As** list, expand **List** and select **Table**.
5. To configure the Sort by fields, in the **Configure Chart: Table** page, select **Product Version (Agent)** under Agent Properties in the list, click **Value (Descending)**, then click **Next**.
6. In the Columns tab, remove all preconfigured columns except **System Name**, then click **Next**.
7. In the Filter tab, configure these columns, then click **Run**:
   - a For the Property column, select **Product Version (Agent)** from the Available Properties list.
   - b For the Comparison column, select **Less than**.
   - c For the Value column, type the current McAfee Agent version number.

   > Typing the current agent number means that the query finds only versions "earlier than" that version number.

Now your new query can run from a product deployment to update the old McAfee Agent versions.

## Update the McAfee Agents with a product deployment project

Update the old McAfee Agent versions found using an Agent Version Summary query and a Product Deployment task.

### Task

For option definitions, click **?** in the interface.

1. Click **Menu** | **Software** | **Product Deployment**, then click **New Deployment**.
2. From the New Deployment page, configure these settings:
   - a Type a name and description for this deployment. This name appears on the **Product Deployment** page after the deployment is saved.
   - b Next to Type, select **Fixed**.
   - c Next to Package, select the McAfee Agent that you want installed on the systems. Select the language and repository branch (Evaluation, Current, or Previous) that you want to deploy from.
   - d Next to Command line, specify any command-line installation options. See the McAfee Agent Product Guide for information on command-line options.
   - e In the **Select the systems** group, click **Select Systems**, and from the dialog box, click the **Queries** tab and configure these options, then click **OK**:
     - Select the Agent Version Summary table query that you created.
     - Select the system names displayed in the Systems list.

The Total field displays the number of systems selected.

f Next to **Select a start time**, select **Run Immediately** from the list.

3 Click **Save**.

The Product Deployment project starts running and allows you to monitor the deployment process and status. See the McAfee ePolicy Orchestrator Product Guide for details.

**See also**
*Create a new Agent Version Summary query* on page 176

# Finding inactive systems

Most environments are changing constantly, new systems are added and old systems removed. These changes create inactive McAfee Agent systems that, if not deleted, can ultimately skew your compliance reports.

As systems are decommissioned, or disappear because of extended travel, users on leave, or other reasons, remove them from the System Tree. An example of a skewed report might be your DAT report on compliance. If you have systems in your System Tree that have not reported into the McAfee ePO server for 20 days, they appear as out of date by 20 days and ultimately skew your compliance reports.

## Initial troubleshooting

Initially, when a system is not communicating with the McAfee ePO server, try these steps:

1 From the System Tree, select the system and click **Actions** | **Agents** | **Wake Up Agents**.

> Configure a **Retry interval** of, for example, 3 minutes.

2 To delete the device from McAfee ePO, but not remove the agent in the System Tree, select the system and click **Actions** | **Directory Management** | **Delete**. Do not select **Remove agent on next agent-server communication**.

3 Wait for the system to communicate with McAfee ePO again.

> It appears in the System Tree Lost&Found group.

## Dealing with inactive systems

You can create a query and report to filter out systems that have not communicated with the McAfee ePO server in **X** number of days. Or your query and report can delete or automatically move these systems.

It is more efficient to either delete or automatically move these inactive systems. Most organizations choose a deadline of between 14–30 days of no communication to delete or move systems. For example, if a system has not communicated with the McAfee ePO server after that deadline you can:

- Delete that system.
- Move that system to a group in your tree that you can designate as, for example, *Inactive Agents*.

> A preconfigured Inactive Agent Cleanup Task exists, disabled by default, that you can edit and enable on your server.

## Change the Inactive Agents query

If the default **Inactive Agents** query is not configured to match your needs, you can duplicate the query and use it as a base to create your custom query.

Deleting the inactive agents that have not communicated in last month is the default setting for the preconfigured Inactive Agents query. If you want to change the default timer setting, to for example two weeks, you must make a copy of the Inactive Agents query timer.

The instructions in this task describe how to create a copy of the existing Inactive Agents query to change the deadline to 2 weeks.

### Task

For option definitions, click **?** in the interface.

1. To duplicate the Inactive Agents query, click **Menu** | **Reporting** | **Queries & Reports**, then find the **Inactive Agents** query in the list.
2. In the Actions column of the Inactive Agents query, click **Duplicate**.
3. In the Duplicate dialog box change the name, select a group to receive the copy of the query, then click **OK**.
4. Navigate to the duplicate query that you created and, in the **Actions** column, click **Edit** to display the preconfigured Query Builder.

   The preconfigured settings for the chart and table are probably what you need to automatically delete your inactive agent systems.
5. To change the Filter tab settings from once a month to every two weeks, set the **Last Communications** property, **Is not within the last** comparison, to **2** **Weeks** value.

   Don't change the **and Managed State** property, **Equals** comparison, and **Managed** value.
6. Click **Save**.

Now your new Inactive Agents query is ready to run from a server task to delete systems with an inactive agent.

## Delete inactive systems

Use the Inactive Agent Cleanup server task with the preconfigured query named Inactive Agents to automatically delete inactive systems.

### Before you begin

To complete this task, you must have either enabled the Inactive Agents query or duplicated the query.

Deleting a system from the System Tree deletes only the record for that system from the McAfee ePO database. If the system physically exists, it continues to perform normally with the last policies it received from the McAfee ePO server for its applicable products.

### Task

For option definitions, click **?** in the interface.

1. To create a duplicate of the Inactive Agent Cleanup Task, click **Menu** | **Automation** | **Server Tasks**, then find the Inactive Agent Cleanup Task in the server tasks list.
2. Click the preconfigured **Inactive Agent Cleanup Task**, click **Actions** | **Duplicate**.

3 In the Duplicate dialog box, change the server task name, then click **OK**.

4 In the server task row you created, click **Edit** to display the Server Task Builder page.

5 From the Descriptions tab, type any necessary notes, click **Enabled** in **Schedule status**, then click **Next**.

6 From the Actions tab, configure these settings:

  a From the **Actions** list, select **Run Query**,

  b For Query, click **...** to open the **Select a query from the list** dialog box.

  c Click the group tab where you saved your copy of the Inactive Agents query, select your query, then click **OK**.

  d Select your language.

  e In Sub-Actions, select **Delete Systems** from the list.

> Do **not** click **Remove agent**. This setting causes McAfee ePO to delete the McAfee Agent from the inactive systems when they are removed from the System Tree. Without the agent installed, when the removed system reconnects to the network it cannot automatically start communicating with the McAfee ePO server and reinsert itself back into the System Tree.

  **(Optional)** Instead of using the default sub-action Delete Systems, you can select **Move Systems to another Group**. This moves the systems found by the query to a designated group, for example, Inactive Systems in your System Tree.

7 Click **Next**, schedule when you want this server task to run, then save the server task.

Now any inactive systems are automatically removed from the McAfee ePO server, and your system compliance reports provide more accurate information.

## Measuring malware events

Counting malware events provides an overall view of attacks and threats being detected and stopped. With this information, you can gauge the health of your network over time and change it as needed.

Creating a query that counts total infected systems cleaned per week is the first step in creating a benchmark to test your network malware status. This query counts each system as a malware event occurs. It counts the system only once even if it generated thousands of events.

