Best Practices Guide

McAfee ePolicy Orchestrator 5.0.0
Software
COPYRIGHT
Copyright © 2013 McAfee, Inc. Do not copy without permission.

TRADEMARK ATTRIBUTIONS
McAfee, the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundscore, Foundstone, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee Total Protection, TrustedSource, VirusScan, WaveSecure are trademarks or registered trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other names and brands may be claimed as the property of others.

Product and feature names and descriptions are subject to change without notice. Please visit mcafee.com for the most current products and features.

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

5 Managing endpoint security with policies and packages 47
Managing policies .......................................................... 47
McAfee Agent policy ...................................................... 48
  Configure an agent server communication interval ................. 49
  Send a policy change immediately .................................. 49
Deploy packages ............................................................ 50

6 Using client and server tasks in your managed environment 51
How client tasks deploy products ....................................... 51
  Product deployment workflows ...................................... 51
  Configuring product updates ........................................ 54
Modifying McAfee ePO with server tasks ............................. 56

7 Reporting with queries 57
Reporting features .......................................................... 57
How to use custom queries .............................................. 58
  Create custom event queries ....................................... 59
  How event summary queries work ................................ 64
  Create custom table queries ........................................ 70

Scaling your managed network

8 Using repositories and Agent Handlers 75
What repositories do ...................................................... 75
Repository types .......................................................... 76
  FTP repositories ....................................................... 76
  HTTP repositories .................................................... 77
  UNC share repositories ............................................. 77
  SuperAgent repositories ............................................. 77
Where to place repositories ............................................. 79
How many repositories do you need? ................................ 80
  Disable server Master Repository ................................ 82
  Calculating repository replication bandwidth .................... 83
  Calculating client updates bandwidth ............................ 84
  Global Updating restrictions ....................................... 85

Maintaining and optimizing your McAfee ePO software

9 Maintaining your McAfee ePO server 89
Monitoring server performance ........................................ 89
  Finding and using Performance Monitor .......................... 90
  Use "perfd" with ePolicy Orchestrator ............................. 91
  Check event processing .............................................. 92
Estimating and adjusting the ASCI .................................... 93
  Estimating the best ASCI ........................................... 93
  Configure the ASCI setting ........................................ 93
Maintaining your SQL database ........................................ 94
  Maintaining the McAfee ePO SQL database ....................... 94
Recommended tasks ..................................................... 96
  Recommended daily tasks .......................................... 97
  Recommended weekly tasks ....................................... 100
  Recommended monthly tasks .................................... 102
10 Automating and optimizing McAfee ePO workflow

Find systems with the same GUID ........................................ 105
Purging events automatically .................................................. 106
  Create a purge events server task ........................................ 106
  Purge events by query ....................................................... 108
Creating an automatic content pull and replication .................. 109
  Pull content automatically ................................................ 109
Confirm 1051 and 1059 events are filtered .............................. 111
  Filter 1051 and 1059 events .............................................. 111
Finding systems that need a new agent ................................. 112
  Create a new Agent Version Summary query with table output .... 112
  Create a Product Deployment project to update the McAfee Agents 113
Finding inactive systems ..................................................... 114
  Change the Inactive Agents query ...................................... 114
  Delete inactive systems ................................................... 115
Measuring malware events ................................................... 116
  Create a query that counts systems cleaned per week ............. 117
Finding malware events per subnet ........................................ 118
  Create a query to find malware events per subnet ................ 119
Automating DAT file testing .................................................. 119
  Pull and copy DAT updates from McAfee .............................. 120
  Create a test group of systems ......................................... 123
  Configure an agent policy for the test group ....................... 124
  Configure an on-demand scan of the test group ................... 124
  Schedule an on-demand scan of the test group ..................... 125
  Configure an Automatic Response if malware is detected in the test group .................................................. 126
Creating an automatic compliance query and report ................ 127
  Create a server task to run compliance queries .................... 128
  Create a report to include query output .............................. 130
  Create a server task to run and deliver a report .................. 130

11 Plan your disaster recovery .............................................. 133
Use Disaster Recovery .......................................................... 133
Use server clusters for disaster recovery .............................. 133
Use cold and hot spares on one physical site ......................... 134
Use cold and hot spares on two physical sites ......................... 134

A Getting more information .................................................. 137

Index ................................................................................. 139
Preface

This guide provides information about suggested best practices for using your McAfee® ePolicy Orchestrator® (McAfee ePO®) 5.0.0 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.

- **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 5.0. This document is not meant to be a comprehensive guide for all implementations. Instead, it should be used to assist in planning and maintaining your McAfee ePO managed environment.

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

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

Task

2. Under Self Service, access the type of information you need:

<table>
<thead>
<tr>
<th>To access...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>User documentation</td>
<td>1. Click Product Documentation.</td>
</tr>
<tr>
<td></td>
<td>2. Select a product, then select a version.</td>
</tr>
<tr>
<td>KnowledgeBase</td>
<td>• Click Search the KnowledgeBase for answers to your product questions.</td>
</tr>
<tr>
<td></td>
<td>• Click Browse the KnowledgeBase for articles listed by product and version.</td>
</tr>
</tbody>
</table>
Introduction

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

Contents

- How to use this guide
- Using McAfee ePO software in your network
- Components

How to use this guide

This document is one component of the McAfee ePO software documentation set and supplements the information in those documents.

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. See What's in this guide for a list of the other documents in the set.

You should use the information in this document during these four stages:

1. **Installing and configuring your McAfee ePO software** — Use these chapters:
   - Configuring your hardware
   - Installing and upgrading McAfee ePO software
   - Using the McAfee Agent and your System Tree

2. **Managing and reporting on your McAfee ePO environment** — Use these chapters:
   - Managing endpoint security with policies and packages
   - Using Client and Server tasks in your managed environment
   - Reporting on your managed environment with queries

3. **Scaling your McAfee ePO server managed network** — Using repositories and Agent Handlers

4. **Maintaining and optimizing your McAfee ePO software** — Use these chapters:
   - Maintaining McAfee ePO
   - Automating and optimizing McAfee ePO Workflow
   - Plan your Disaster recovery

See also

What's in this guide on page 8
Find product documentation on page 8
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 network 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.

• Using the built-in query system wizard, you can create reports that display informative user-configured charts and tables containing your network security data.

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

• Enforce policies on your endpoints

• Distributes McAfee software, including new products, upgrades, and patches

• Reports on your enterprise network 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 the data about your network managed systems, McAfee ePO, Agent Handlers, and repositories

3. **McAfee Agent installed in clients** — Provides policy enforcement, product deployments and updates

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 located on the same network segment as the McAfee ePO database.

9 **Ticketing system** — Connects to your McAfee ePO server to help manage your issues and tickets

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

Chapter 2  Configuring your hardware
Chapter 3  Installing and upgrading McAfee ePO software
Chapter 4  Using the McAfee Agent and your System Tree
Configuring your hardware

How you configure the McAfee ePO software is influenced by many factors, including the size of your network and the hardware you use.

Contents
- Server hardware requirements
- Planning your hardware configuration
- Planning your hard disk configuration
- Using a SAN with your SQL database

Server hardware requirements

Before you install the McAfee ePO software, you must determine the hardware requirements 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. That is not true. 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 distribution of content.

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 McAfee ePO servers 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.

When choosing the operating systems for your servers, you must use a 64-bit versions operating system for the McAfee ePO server. You can use either 32-bit or 64-bit versions for the SQL database server operating system.

The McAfee ePO server performance is determined by the SQL database, where the McAfee ePO server data is stored. The SQL 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.
<table>
<thead>
<tr>
<th>Node count</th>
<th>McAfee ePO server</th>
<th>SQL Server</th>
<th>Agent Handler</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CPU cores*</td>
<td>RAM (GB)</td>
<td>Hard drive (GB)</td>
<td>CPU cores*</td>
</tr>
<tr>
<td>&lt; 10,000</td>
<td>4</td>
<td>8</td>
<td>20</td>
<td>4</td>
</tr>
<tr>
<td>10,000–25,000</td>
<td>4</td>
<td>8–16</td>
<td>20–40</td>
<td>4</td>
</tr>
<tr>
<td>25,000–75,000</td>
<td>8</td>
<td>16–32</td>
<td>20–40</td>
<td>8</td>
</tr>
<tr>
<td>75,000–150,000</td>
<td>8</td>
<td>32–64</td>
<td>40–80</td>
<td>16</td>
</tr>
<tr>
<td>150,000+</td>
<td>16</td>
<td>64–128</td>
<td>40–80</td>
<td>32+</td>
</tr>
</tbody>
</table>

* These are physical Quad CPUs running at 2.2 GHz and 7.2 Gigatransfers per second (GT/s)

** Estimated event load for six 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.

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**

You can reduce hardware costs in an organization with fewer than 10,000 nodes by installing the McAfee ePO server and SQL database on the same physical server. This organization is easily managed by the McAfee ePO server and offers room for growth. You can also have multiple McAfee products deployed in the environment, such as McAfee® VirusScan® Enterprise (VSE) and McAfee® Host Intrusion Prevention (HIPS).
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 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 Database engine is limited to 1 GB.

The hardware used for McAfee ePO server and SQL database must be up-to-date hardware with these minimum requirements:

- 4 Quad processor CPUs
- 8 GB of RAM
- 20 GB of free hard drive space

**Example 2 — 10,000 to 75,000 nodes**

You can use a single McAfee ePO server to manage an organization ranging from 10,000 to 25,000 nodes with properly placed repositories to update content and software to the agents.

As your node count approaches 25,000 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 10,000 to 75,000 nodes with the servers on different hardware.

Figure 2-2   McAfee ePO network components for 10,000 to 75,000 nodes

In this figure the 10,000 to 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.