Once this query is created, you can:

- Add it as a dashboard to quickly monitor your network malware attacks.
- Create a report to provide history of your network status.
- Create an Automatic Response to notify you if a threshold of systems is affected by malware.

This dashboard is an example.

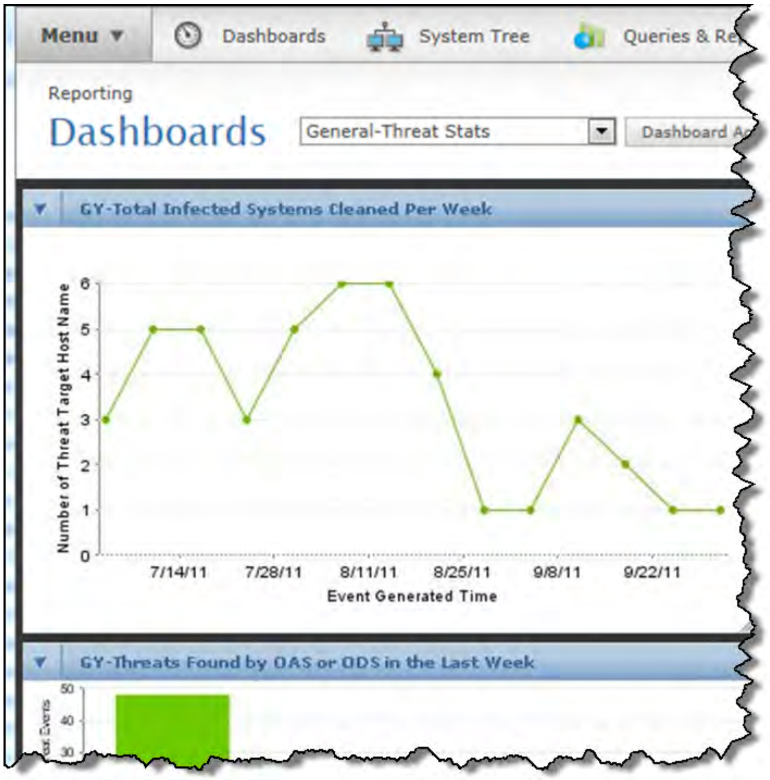


**Figure 13-6 Dashboard showing total infected systems cleaned per week**

## Create a query that counts systems cleaned per week

Creating a query to count the number of systems cleaned per week is a good way to benchmark the overall status of your network.

### Task

For option definitions, click **?** in the interface.

1. Click **Menu** | **Reporting** | **Queries & Reports**, then click **Actions** | **New**.
2. On the Query Wizard **Result Types** tab for the Feature Group, select **Events**, then in the **Result Types** pane, click **Threat Events**, then click **Next**.
3. On the Chart tab, in the Display Results As list, select **Single Line Chart**.
4. In the Configure Chart: Single Line Chart pane, configure these settings, then click **Next**:
   - In Time base is, select **Event Generated Time**.
   - In Time unit, select **Week**.
   - In Time Sequence is, select **Oldest First**.
   - In Line values are, select **Number of**.
   - Select **Threat Target Host Name**.
   - Click **Show Total**.
5. In the Columns tab, in the Available Columns list select these columns to display, then click **Next**:
   - **Event Generated time**
   - **Threat Target Host Name**
   - **Threat Target IPv4 Address**
   - **Event Category**
   - **Threat Severity**
   - **Threat Name**

6 In the Filter tab, Available Properties list, configure this **Required Criteria**:

- For **Event Generated Time**, select these settings from the **Is within the last** list, **3** and **Months**.
- For **Event Category**, select these settings from the **Belongs to list**, **Malware**.
- For **Action Taken**, select these settings from the lists **Equals** and **Deleted**.

7 Click **Save** to display the Save Query page, then configure these settings:

- For Query Name, type a query name, for example, `Total Infected Systems Cleaned Per Week`.
- For Query Description, type a description of what this query does.
- For Query Group, click **New Group**, type the query group name, then click **Public**.

8 Click **Save**.

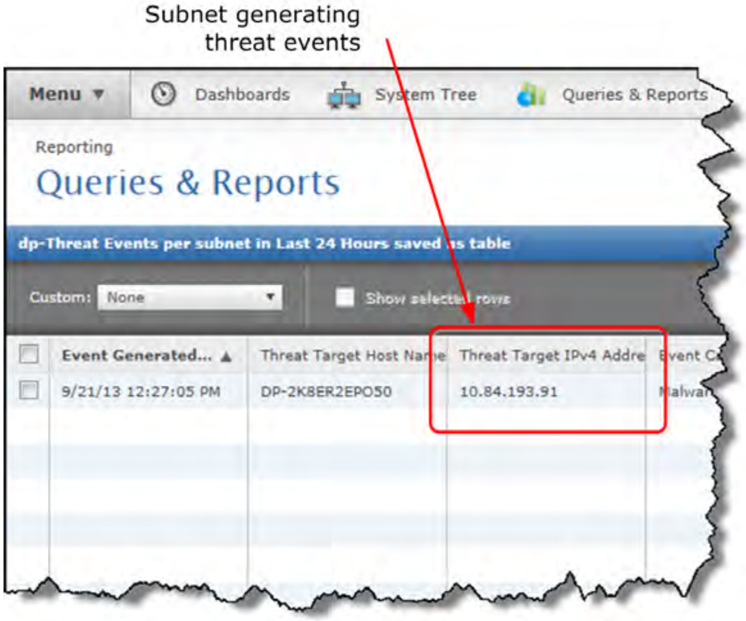
When you run this query, it returns the number of infected systems cleaned per week. This information provides a benchmark of the overall status of your network.

# Finding malware events per subnet

Finding threats by subnet IP address shows you whether a certain group of users needs process changes or additional protection on your managed network.

For example, if you have four subnets, and one subnet is continuously generating threat events, you might learn that group has been passing around an infected USB drives.

This example shows the systems and their subnet generating the most malware events.



Subnet generating threat events

Reporting

Queries & Reports

dp-Threat Events per subnet in Last 24 Hours saved as table

| □ | Event Generated... ▲ | Threat Target Host Name | Threat Target IPv4 Addre | Event C |
|---|---|---|---|---|
| □ | 9/21/13 12:27:05 PM | DP-2K8ER2EPO50 | 10.84.193.91 | Malwar |

**Figure 13-7 Query output showing subnets with threats**

## Create a query to find malware events per subnet

Create a query to find malware events and sort them by subnet. This query helps you find networks in your environment that are under attack.

### Task

For option definitions, click **?** in the interface.

1. To duplicate the existing **Threat Event Descriptions in the Last 24 Hours** query, click **Menu** | **Reports** | **Queries & Reports**, then find and select the **Threat Target IP Address** query in the list.
2. Click **Actions** | **Duplicate** and in the Duplicate dialog box, edit the name, select the group to receive the copy, then click **OK**.
3. In the Queries list, find the new query that you created and click **Edit**.

   The duplicated query is displayed in the Query Builder with the Chart tab selected.
4. In the Display Results As list, select **Table** under **List**.
5. In the Configure Chart: Table dialog box, select **Threat Target IPv4 Address** from the sort by list and **Value (Descending)**, then click **Next**.
6. In the Columns tab, you can use the preselected columns.

   > It might help to move the **Threat Target IPv4 Address** closer to the left of the table, then click **Next**.

   Don't change the default Filter tab settings.
7. Click the Summary tab, confirm that the query settings are correct, then click **Save**.
8. In the Queries list, find the query that you created, then click **Run**.

Now you have a query to find malware events and sort them by IP subnet address.

## Automating DAT file testing

Use the built-in functionality provided by McAfee ePO to automatically validate DAT and content files that are downloaded from the McAfee public site.

> McAfee Labs rigorously test the content, such as DAT and engine files, before they are released on the public update servers. Because every organization is unique, you can perform your own validation to ensure the compatibility of DATs and content in your unique environment.

The validation processes vary from organization to organization. The process in this section is meant to automate much of the validation process and reduce the need for administrator intervention.

> To confirm that only validated DAT files are distributed in your environment, move the content manually from the Evaluation branch into the Current branch of the repository.

### DAT file validation overview

An overview of the automated DAT validation process is shown in this figure.

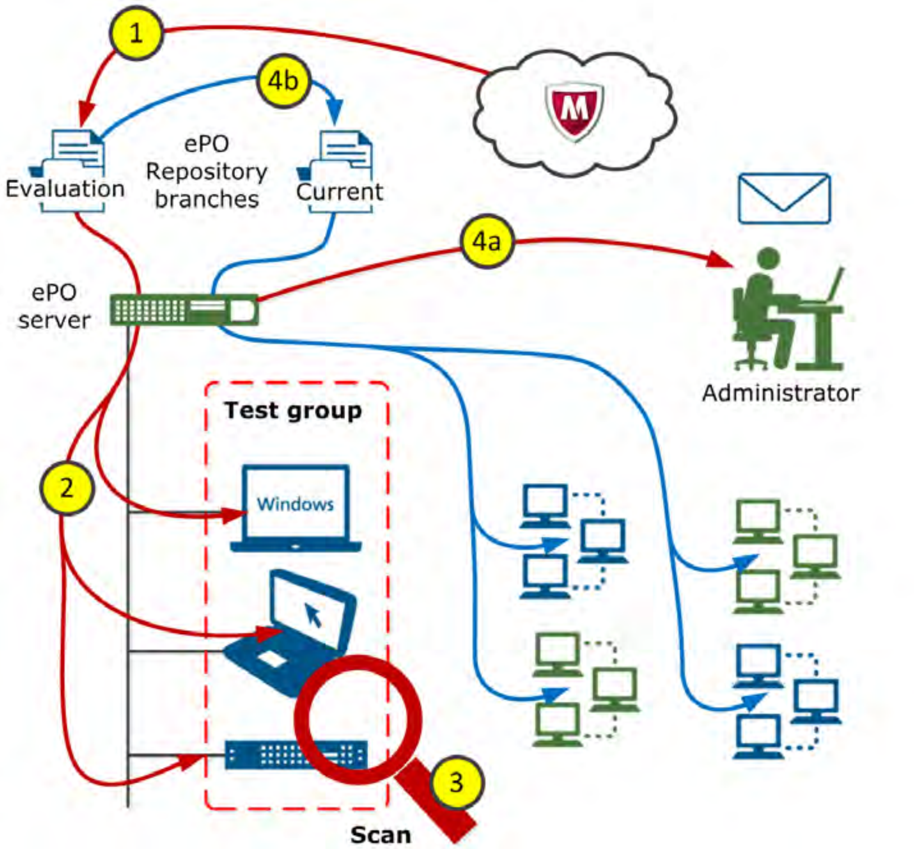


**Figure 13-8 Automatic DAT file testing steps**

These steps describe of the numbers shown in the figure.

1. A server task pulls DAT updates from the McAfee public site to the Evaluation branch of the Master Repository.
2. A McAfee Agent policy applies the DAT files from the Evaluation repository branch restricted to a group of systems in a Test group.
3. An On-Demand Scan task runs frequently on the test group.
4. Depending on the On-Demand Scan scan output, one of these scenarios occurs:
   - a If malware is detected in the test group, an Automatic Response email is sent to the appropriate administrators. The email tells the administrators to stop distribution of the DAT files from the Current repository.
   - b Otherwise, after a specified time, a server task copies the files from the Evaluation branch to the Current branch of the repository. Then those files are automatically sent to the rest of the managed systems.

## Pull and copy DAT updates from McAfee

To create an automated DAT file testing process requires configuring tasks to pulls the DATs from McAfee and copy them to the Current branch of the repository.
The McAfee ePO platform provides three repository branches in your Master and Distributed Repositories:

- Current branch — By default, the main repository branch for the latest packages and updates.
- Evaluation branch — Used to test new DAT and engine updates before deploying to your entire organization.
- Previous branch — Used to save and store prior DAT and engine files before adding the new ones to the Current branch.

You must create two server tasks to automate the DAT file testing.

- One task pulls the DAT files hourly to the Evaluation branch to ensure that the latest DAT is in the Evaluation branch shortly after McAfee releases it to the public.

  > Running the task hourly allows you to get an extra DAT file in case the initial file, released at 11:00 a.m., was replaced later in the day.

- One server task waits until after the test group of systems is scanned for a few hours. Then, if the server task is not stopped by the administrator, it automatically copies the DAT files from the Evaluation branch to the Current branch.

### Tasks

- *Configure task to pull DAT to Evaluation branch* on page 185
  To automate your DAT file testing process, you must create a task to automatically pull DAT files from the McAfee public site into the Evaluation repository branch.
- *Configure server task to copy files from Evaluation to Current branch* on page 186
  To automate your DAT file testing process, create a task to automatically copy DAT files from the **Evaluation** branch of the repository to the **Current** branch.

## Configure task to pull DAT to Evaluation branch

To automate your DAT file testing process, you must create a task to automatically pull DAT files from the McAfee public site into the Evaluation repository branch.

You might want to configure this task to distribute only DAT files, if your organization tests the engine for a longer time, than the few hours in this example, or restricts their automatic release.

### Task

For option definitions, click **?** in the interface.

1. Click **Menu** | **Automation** | **Server Tasks**, then click **Actions** | **New Task**, to display the **Server Task Builder** wizard.
2. In the Description tab, type a server task name, for example, `DAT pull hourly to Evaluation repository`, and a description to appear on the Server Task page.
3. In Schedule status, click **Enable**, then click **Next**.
4. In the Actions tab, configure these settings:
   - From the **Actions** list, select **Repository Pull**.
   - From the Source site list, select **McAfeeFtp** or **McAfeeHttp**, depending on the McAfee public site you want to use.
   - From the Branch list, select **Evaluation.**
   - Deselect **Move existing package to Previous branch**, if needed.
   - From Package types, click **Select packages**.

5 From the Available Source Site Packages dialog box, select **DAT** and **Engine**, then click **OK**.

McAfee recommends that, at minimum, you pull the DAT and engine files from the McAfee public website.

If you have multiple distributed repositories, you can chain a replication task to the same pull task to replicate your Evaluation branch to your distributed repositories.

6 In the Schedule tab, configure these settings:

- For the Schedule type, click **Hourly**.
- For the Start date, select today's date.
- For the End date, click **No end date.**
- From Schedule, configure the task to run every hour at 10 minutes past the hour.

7 Click **Next**, confirm that all settings are correct in the Summary tab, then click **Save**.

To confirm that the automatic DAT file pull is working, go to **Menu** | **Software** | **Master Repository** and use the Check-In date information to confirm that the Evaluation branch DAT file was updated within the last two hours.