McAfee ePO server minimum hardware:
- Quad processor CPU
- 8 to 32 GB of RAM
- 20 to 40 GB of hard drive space

SQL Server minimum hardware:
- 16 Quad processor CPUs
- 8 to 32 GB of RAM
- 0.5 to 1.0 TB of hard drive space

**Example 3 — 75,000 to 150,000 nodes**

You can manage an organization ranging from 75,000 to 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 to 150,000 nodes.

Figure 2-3  75,000 to 150,000 node McAfee ePO network components

This 75,000 to 150,000 node organization example includes:

1. The McAfee ePO server
2. Separate SQL Server
3. Separate McAfee ePO Agent Handler 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.

McAfee recommends that you install a second Agent Handler, installed at a remote site, for redundancy, and leave the McAfee ePO server as a last resort, for an organization with 75,000 to 150,000 nodes.

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

McAfee ePO server minimum hardware:
- 8 Quad processor CPUs
- 32 to 64 GB of RAM
- 40 to 80 GB of hard drive space

SQL Server minimum hardware:
• 16 Quad processor CPUs
• 32 to 128 GB of RAM
• 1.0 to 2.0 TB of hard drive space

Agent Handler minimum hardware:
• 4 Quad processor CPUs
• 8 GB of RAM
• 40 to 80 GB of hard drive space

**Example 4 — 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.

McAfee ePO server minimum hardware:
• 16 Quad processor CPUs
• 64 to 128 GB of RAM
• 40 to 80 GB of hard drive space

SQL Server minimum hardware:
• 32 Quad processor CPUs
• 64 to 128 GB of RAM
• 1.0 to 2.0 TB of hard drive space

Agent Handler minimum hardware:
• 4 Quad processor CPUs
• 8 GB of RAM
• 40 to 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 75*
*Planning your hard disk configuration on page 22*
*Using a SAN with your SQL database on page 25*
*Sharing the SQL database hardware on page 22*
*Server hardware requirements on page 15*
Planning you hardware configuration

The physical hardware configuration you use for the McAfee ePO server and SQL Server is determined primarily by 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 and Host Intrusion Prevention.

If in the future you plan to manage more McAfee products and to add many more nodes, split the one server into two physical servers, one dedicated to the McAfee ePO server and the other for the SQL Server.

See also
Planning your hard disk configuration on page 22

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.

<table>
<thead>
<tr>
<th>Node count</th>
<th>McAfee ePO and SQL on one server</th>
<th>Use VM server</th>
<th>McAfee ePO DB on shared SQL Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>100–5,000</td>
<td>OK</td>
<td>Optional</td>
<td>Optional</td>
</tr>
<tr>
<td>5,000–25,000</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
</tr>
<tr>
<td>25,000–75,000</td>
<td>Not recommended</td>
<td>Not recommended</td>
<td>Not recommended</td>
</tr>
<tr>
<td>75,000 or more</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

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 now you might have only 5,000 nodes to manage 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 two servers.

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 ASCIs per second than the RAID 5 server when using the same hardware.

Example 2 — 5,000 to 10,000 nodes

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

- Operating system
- McAfee ePO
- SQL database
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 2-5  Disk partition and RAID configuration for 5,000 to 10,000 nodes**

**Example 3 — 10,000 to 75,000 nodes**

If you have 10,000 to 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 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 with individual partitions for the SQL database (the MDF file) and the SQL transaction log (the LDF file).
- RAID 1 for the log partition
- RAID 10 for the 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.

**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 ePO application

For the Agent Handler server, use:
- RAID 1 for the operating system
- RAID 10 for the ePO application

For the SQL Server, use:
- RAID 1 for the operating system, and provide individual partitions for the SQL database (the MDF file), the SQL transaction log (the LDF file), and the SQL Temp database
- RAID 10 for the 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.

---

**Using a SAN with your SQL database**

Storage area network (SAN) devices are the standard configuration for SQL databases that require backup 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 should be understood.

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 assist in planning 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 often without causing an excessive number of transactions on the SAN.

- **Tier 3 SAN** — Used for databases that do not require much space or many I/O transactions.
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
- Upgrading an existing McAfee ePO server
- Moving the server
- Moving agents between servers

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 Software 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 4.5 or 4.6 32-bit operating system version to 5.0 or later 64-bit operating system, use the Upgrade Compatibility Utility. See the McAfee ePolicy Orchestrator Software Installation Guide for details about this 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.

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 a 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. This includes your SQL database and any McAfee Agent keys. For detailed backup procedures, see KnowledgeBase article KB66616 and for detailed McAfee ePO Cluster Backup and Disaster Recovery procedures, see KnowledgeBase article KB75497.

• Make any hardware changes or remove any repositories that you want to decommission.

• Make sure that your hardware and bandwidth meet these minimum requirements before upgrading.

• Confirm 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. If the task is not in use remove it.

• Validate your tree and remove any agents that have not communicated with the McAfee ePO server in 14 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 ePO McAfee Agent installed.

• Purge events that are not needed. Try to delete any events older than 60 days.
• Backup, re-index, and check your disk space on the SQL Server. Confirm 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 KB67184.

• Remove old versions of software that you are not using. For example, patches for older versions of products that are no longer used.

  Replicate those patches to your distributed repositories prior to upgrading.

• 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 install the McAfee ePO server software on a VM, link it to your existing SQL database, and confirm the installation works.

• Validate all your settings to confirm that they are in place after the upgrade.

  For a McAfee ePO 5.0 installation and patch upgrade checklist for known issues, see KnowledgeBase article KB76739.

Using product version numbers
The product version numbers help you determine what software products, new patches, and hotfixes to install. These products, patches, and hotfixes are released by McAfee on a regular basis. As with all software products new patches and hotfixes are released on a regular basis 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 "5.0.0.1160" as an example, the number:
• 5. — "5" indicates a major release version
• 5.0. — The first "0" indicates a minor version, with "0" indicating it is the first releases of a version 5 product.
• 5.0.0. — The second "0" indicates it the patch number, in this case, it also means no patch.
• 5.0.0.1160 — 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 server and the McAfee Agent. Many users assume that the McAfee Agent version number must match the McAfee ePO server version number. This is not true.

The agent and server versions are disjointed and do not have to be on the same major version. For example, the McAfee ePO server 5.0 works fine with McAfee Agent 4.6 or 4.8.

  There are limits to how far back the McAfee ePO server supports McAfee 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 need to move your McAfee ePO server from one physical server to another, you can maintain all of your settings.

For example, you might want to move your McAfee ePO server configuration to new server hardware if the 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.

Manually moving your McAfee ePO server

The backup and disaster recovery process for McAfee ePO servers is described in KnowledgeBase article 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.

• These items that are outside your database:
  • McAfee Agent keys that secure the communication between the server and all of your agents
  • Software checked into the Master Repository
  • Extensions to manage all your product policies
  • Secure Sockets Layer (SSL) certificates
  • Server settings such as communication ports

After you have backed up all of 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. This is the ideal situation and reduces any potential problems.

However, the DNS name or IP address might need to be changed. For example, if you are changing the IP scheme a new IP address might be required, or if you change the DNS name and keep the old IP address you have to 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:
Moving agents between servers

If you need to create a new 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 between copying your existing McAfee ePO SQL database to your new McAfee ePO server and having the McAfee Agents 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:

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

Exporting and importing the ASSC keys

After you install all the 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 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 4.5 or later.

The Transfer Systems task allows you to:
• 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 make changes on 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.

**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** | **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**.

![Figure 3-1 System Tree Transfer Systems example](image)

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

Once a managed system is marked 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.
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
- Deploying agents
- What the System Tree does

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 5.0.

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 hot fixes
• 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.

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 solutions. 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. All those items are controlled by the McAfee Agent. 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 have the flexibility to choose which products fit your organization instead of being dictated by your security vendor.
• You can add controlled patching of individual products. For example, if there is a patch for the Endpoint Encryption product, VirusScan Enterprise cannot be affected by the patch.
• The patch process is consistent across all products because the McAfee ePO server controls the process.

Figure 4-1 One McAfee Agent communicates with many products
• You 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. Your custom package 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.

![Figure 4-2 McAfee Agent internal file structure](image)

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
- Manual execution
- A logon script
- The McAfee ePO server
- An image that includes the McAfee Agent
- Third-party tools

See the *McAfee ePolicy Orchestrator Product Guide* for details about these deployment methods.

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 McAfee Agent executable, such as the SiteList.XML file, that
are unique to your environment, which is why the McAfee Agent file can only be obtained from your organization's McAfee ePO server. You cannot download a generic McAfee Agent from the McAfee download site and deploy it.

**Tasks**

- *Creating the McAfee Agent file on page 36*
  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 40*
  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 pane, click System Tree Actions | New Systems.
2. From the New Systems dialog box, click Create and download agent installation package, then click OK.

![Figure 4-3  Create agent file from the System Tree](image)

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.](image)

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 ePolicy Orchestrator 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.

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 per day. This process requires the following:
The systems in your AD tree must be well maintained. This 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, have the admin$ share enabled, and there must be 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.

![Figure 4-4 System Tree systems list showing shell systems](image)

Shell systems appear in the previous 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.

On a regular basis delete these shell systems using a McAfee ePO server task, if needed.
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** | **System Tree**.
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 specific ones only.

   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 login 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 to make sure that all your systems get a McAfee Agent installed.

To obtain complete McAfee ePO compliance requires planning and communication with your build team to ensure that the McAfee Agent is part of every system from the beginning. That also ensures any required McAfee product and associated policy is pulled from the McAfee ePO server by the McAfee Agent on your systems. This ensures maximum coverage and is imperative for environment security.

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.

To install all the endpoint products on your managed systems you can either:

- Let the McAfee Agent automatically call in to the McAfee ePO server within 10 minutes and receive whatever policy and products are dictated by McAfee ePO.

- You can make 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.](image)

Here are some pointers to help you decided 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.

- If your build process occurs on a network where your imaged systems do not have network connectivity to the McAfee ePO server, make the endpoint products part of your imaging process.