## Configure server task to copy files from Evaluation to Current branch

To automate your DAT file testing process, create a task to automatically copy DAT files from the **Evaluation** branch of the repository to the **Current** branch.

### Before you begin

You must have created the server task to automatically copy the DAT and content files to the **Evaluation** branch of the repository. See Configure task to pull DAT to Evaluation branch on page 185 for details.

The daily server task to pull the DAT file, or DAT and Engine file, into the Current branch of the Master Repository runs four hours after another server task has pulled the same files into the Evaluation branch. This task means that you are validating the files for a total of two or three hours on your test group. If you want to perform further validation, make this task run later in the day, for example 4:00 or 5:00 p.m.

Your systems might not get updated with the most current DAT until the next day, if the systems in your environment are turned off when the workday ends. This pull time depends on your organization's policies and your tolerance for risk.

Confirm that you also copied the files to the distributed repositories as needed.

### Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Automation** | **Server Tasks**, then click **Actions** | **New Task**.

2 In the Server Task Builder Descriptions tab, type a task name and notes, then in **Schedule status**, click **Enabled**, then click **Next**.

3 In the Actions tab, configure these settings, then click **Next**:

- For Actions list, select **Change the Branch for a Package**, select **All packages of type 'DAT' in branch 'Evaluation'** as the package to change, **Copy** as the action, then click **Current** as the target branch.
- Click **+** to create another action, and from the second Actions list, select **Change the Branch for a Package**, select **All packages of type 'Engine' in branch 'Evaluation'** as the package to change, **Copy** as the action, and **Current** as the target branch.

4 In the Schedule tab, change these settings:

- For Schedule type, click **Daily**.
- For Start date, select today's date.
- For End date, click **No end date**.
- Change the Schedule settings to configure the task to run at 2:00 or 3:00 p.m.

> Historically, McAfee releases DAT files only once a day, at approximately 11:00 a.m. Eastern Time. In the rare case that a second DAT file is released later in the day, it requires an administrator to disable the copy task to your Current Branch.

- Click **Next**, confirm that all settings are correct in the Summary tab, then click **Save**.

To confirm that the DAT file copy from the Evaluation branch to the Current branch is working, go to **Menu** | **Software** | **Master Repository** and use the Check-In date information to confirm that the Evaluation branch DAT file was copied to the Current branch at the time configured in the schedule.

**See also**

*Configure task to pull DAT to Evaluation branch* on page 185

## Create a test group of systems

To safely test DAT and content files, create a test group of systems used to run the files in your Evaluation repository.

McAfee recommends that the test group of systems you use meet the following criteria:

- Use a representative sampling of system server builds, workstation builds, and operating systems and Service Packs in your environment for validation.
- Use 20–30 systems for validation for organizations with less than 10,000 nodes. For larger organizations, include at least 50 types of systems.

> You can use VMware images that replicate your operating system builds. McAfee recommends that these systems be in a "clean" state to ensure that no malware has been introduced.

You do not have to move systems into their own test group. You can use Tags to apply policies and tasks to individual systems that are scattered throughout your System Tree. Tagging these systems has the same effect as creating an isolated test group, but allows you to keep your systems in their current groups. This option is slightly more complex and is not described in this section.

### Task

For option definitions, click **?** in the interface.

1 To create a System Tree group, click **Menu** | **Systems Section** | **System Tree**.

2 From the System Tree group list, select where you want to add your new group, then click **System Tree Actions** | **New Subgroups**, and in the New Subgroups dialog box, type a name, for example `DAT Validation`, then click **OK**.

3 To add systems to your test group, you can drag systems from other groups to your newly created subgroup, add new systems, or add virtual machine systems.

You created a test group as an isolated group of systems. This test group allows you to test new DAT and engine updates before you deploy the updates to all other systems in your organization.

## Configure an agent policy for the test group

You must create a McAfee Agent policy with an update task that automatically copies DAT and content files to the systems in your test group.

### Task

For option definitions, click **?** in the interface.

1 In the **System Tree**, click **Menu** | **Systems Section** | **System Tree**, then click the test group you created in *Create test group of systems*.

In that example, the group name is `DAT Validation`.

2 To duplicate the existing policy, click the **Assigned Policies** tab, select **McAfee Agent** from the **Product** list, then in the **Category** list in the **General** policy row, click **My Default**.

3 On the **My Default** page, click **Duplicate**, and in the **Duplicate Existing Policy** dialog box, type the name, for example `Update from Evaluation`, add any notes, then click **OK**.

This step adds a policy, named `Update from Evaluation`, to the Policy Catalog.

4 Click the **Updates** tab to change the repository used by this policy.

5 In the Repository branch to use for each update type, click the **DAT** and **Engine** list down-arrows, then change the listed repositories to **Evaluation**.

6 Click **Save**.

Now you have created a new McAfee Agent policy to use with an update task that automatically copies the DAT and content files to the systems in your test group from the Evaluation repository.

## Configure an on-demand scan of the test group

Create an on-demand scan task, launched after you update the DAT files to your test group, to scan for any problems that occur in your test group.

**Before you begin**

You must have created the test group in your System Tree before you can complete this task. See Create a test group of systems on page 187 for details.

This configuration assumes you are not using user systems as your test systems. If you are using actual user systems, you might need to modify some of these scan configurations.

### Task

For option definitions, click **?** in the interface.

1 To create a new on-demand scan task, click **Menu** | **Policy** | **Client Task Catalog**, then from the **Client Task Catalog** page in the **Client Task Types** list, expand VirusScan Enterprise and click **On Demand Scan**.

2 In the Client Task Catalog page, click **New Task**, and in the New Task dialog box, confirm **On Demand Scan** is selected and click **OK**.

3 On the **Client Task Catalog : New Task** page, in **Task Name** and **Description**, type a name, for example, `Evaluation test group ODS task`, and add a detailed description.

4 Click the **Scan Locations** tab, then configure these settings:

   a For the **Locations to scan**, at a minimum, configure:

   - Select **Memory for rootkits**.
   - Select **Running Processes**.
   - Select **All local disks**.
   - Select **Windows folder**.

   b For the **Scan options**, click **Include subfolders** and **Scan boot sectors**.

5 Click the **Scan Items** tab, then configure these settings:

   a For **File types to scan**, click **All files**.

   b For **Options**, click **Detect unwanted programs**.

   c For **Heuristics**, click **Find unknown program threats** and **Find unknown macro threats**.

6 Do not configure any **Exclusions**.

7 Click the **Actions** tab, configure **When a threat is found** as **Clean files**, then **Delete files**.

   a For **When a threat is found**, configure **Clean files**, then **Delete files**.

   b For **When an unwanted program is found**, configure **Clean files**, then **Delete files**.

8 Click the **Performance** tab and configure **System utilization** as **Low** and **Artemis** as **Very Low**.

> Do not change any settings on the **Reports** tab.

9 Click the **Task** tab, then configure these settings:

   a For **Platforms where this task will run**, click both **Run this task on servers** and **Run this task on workstations**.

   b For **User account to use when running task**, set your credentials and select the test group domain.

10 Click **Save**.

Now the on-demand scan task is configured to scan for any problems that might occur in your test group. Next you need to configure a client task to schedule when to launch the task.