- Once you install the McAfee Agent on a client, even though the first agent-server communication occurs almost immediately, it takes several more minutes to download, install, and update the VirusScan Enterprise product using a client task. If timing is a concern, and you don’t want to wait 15 or 20 minutes for the products to install, make the McAfee products part of your image.
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*, it can cause one of the most common problems seen in McAfee ePO, not resetting the McAfee Agent global unique identifier (GUID). This causes the systems to not appear in the System Tree.

To solve this problem, you must 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 will use the same GUID. This has a very negative effect in your environment. See the *McAfee ePolicy Orchestrator 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 Agent GUIDs if the computers are not displayed in the McAfee ePO directory. See KnowledgeBase article KB56086 for details.

**See also**

*Find systems with the same GUID on page 105*

**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
- BMC Client Automation (formerly Marimba)
- Simple logon scripts
- Novell Zenworks

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

The McAfee Agent file, named FramePkg.exe, has several installation switches. At a minimum you need to tell the McAfee Agent to install itself. 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 configuration 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.

This is an ideal option if your AD structure is nicely 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.

Chapter 5  Managing endpoint security with policies and packages
Chapter 6  Using client and server tasks in your managed environment
Chapter 7  Reporting with queries
Managing endpoint security with policies and packages

Policies are the settings that govern each product on the endpoint. Packages are the binaries that can be deployed by the McAfee Agent to your endpoints.

Policies include the settings for any supported products from McAfee 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. This includes deploying a full product, such as, a new version of VirusScan Enterprise or McAfee SiteAdvisor 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 you have to deploy VirusScan Enterprise with McAfee ePO.

Contents

- Managing policies
- McAfee Agent policy
- Deploy packages

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

![System Tree Assigned Policies products list](image)

**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) web page.

*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 of 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 System. Less complex policies can apply to all systems, for example the McAfee Agent policies govern all the 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* for details about the McAfee Agent policy default settings.

**See also**

*Estimating and adjusting the ASCI* on page 93
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

For example, if a change is made to a policy for a point-product managed by McAfee ePO at the ASCI time, that change is pulled down by the agent and applied 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 ASCI 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 | 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 Get 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 the McAfee ePO server to 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 can be deployed to an endpoint. All packages that can be deployed 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 in to 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.
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
- Modifying McAfee ePO with server tasks

How client tasks deploy products

Client tasks run on the clients to deploy products and are typically scheduled to run at a specific time. 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, if you have their extensions checked in to McAfee ePO. But the major tasks dedicated to the McAfee Agent are:

- **Product deployment** — Tells the agent which products you want it to deploy to the client
- **Product update** — Uses the McAfee Agent 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 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 52
- Estimating the best ASCI on page 93

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

Figure 6-1 Deploy Products project page

- 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 into 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. To keep that repository from being overwhelmed, you must randomize your deployment.

To find out the exact size of your repository you can check the installation folder where the McAfee ePO server is located under C:\Program Files(X86)\McAfee\ePolicy Orchestrator\DB\Software.

Many customers forget to enable randomization on their tasks and choose a specific time for their task to run such as noon on a daily basis. If you haven’t configured randomization and you deploy a product or signature update at noon on a daily basis, this generates a significant spike in traffic to your repositories at that exact time. This could impact network performance.

Randomization is critical to any client task that uses bandwidth. 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 8.8, which is 56 MB, deployed to 1,000 nodes, pulled across 3 repositories, equals about 56 GB of data. That 56 GB of data is being pulled across three repositories which equals about 19 GB per repository.

\[56 \text{ MB (VSE)} \times 1,000 \text{ (nodes)} = 56 \text{ GB (total)} / 3 \text{ (repositories)} = \text{approximately 19 GB per repository}\]

The following formula calculates the bandwidth needed 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.

\[19 \text{ GB (per repository)} / 9 \text{ (hours)} = \text{approximately 2.1 GB per hour}\]
Configuring 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 Assignment, then click My Organization in the System Tree pane.

2. From the Assigned Client Task page, click Actions | New Client Task Assignment.

3. From the System Tree Client Task Assignment Builder page, select the following and click Next:
   • Under Product, select McAfee Agent
   • Under Task Type, select Product Update
   • Under Task Name, select Create New Task

4. In the System Tree, Client Task Catalog : New Task page:
   • Type a task name, for example Daily Master Updates, and a description.
   • Click Selected packages, for example, select Engine and DAT.
   • Click Save.

This is an example of a Daily Master Update task that downloads the VirusScan Enterprise DAT and engine files.

![Figure 6-3 Client Task Assignment Builder with packages selected](image)
5 Back in the Client Task Assignment Builder page, click Assign in the client task that you just created.

6 Under Select a group to assign the task, select My Organization, or the group where you want the client task assigned, then click OK.

7 In 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.

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.

See also
Automating DAT file testing on page 119
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.

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 means 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 on a regular basis
- 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 116
- Creating an automatic content pull and replication on page 109
- Purging events automatically on page 106
- Finding inactive systems on page 114
- Create a server task to run compliance queries on page 128
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 into your McAfee ePO system.