## Schedule an on-demand scan of the test group

Schedule your on-demand scan task to run five minutes after each McAfee Agent policy update from the Evaluation repository to the test group.

> **Before you begin**
> You must have created a test group of systems and an on-demand scan of the test group to complete this task. See Create a test group of systems on page 187 and Configure an on-demand scan of the test group on page 188.

### Task

For option definitions, click **?** in the interface.

1 Click **Menu** | **Policy** | **Client Task Catalog**.

2 On the Client Task Catalog page, select **VirusScan Enterprise** and **On Demand Scan** in Client Task Types.

3 Find the on-demand scan you created, click **Assign** in the Actions column, select the test group of systems you created to assign the task, then click **OK**.

4 In the Client task Assignment Builder, configure these settings, then click **Next**:

   a For **Product** list, select **VirusScan Enterprise**.

   b For **Task Type** list, select **On Demand Scan**.

   c For **Task Name** list, select the ODS task you created in *Configure On Demand Scan of test group*.

5 In the **Schedule** tab, configure these settings:

   a For **Schedule status**, click **Enabled**.

   b For **Schedule type**, select **Daily** from the list.

   c For **Effective period**, select today's date as the **Start date**, then click **No end date**.

   d For **Start time**, configure these settings:

   - Select **11:05 AM** from the time lists.
   - Click **Run at that time, and then repeat until**, then select **2:00 PM** from the time lists.
   - For During repeat, start task every, select **30 minute(s)** from the lists.

   e For Task runs according to, click **Local time on managed systems**.

   f For Options, deselect everything.

6 Click **Next**, check the Summary page, then click **Save**.

Your on-demand scan task is now scheduled to run every 5 minutes, from 9:05 a.m. until 2:00 p.m., after each agent policy update, from the Evaluation repository to the test group.

## Configure an Automatic Response for malware detection

If malware is found by the on-demand scan in the test group, you want to block the files from being copied automatically to the Current repository. Set up an automatic notification to the administrator.

> **Before you begin**
>
> You must have already created an on-demand scan task to scan for any problems that might occur in your test group.

### Task

For option definitions, click **?** in the interface.

1 To display the Response Builder, click **Menu** | **Automation** | **Automatic Responses**, click **New Response**, then configure these settings in the Descriptions tab, then click **Next**.

   a Type a name, for example `Malware found in test group`, and a detailed **Description.**

   b For Language, select a language from the list.

   c For Event Group, select **ePO Notification Events** from the list.

   d From **Event type**, select **Threat** from the list.

   e For Status, click **Enabled**.

2 Configure these settings in the Filter tab, then click **Next**.

   a For Available Properties list, select **Threat Category**.

   > Optionally, you can add additional categories, such as an access protection rule being triggered.

b In the Required Criteria column and the **Defined at** row, click … to select the test group of systems you created in the **Select System Tree Group** dialog box, then click **OK**.

c In the Threat Category row, select **Belongs to** from the Comparison list and **Malware** from the Value list. Click **+** to add another category.

d Select **Belongs to** from the Comparison list and **Access Protection** from the Value list.

3 Configure these settings in the Aggregation tab, then click **Next**.

a For **Aggregation**, click **Trigger this response for every event**.

b Do not configure any **Grouping** or **Throttling** settings.

4 Configure these settings in the **Actions** tab:

a Select **Send Email** from the **Actions** list.

b For Recipients, type the email address of the Administrator to be notified.

c For Importance, select **High** from the list.

d For Subject, type an email header, for example `Malware found in the Test Group!`

e For Body, type a message, for example `Research this NOW and stop the server task that pulls content into the Current branch!`

f Following the message body, insert these variables to add to the message, and click **Insert**:

- **OS Platform**
- **Threat Action Taken**
- **Threat Severity**
- **Threat Type**

Your email body looks similar to this:

```
Research this NOW and stop the server task that pulls content into the Current branch!

{listOfOsPlatform}{listOfThreatActionTaken}{listOfThreatSeverity}{listOfThreatType}
```

5 Click **Next**, confirm that the configuration is correct in the Summary tab, then click **Save**.

Now you have an Automatic Response configured that sends an email to an administrator any time malware is detected in the test group running the Evaluation DAT file.

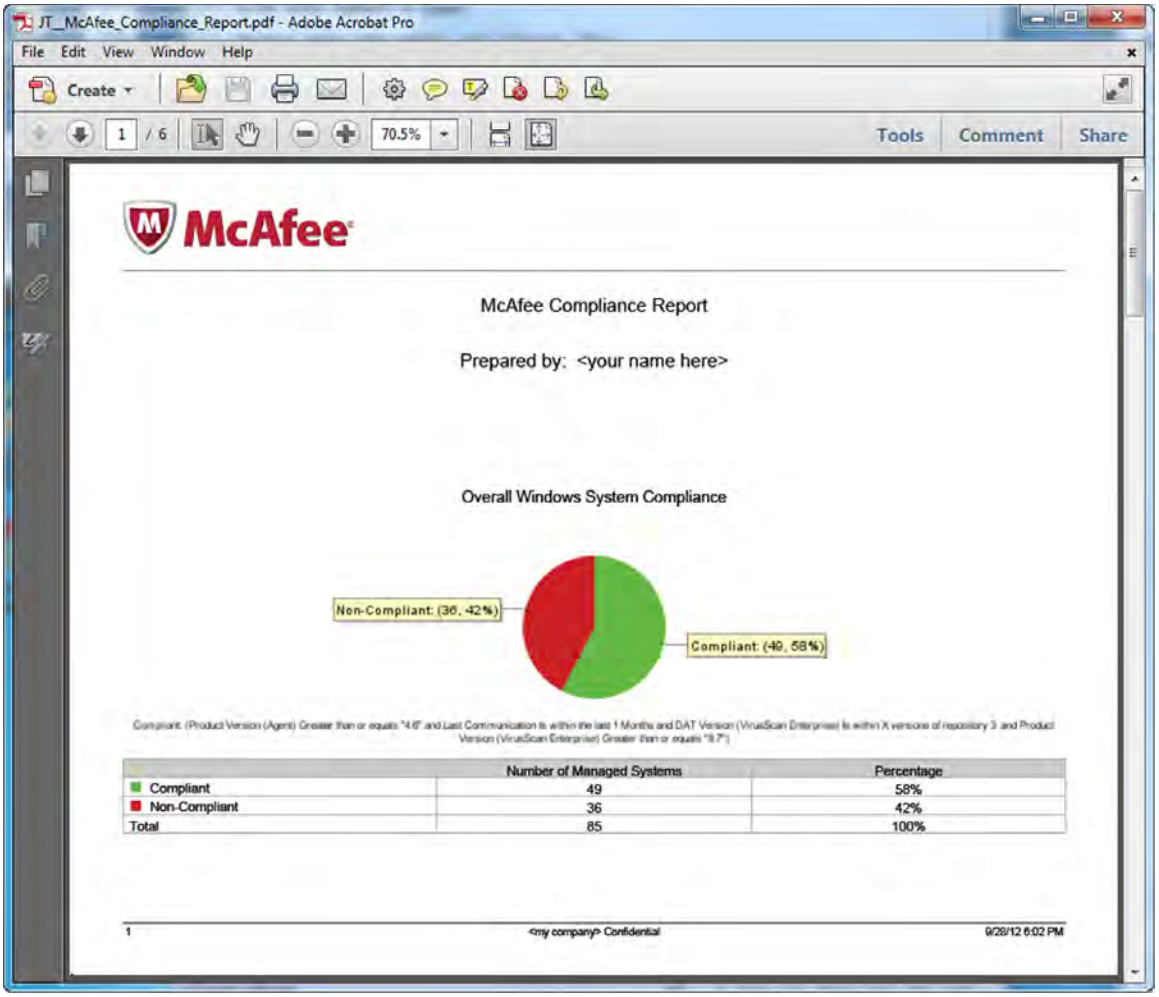
**See also**
*Configure an on-demand scan of the test group* on page 188

## Create an automatic compliance query and report

You can create a compliance query and report to find which of your managed systems meet specific criteria.

For example, you can find systems that don't have the latest DATs or have not contacted the McAfee ePO server in over 30 days.

This is an example of the report created using the query output and automatically delivered to the Administration team.



McAfee Compliance Report

Prepared by: <your name here>

Overall Windows System Compliance

Compliant: (Product Version (Agent) Greater than or equals "4.6" and Last Communication is within the last 1 Months and DAT Version (VirusScan Enterprise) is within X versions of repository 3 and Product Version (VirusScan Enterprise) Greater than or equals "8.7")

| | Number of Managed Systems | Percentage |
|---|---|---|
| 🟩 Compliant | 49 | 58% |
| 🟥 Non-Compliant | 36 | 42% |
| Total | 85 | 100% |

1 <my company> Confidential 9/28/12 6:02 PM

**Figure 13-9 Sample automatic compliance query and report output**

To find this important information automatically, use these tasks.

## Tasks

- *Create a server task to run compliance queries* on page 193
  You must create a server task to run your compliance queries weekly to automate generating your managed systems' compliance report.
- *Create a report to include query output* on page 194
  Once you have the query data saved, you must create a report to contain the information from the queries you ran before you can send it to the administrator team.
- *Create a server task to run and deliver a report* on page 194
  You must create a server task to automatically run the report and send the compliance report to your administrators.

## Create a server task to run compliance queries

You must create a server task to run your compliance queries weekly to automate generating your managed systems' compliance report.

Follow these steps to create a server task that runs your compliance queries every Sunday morning at 2:00 a.m. Running the queries on Sunday morning allows you to run the report on Monday morning at 5:00 a.m. and deliver it by email to the administrators.

### Task

For option definitions, click **?** in the interface.

1. Click **Menu** | **Automation** | **Server Tasks**, then click **Actions** | **New Task**.
2. In the Server Task Builder:
   - a. In the, **Descriptions** tab, type a name and notes.
   - b. In the **Schedule status**, click **Enabled**.
   - c. Click **Next**.
3. In the Actions tab, configure these settings.
   - a. In the Actions list, select **Run Query** and configure these settings:
     - For Query, select **VSE: Compliance Over the Last 30 Days**.
     - Select your language.
     - For Sub-Actions, select **Export to File** then click **OK**.
     - For C:\reports\, type a valid file name.
     - For If file exists, select **Overwrite**.
     - For Export, select **Chart data only**.
     - For Format, select **CSV**.
   - b. Click **+** to create another action, and in the second **Actions** list, select **Run Query** and configure these settings, then **Next**.
     - For Query, select **Inactive Agents**.
     - Select your language.
     - For Sub-Actions, select **Export to File**.
     - For C:\reports\, type a valid file name.
     - For If file exists, select **Overwrite**.
     - For Export, select **Chart data only**.
     - For Format, select **CSV**.
4. In the **Schedule** tab, change these settings, then click **Next**.
   - a. For Schedule type, click **Weekly**.
   - b. For Start date, select today's date.
   - c. For End date, click **No end date**.
   - d. Change the **Schedule** settings to configure the task to run on **Monday** at **2:00 AM**.

     You can set the schedule to run whenever and as often as you want.
   - e. Confirm that all settings are correct in the Summary tab, then click **Save**.

That completes creating the server task to automatically run the two compliance queries, then save the output of the queries to CSV files.

# Create a report to include query output

Once you have the query data saved, you must create a report to contain the information from the queries you ran before you can send it to the administrator team.

### Before you begin

Before you create your report page, you must know the format of the queries you are adding to the report. In this example the queries have these formats:

- **VSE: Compliance Over the Last 30 Days** — Chart
- **Inactive Agents** — Table

Create a report that contains the data captured from your compliance queries, which is run automatically using a server task, then emailed to the administrators every Monday morning.

### Task

For option definitions, click **?** in the interface.

1. Click **Menu** | **Reporting** | **Queries & Reports**, then select the **Report** tab.
2. Click **Actions** | **New**.

   A blank Report Layout page appears.
3. Click **Name** and type a name for the report, click **Description** and, optionally, type a description, click **Group** and select an appropriate group to receive the report, then click **OK**.
4. In the Report Layout pane, drag-and-drop these query input formats from the **Toolbox** list:
   - For the VSE: Compliance Over the Last 30 Days chart query, drag the **Query Chart** tool into the **Report Layout** pane, then from the **Query Chart** list select **VSE: Compliance Over the Last 30 Days**, then click **OK**.
   - For the Inactive Agents table query, drag the **Query Table** tool into the **Report Layout** pane, then from **Query** table list, select **Inactive Agents**, then click **OK**.
5. Click **Save**, and the new compliance report is listed in the Reports tab.
6. To confirm that your report is configured correctly, click **Run** in the **Actions** column for your report, then verify that the **Last Run Status** displays **Successful**.
7. To see the report, click the link in the **Last Run Result** column, then open or save the report.

That completes creating the report to display the two compliance queries and save their output to a PDF file.

# Create a server task to run and deliver a report

You must create a server task to automatically run the report and send the compliance report to your administrators.

### Before you begin

Before you can run this report, you must have already:

- Created and scheduled a server task that runs the compliance queries.
- Created the report that includes the output of these queries.

Follow these steps to:

- Automatically run a report that contains the data captured from your compliance queries.
- Use a server task to email the report to the administrators every Monday morning at 5:00 a.m.

### Task

For option definitions, click **?** in the interface.

1. Click **Menu** | **Automation** | **Server Tasks**, then click **Actions** | **New Task**.
2. In the Server Task Builder, then click **Next**.
   - a. In the **Descriptions** tab, type a name and notes.
   - b. In the **Schedule status**, click **Enabled**.
3. In the Actions tab, select **Run Report**, configure these settings, then click **Next**.
   - a. For Select a report to run, select the compliance report you configured in Create a report to include query output on page 194.
   - b. Select your language.
   - c. For Sub-Actions, select **Email file**.
   - d. For Recipients, type the email addresses of your administrators.

     Separate multiple email addresses with commas.
   - e. For Subject, type the information you want to appear in the subject line of the email.
4. In the Schedule tab, change these settings, then click **Next**.
   - a. For **Schedule type**, click **Weekly**.
   - b. For Start date, select today's date.
   - c. For End date, click **No end date**.
   - d. Change the Schedule settings to configure the task to run on **Monday** at **5:00 AM**.

     You can set the schedule to run whenever and as often as you want.
   - e. Confirm that all settings are correct in the Summary tab, then click **Save**.

That completes the final task to create a compliance report that runs automatically and is delivered to your administrators every Monday morning at 5 a.m.