Contents

- Reporting features
- How to use custom queries

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.

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 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.

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

**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:

- You can determine exactly which kind of query that you want to create before you create it.
- 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 is very 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 Query. 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 into 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**.
• **Managed Systems** — In the Feature Group, select **System Management**. Under Result Types, select **Managed Systems**.

![Query Builder with Managed Systems selected](image)

**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 Labels selection list](image)

**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**.

![Query Builder Columns selection](image)

**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 laptop or desktop systems
- Only specific operating system platforms. For example, servers or workstations.
- Only systems that have an older DAT version
• Only 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.

Figure 7-6  Query Builder Filters selection
5 Click **Next** to not create any filters and display all of the operating system types.

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

![Figure 7-7 Query Builder Edit Query option](image)

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 the 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 106*
**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 Query**.

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

![Figure 7-8 Query Builder with Client Events selected](image)

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 **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.

![Query Builder output](image)

**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 Query**.
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**.

![Query Builder with Threat Events selected](image)

**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 KB54677.

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

The McAfee ePO server displays approximately 8,000 threat events total.

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

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

\[(10,000 \text{ nodes}) \times (1 \text{ to } 2 \text{ million events}) = \text{estimated number of events}\]

For example, if you have 50,000 nodes, your range is 5 to 10 million total client and threat events.

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 the Purging events automatically section?
- 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 because 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 there a few access protection rules are being triggered repeatedly on VirusScan Enterprise, as shown in this figure.

![Query wizard output showing drill down of Access Protection rule](image)

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

At this point, determine whether these are important events in your organization that 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 the Event summary queries and Purge events automatically.

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 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 108
- Purging events automatically on page 106
- How event summary queries work on page 64
- Filter 1051 and 1059 events on page 111
- Confirm 1051 and 1059 events are filtered on page 111
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 Query.
2. Click Events in the Features Group and Client Events in the Result Type.
3. In the Display Results As pane, click List, then click Table, then click Next.

![Query Builder showing table format selected](image)

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.

![Query Builder with Event ID filter](image)

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

6 Click the plus sign, +, at the right to add another comparison row, add 1051 and 1059 in the Value column, then click Run.

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

![Query Builder output](image)

**Figure 7-15** Query Builder output

7 (Optional) You can select all of these 1051 and 1059 events, then click Actions | Purge to purge them in real time.

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 Create a new server task and give it an appropriate name.

For example, Purge of 1051 and 1059 Events Nightly.

9 Click Purge Threat Event Log from the Actions list, then click Purge by Query.
10 In the list, find and click the custom query that you just created.

![Figure 7-16  Query Builder with Purge Threat Event Log selected](image)

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

**See also**
*Confirm 1051 and 1059 events are filtered* on page 111
*Purging events automatically* on page 106
Scaling your managed network

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

Distributed repositories work as file shares that store and distribute security content for your managed client systems. Agent Handlers distribute agent-server communication by directing managed systems to report to a specific Agent Handler instead of connecting to the McAfee ePO server.

Repositories and Agent Handlers play an important role in your McAfee ePO infrastructure. How you configure them and deploy them depends on your environment.

Contents

- What repositories do
- Repository types
- Where to place repositories
- How many repositories do you need?
- Global Updating restrictions

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 be deployed to your clients
- Security content such as DATs and signatures
- Patches and any other software needed to carry out the 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 certain protocols be used 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 77

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:
• Generally 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 very 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, this 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.

All of 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 agents in its network subnet. 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.

The McAfee ePolicy Orchestrator Product Guide provides detailed information about SuperAgents and how to configure them.

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 a new SuperAgent policy**

To convert client systems to SuperAgents, you must assign a SuperAgent policy to those systems.

**Task**

1. Click *Menu* | *Policy* | *Policy Catalog*, then from the *Product* drop-down menu, select *McAfee Agent*, and from the *Category* drop-down menu, select *General*.
2. Click the *My Default* policy to start editing the policy. If you want to create a policy, click *Actions* | *New Policy*.
   
   The *McAfee Default* policy cannot be modified.
3. From the *General* tab, select *Convert agents to SuperAgents* to convert the agent to a SuperAgent and update its repository with the latest content.
4. 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*.
5. Select *Enable Lazy caching* to allow SuperAgents to cache content when it is received from the McAfee ePO server.
6. 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**

1. Select *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 SuperAgents 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 **Assign Policies** tab, then select **McAfee Agent** from the Product list.

2. From the **Actions** column for the **General** category, click **Edit Assignments**.

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. This converts 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.

   ![Info](Before the system appears as a SuperAgent in the group two ASCI 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 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 are located.

To answer these questions you need to 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 McAfee VirusScan 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 System 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.
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 need to download those daily DAT files.

### Example 1: Downloading directly from the central ePO server

To download the daily DAT file randomly from the central 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.

## 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.

The following table is an estimate of the updates a repository can handle and the hardware needed. These specifications can be influenced by many factors, for example how you update content, products, and patches.

<table>
<thead>
<tr>
<th>Server hardware</th>
<th>Nodes updated</th>
<th>Dedicated or shared client hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single 3 GHz processor with 4 GB of memory</td>
<td>3,000</td>
<td>Shared with other applications</td>
</tr>
<tr>
<td>Single 3 GHz processor with 4 GB of memory</td>
<td>3,000–7,000</td>
<td>Dedicated</td>
</tr>
<tr>
<td>Server class hardware, dual-quad processor and 8 GB of RAM</td>
<td>5,000–7,000</td>
<td>Dedicated</td>
</tr>
</tbody>
</table>

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 Endpoint Encryption, SiteAdvisor, and Policy Auditor, your repository disk space is in the 1 GB range.

To find out the exact size of your repository you can check the installation folder where the McAfee ePO server is located under C:\Program Files(X86)\McAfee\ePolicy Orchestrator\DB\Software.

These examples provide some examples of three common organization sizes and their repository size.

### Example 1 — 3,000 node organization with one office

An organization with 3,000 nodes of workstations and servers, uses McAfee VirusScan Enterprise, Host Intrusion Prevention System, Encryption, and Host Data Loss Protection. It 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 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 to 20,000 node organization with four offices**

An organization with 15,000 to 20,000 nodes, has one data center in New York where all traffic destined for the Internet must be routed. Four offices in the U.S. located in New York, San Francisco, Dallas, and Orlando. Each office has approximately 3,000 to 4,000 nodes with 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 Endpoint Encryption, VirusScan Enterprise, Host Intrusion Prevention System, 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 Agents 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 to 60,000 node organization with multiple global offices**

An organization with 40,000 to 60,000 nodes, distributed across three major regions of the U.S. offices, has one data center in New York and three additional offices across the country. Each office has approximately 7,000 nodes.

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 one McAfee ePO server resides in the UK data center and runs VirusScan Enterprise, Host Intrusion Prevention System, and SiteAdvisor.

The APAC offices include two smaller offices.

<table>
<thead>
<tr>
<th>Region</th>
<th>Office</th>
<th>Number of nodes</th>
<th>Servers</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S.</td>
<td>New York, Data Center</td>
<td>7,000</td>
<td>Repository</td>
</tr>
<tr>
<td>U.S.</td>
<td>Office 1</td>
<td>5,000</td>
<td>Repository</td>
</tr>
<tr>
<td>U.S.</td>
<td>Office 2</td>
<td>6,000</td>
<td>Repository</td>
</tr>
<tr>
<td>U.S.</td>
<td>Office 3</td>
<td>5,000</td>
<td>Repository</td>
</tr>
<tr>
<td>EMEA</td>
<td>U.K., Data Center</td>
<td>3,000</td>
<td>McAfee ePO server</td>
</tr>
<tr>
<td>EMEA</td>
<td>Office 1</td>
<td>200</td>
<td>Repository</td>
</tr>
<tr>
<td>EMEA</td>
<td>Office 2</td>
<td>1,000</td>
<td>Repository</td>
</tr>
<tr>
<td>EMEA</td>
<td>Office 3</td>
<td>3,000</td>
<td>Repository</td>
</tr>
<tr>
<td>APAC</td>
<td>Office 1</td>
<td>500</td>
<td>Repository</td>
</tr>
<tr>
<td>APAC</td>
<td>Office 2</td>
<td>300</td>
<td>Repository</td>
</tr>
</tbody>
</table>

**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 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 UK. Plus these WAN links are already saturated with traffic. This means replication from the McAfee ePO server to an APAC repository is not feasible unless it is done during off hours. This is a reasonable option 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 the UK. 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 our 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. And 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 very 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 specifically created for local access. Making this change forces the agents to use only the repositories you created manually. You can specify which repositories agents should access when selecting a repository within a policy.

In smaller environments, where fewer nodes are managed, there’s no need to make this change. The server can handle all of these tasks without impacting performance.

You can use the Policy Catalog to disable the McAfee ePO server repository.
**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 Agents**, then from the Category list, select **Repositories**, 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.

![Repositories with McAfee ePO server disabled](image)

**Figure 8-1** 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.

**Calculating repository replication bandwidth**

Replication consumes valuable bandwidth in all environments. Before you install repositories, calculate the bandwidth required for the replication.

If you are only replicating DAT files, the bandwidth use will be approximately 70 Mb of replication per day. Agents don’t use all the 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. In order to determine if you need a repository in a specific location, you must determine what is more costly in terms of bandwidth usage; replicating 70 Mb worth of data to a repository, or telling the agents to go to the next nearest repository that might not be located near the agents.
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.

At a minimum, each of your clients must download, on average, 400 KB per day for DAT files. The following examples show how to calculate the bandwidth used for the client updates using this formula:

\[(\text{Size of update file}) \times (\text{Number of nodes}) = \text{Amount of data pulled per day}\]

The following examples use this formula to calculate the amount of data pulled per day and describe if creating a local repository reduces the bandwidth.