14

# Plan your disaster recovery

Configure the McAfee ePO server for a disaster recovery scenario as soon as possible after you complete your installation.

**Contents**

## Use Disaster Recovery

The Disaster Recovery feature helps you quickly recover or reinstall your McAfee ePO software.

Disaster Recovery uses a Snapshot feature that periodically saves your McAfee ePO configuration, extensions, keys, and more to snapshot records in the McAfee ePO database. For complete details about Disaster Recovery, see the McAfee ePolicy Orchestrator Product Guide. For additional information see KnowledgeBase Article McAfee ePO server backup and disaster recovery procedure, KB66616.

The records saved by the snapshot contain the entire McAfee ePO configuration at the specific time the snapshot is taken. Once the snapshot records are saved to the database, you can use the Microsoft SQL backup feature to save the entire McAfee ePO database and restore it to another SQL Server.

The McAfee ePO software Disaster Recovery configuration includes these general steps performed on the McAfee ePO primary server:

1. Take a snapshot of the McAfee ePO server configuration and save it to the primary SQL database. This can be done manually or through a default server task provided for this purpose.

2. Back up the SQL database using the Microsoft SQL Server Management Studio or the BACKUP (Transact-SQL) command-line process.

3. Copy the SQL database backup file, created in step 2, to the duplicate SQL Server used to restore the database.

4. Reinstall the McAfee ePO software using the **Restore** option when the McAfee ePO Setup launches.

# Use server clusters for disaster recovery

If you require zero downtime when a hardware failure occurs, you can cluster your McAfee ePO server and SQL Servers. However, zero downtime requires additional hardware and increases the cost of implementation.

You might choose to cluster only the SQL Servers to minimize downtime. If the McAfee ePO server fails due to a hardware failure, you can reinstall its operating system, which takes only a few hours, and point the McAfee ePO server to your SQL database.

The full restore procedures are described in McAfee ePO server backup and disaster recovery procedure, KnowledgeBase article KB66616.

# Use cold and hot spares on one physical site

If your large production environment requires minimal downtime, you can use a cold or hot spare McAfee ePO server. The spare server runs a restored installation of McAfee ePO and points to your SQL database.

If you have only one physical site, cluster your SQL Servers. If your McAfee ePO server fails, you can simply change the IP address of the spare McAfee ePO server to the IP address of the failed McAfee ePO server. This IP address change is transparent to the agents and provides the least downtime in a disaster situation.

! You must have a last-known-good SQL database backup for this IP address change to work.

See the McAfee ePolicy Orchestrator Product Guide for full restore procedures.

# Use cold and hot spares on two physical sites

For total disaster recovery, use two physical sites, one primary site and one secondary site.

Your primary site has a clustered SQL Server and a single McAfee ePO server. The secondary site should have a hot or cold spare McAfee ePO server and an SQL database. We recommend that you locate the secondary McAfee ePO server at another physical site that has a different IP address and different DNS name. You can use SQL replication or SQL Log Shipping to copy the McAfee ePO database from the primary site to the secondary site's SQL Server on a nightly or weekly basis during non-business hours. Then make sure that your secondary McAfee ePO server is selecting your secondary SQL Server. See the Microsoft article, Types of Replication Overview for details.

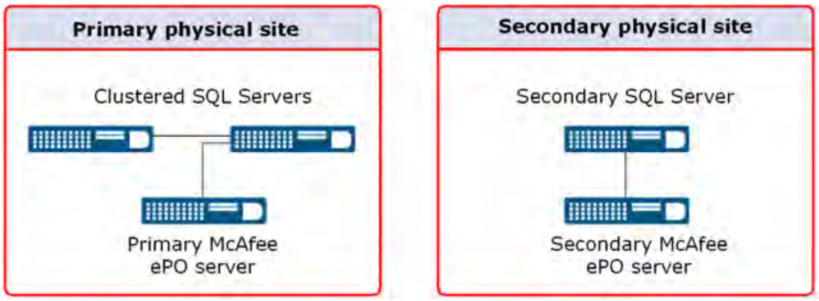


**Figure 14-1 Primary and secondary McAfee ePO site configuration**

If the primary site fails to communicate, configure all agents previously communicating with the primary McAfee ePO server to communicate with the secondary server. The agents find the McAfee ePO server by communicating to its IP address first, and if that fails they use its DNS name. If the agents find that the primary McAfee ePO server's IP address is not available, these steps occur.

1. The agents query the DNS where you have changed the IP address for the primary server.
2. The agents select the IP address of the secondary server.
3. The agents try to connect to the secondary McAfee ePO server and SQL database.

See the McAfee ePolicy Orchestrator Product Guide for full restore procedures.

# A

# Additional Information

## Contents

## Ports used to communicate through a firewall

These tables list the ports your McAfee ePO server uses to communicate through a firewall.

These are the definitions of traffic directions used in these tables:

- Inbound — Connection is from a remote system.
- Outbound — Connection is from the local system.
- Bidirectional — Connection is initiated from either direction.

### McAfee ePO 5.1 ports

| Port | Default | Description | Traffic direction |
|---|---|---|---|
| Agent-server communication port | 80 | TCP port used by the McAfee ePO server service to receive requests from agents. | Inbound connection to the Agent Handler and the McAfee ePO server from the McAfee Agent.<br>Inbound connection to the McAfee ePO server from the remote Agent Handler. |
| Agent-server communication secure port<br>Software Manager | 443 | TCP port used by the McAfee ePO server service to receive requests from agents and remote Agent Handlers.<br>TCP port used by the McAfee ePO server's Software Manager to connect to McAfee ePO. | Inbound connection to the Agent Handler and the McAfee ePO server from the McAfee Agent.<br>Inbound connection to the McAfee ePO server from the remote Agent Handler. |

| Port | Default | Description | Traffic direction |
|---|---|---|---|
| Agent wake-up communication port<br>SuperAgent repository port | 8081 | TCP port used by agents to receive agent wakeup requests from the McAfee ePO server or Agent Handler.<br>TCP port used by SuperAgents configured as repositories to receive content from the McAfee ePO server during repository replication, and to serve content to client systems. | Inbound connection from the McAfee ePO server or Agent Handler to the McAfee Agent.<br>Inbound connection from client systems to SuperAgents configured as repositories. |
| Agent broadcast communication port | 8082 | UDP port used by SuperAgents to forward messages from the McAfee ePO server or Agent Handler. | Outbound connection from the SuperAgents to other agents. |
| Console-to-application server communication port | 8443 | TCP port used by the McAfee ePO Application Server service to allow web browser UI access. | Inbound connection to the McAfee ePO server from McAfee ePO Console. |
| Client-to-server authenticated communication port | 8444 | Used by the Agent Handler to talk to the McAfee ePO server to get required information (like LDAP servers). | Outbound connection from remote Agent Handlers to the McAfee ePO server. |
| SQL Server TCP port | 1433 | TCP port used to communicate with the SQL Server. This port is specified or determined automatically during the setup process. | Outbound connection from the McAfee ePO server or Agent Handler to the SQL Server. |
| SQL Server UDP port | 1434 | UDP port used to request the TCP port that the SQL instance hosting the McAfee ePO database is using. | Outbound connection from the McAfee ePO server or Agent Handler to the SQL Server. |
| LDAP server port | 1434 | UDP port used to request the TCP port that the SQL instance hosting the McAfee ePO database is using. | Outbound connection from the McAfee ePO server or Agent Handler to an LDAP server. |
| SSL LDAP server port | 389 | TCP port used to retrieve LDAP information from Active Directory servers. | Outbound connection from the McAfee ePO server or Agent Handler to an LDAP server. |

## McAfee ePO ports and traffic quick reference

### Table A-1 McAfee ePO server

| Default Port | Protocol | Traffic direction |
|---|---|---|
| 80 | TCP | Inbound connection to the McAfee ePO server |
| 389 | TCP | Outbound connection from the McAfee ePO server |
| 443 | TCP | Inbound or outbound connection to or from the McAfee ePO server |
| 636 | TCP | Outbound connection from the McAfee ePO server |
| 1433 | TCP | Outbound connection from the McAfee ePO server |
| 1434 | TCP | Outbound connection from the McAfee ePO server |
| 8081 | TCP | Outbound connection from the McAfee ePO server |

Table A-1 McAfee ePO server *(continued)*

| Default Port | Protocol | Traffic direction |
|---|---|---|
| 8443 | TCP | Inbound connection to the McAfee ePO server |
| 8444 | TCP | Inbound connection to the McAfee ePO server |

Table A-2 Remote Agent Handler

| Default Port | Protocol | Traffic direction |
|---|---|---|
| 80 | TCP | Inbound or outbound connection to or from the Agent Handler |
| 389 | TCP | Outbound connection from the Agent Handler |
| 443 | TCP | Inbound or outbound connection to or from the Agent Handler |
| 636 | TCP | Outbound connection from the Agent Handler |
| 1433 | TCP | Outbound connection from the Agent Handler |
| 1434 | TCP | Outbound connection from the Agent Handler |
| 8081 | TCP | Outbound connection from the Agent Handler |
| 8443 | TCP | Outbound connection from the Agent Handler |
| 8444 | TCP | Outbound connection from the Agent Handler |

Table A-3 McAfee Agent

| Default Port | Protocol | Traffic direction |
|---|---|---|
| 80 | TCP | Outbound connection to the McAfee ePO server or Agent Handler |
| 443 | TCP | Outbound connection to the McAfee ePO server or Agent Handler |
| 8081 | TCP | Inbound connection from the McAfee ePO server or Agent Handler<br>If the agent is a SuperAgent repository, inbound connection from other McAfee Agents. |
| 8082 | UDP | Inbound connection to agents<br>Inbound or outbound connection from or to SuperAgents. |

Table A-4 SQL Server

| Default Port | Protocol | Traffic direction |
|---|---|---|
| 1433 | TCP | Inbound connection from the McAfee ePO server or Agent Handler |
| 1434 | UDP | Inbound connection from the McAfee ePO server or Agent Handler |

# Getting more information

Use these links to find valuable information about your McAfee implementation.

## Product videos

- Support Video Tutorials — These links, on the Technical Support ServicePortal page, provide video tutorials listed by product, and created by the McAfee Support Team.
- McAfee Technical YouTube — This YouTube McAfee Technical page, under Security System Management, provides videos describing McAfee ePO processes.

## Important McAfee KB articles

- KB59938 — Provides detailed version information for McAfee ePO.
- KB51109 — Lists every operating system supported by every McAfee product.
- KB67184 — Provides a recommended maintenance plan for your McAfee ePO database using SQL Server Management Studio.
- KB66616 — Provides a McAfee ePO server backup and disaster recovery procedure.
- KB75497 — Provides a McAfee ePO cluster backup and disaster recovery procedure.
- KB76739 — Provides a McAfee ePO 5.0 installation/patch upgrade checklist for known issues.

## Important McAfee KB articles

- KB59938 — Provides detailed version information for McAfee ePO
- KB51569 — McAfee ePO supported platforms, environments and operating systems on Microsoft Windows
- KB51109 — Lists every operating system supported by every McAfee product
- KB67184 — Provides a recommended maintenance plan for your McAfee ePO database using SQL Server Management Studio
- KB66616 — Provides a McAfee ePO server backup and disaster recovery procedure
- KB75497 — Provides a McAfee ePO cluster backup and disaster recovery procedure
- KB76739 — Provides a McAfee ePO 5.0 installation/patch upgrade checklist for known issues
- KB79169 — Supported Products and Extensions in McAfee ePO 5.1
- KB66797 — Ports needed to communicate through a firewall for McAfee ePO 4.x and 5.x
- PD24808 — Create and manage Permission Sets in McAfee ePO 5.1 (pages 55–58)
- KB79169 / KB76737 — McAfee ePO 5.x Supported & Unsupported Products
- KB61057 — Versions of Apache and Tomcat used by McAfee ePO
- KB79283 — How to move / transfer computers from one McAfee ePO server to another
- KB71370 — McAfee ePO Deployment on Virtual Platforms
- KB71298 — Feature dependencies between McAfee ePO and the McAfee Agentt
- KB56386 — Environmental requirements for agent deployment from the McAfee ePO server
- KB79696KB79696 — Unsupported product extensions disabled after upgrade to McAfee ePO 5.1
- KB71078 — Migrating McAfee ePO from a 32-bit to 64-bit system (or different installation path)
- KB54677 — McAfee managed product generated Event IDs in McAfee ePO
- KB79236 — McAfee ePO Agent Handlers require high bandwidth/high available network connection to the McAfee ePO database
- KB60112 — How to reset a password in McAfee ePO
- KB67184 — SQL-recommended maintenance plan using Server Management Studio
- KB67695 — SQL maintenance plan setup using Dbmaint utility
- KB76720 — How to identify why the McAfee ePO database is very large

- KB75055 — User Permissions needed for SQL Database
- KB77901 — Preventing McAfee ePO 5.x from automatically updating the AV engine
- KB56207 — Enabling log level 8 (detailed debug mode) for McAfee ePO Troubleshooting
- KB58966 — Enabling detailed debug mode for the McAfee Agent
- KB52369 — Enable detailed logging in the Orion Log
- KB68980 — Events not being processed — DB Events directory is very large
- KB72895 — Capturing a useful MER for McAfee ePO and the McAfee Agent
- KB53035 — Troubleshooting event and report content with McAfee ePO
- KB66909 — VirusScan Enterprise exclusions Master KB also has impact within McAfee ePO
- KB52634 — How to determine which patch is installed in McAfee ePO
- KB77534 — Version information for the McAfee Agent 4.8.x
- KB51573 — Supported environments for McAfee Agent 4.x

## Other informative articles

- SQL Storage Top 10 Best Practices — This link, from Microsoft SQL, provides a top 10 best practices for storage
- Microsoft SQL Server — This Microsoft SQL Server page provides information for several versions of SQL Server with articles on database and database application design, as well as examples of the SQL Server uses
- Comparing RAID Implementations for SQL — This Microsoft Developer page compares different implementations of RAID levels
- Microsoft SQL Technical Documentation — This Microsoft Developer page lists all SQL Technical Documentation and Technical Articles
- Is RAID 5 Really a Bargain? — This capacity planning article, by Cary Millsap (Hotsos LLC), compares RAID 1 and RAID 5
- Battle Against Any RAID Five-BAARF — This article provides many reasons not to use RAID 5 for redundancy in disk configuration

# Index