**Example 1 — A small office in India**

The small office in India needs to download the 400 KB per day for DAT files to its 200 nodes. Using the formula:

\[(400 \text{ KB}) \times (200 \text{ nodes}) = \text{approximately 80 MB of data randomly pulled per day to India}\]

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 per day over a slow WAN link can negatively impact 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 office 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 needs to download the 400 KB per day for DAT files to its 4,000 nodes. Use the formula:

\[(400 \text{ KB}) \times (4,000 \text{ nodes}) = \text{approximately 1.6 GB of data randomly pulled per day to Tokyo}\]

In the large office in Tokyo with 4,000 nodes uses 1.6 GB of bandwidth per day just to update the DAT files alone. Because replication of the DAT file to Tokyo only uses 70 MB of bandwidth per day it is much more efficient to have a repository in the Tokyo office so all DATs can be 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 needs to download a 23 MB patch update for VirusScan Enterprise to its 1,000 nodes. Use the formula:

\[(23 \text{ MB}) \times (1,000 \text{ nodes}) = \text{approximately 23 GB of data pulled to the New York City office}\]

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 needs to 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 to 300 nodes it cannot benefit from the bandwidth saved using a repository. If there is no local repository, the agents will 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 since 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 would be more efficient to place a repository temporarily at a smaller site so the client's software can download the 56 MB file locally. Then disable this repository once the client is rolled out.

To find out the exact size of your repository you can check the installation folder where the McAfee ePO server is located under C:\Program Files(X86)\McAfee\ePolicy Orchestrator\DB\Software.

See also
How client tasks deploy products on page 51
Product deployment workflows on page 51

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. This is great if you have a smaller environment (fewer than 1,000 nodes) with no WAN links. Global Updating generates a lot 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.

Global Updating is disabled by default when you install McAfee ePO software.

To confirm that the Global Updating setting, click Menu | Configuration | Server Settings and select Global Updating from the Setting Categories list. Confirm that 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 typically occurs twice per 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 can saturate your WAN links and roll out an engine that you might preferred to upgrade in a staged release.

How Global Updates 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.
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.
Maintaining your McAfee ePO server

Generally your McAfee ePO server should not require periodic maintenance, but if your server performance changes, you should take these steps before calling technical support.

- The SQL database used by the McAfee ePO server requires regular maintenance and backups to ensure that McAfee ePO functions correctly.

Contents
- Monitoring server performance
- Estimating and adjusting the ASCI
- Maintaining your SQL database
- Recommended tasks

Monitoring server performance
You can periodically check to see 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 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 used?
- Is the CPU overutilized?

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 extremely 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 Start Performance Monitor for McAfee ePO topic.

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 90

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 is an example of the McAfee ePO Server counters.

![Windows Performance Monitor showing the ePolicy Orchestrator Server counters](image)

Figure 9-1 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**


2. In the Add Counters list, browse, or scroll down to the ePolicy Orchestrator Server counters selection, then click the + to expand the list of counters.

3. Click Add to move the selected counter into the Added counters list, then click OK.

   For example, add the Open ePO Agent Connections. This 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. 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
   - Static event queue length

This example shows the output of the McAfee ePO counters.

![Figure 9-2 Windows Performance Monitor showing McAfee ePO processor time](image)

These are just a few of the tests you can perform with the McAfee ePO server using the Windows 32-bit Performance Monitor. For additional Windows Performance Monitor information, see these websites:
Check event processing

The number of events appearing in the ePolicy Orchestrator database events folder could indicate the performance of your McAfee ePO server.

**Task**

For option definitions, click ? in the interface.

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 very quickly.

   This is an example of the ePolicy Orchestrator Events folder.

   ![Figure 9-3  ePolicy Orchestrator Events folder](image)

   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 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 this probably indicates a performance issue.](image)
Estimating and adjusting the ASCI

You might need to estimate and adjust the agent-server communication interval (ASCI) on your network, depending on your number of systems in your managed environment.

Estimating the best ASCI

To improve your McAfee ePO server performance, you might need to adjust the ASCI setting for your managed network.

To determine if you should change your ASCI, ask how often changes occur for 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 ASCI, then checks again at its next scheduled check-in time.

To estimate your ASCI, your concern is not wasting bandwidth because ASCI communications are only a few kilobytes per ASCI. 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 per 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 ASCI 60 minutes setting to about the 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.

You can determine how many connections are being made to your McAfee ePO server by using the ePO Performance Counters.

This table lists basic ASCI guidelines.

<table>
<thead>
<tr>
<th>Node count</th>
<th>Recommended ASCI interval</th>
</tr>
</thead>
<tbody>
<tr>
<td>100–10,000</td>
<td>60–120 minutes</td>
</tr>
<tr>
<td>10,000–50,000</td>
<td>120–240 minutes</td>
</tr>
<tr>
<td>50,000 or more</td>
<td>240–360 minutes</td>
</tr>
</tbody>
</table>

See also

Monitoring server performance on page 89

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. In Agent-to-server communication and next to Agent-to-server communication interval, type the number of minutes between updates.

   This example shows the Agent-to-server communication interval set to 60 minutes.

![Figure 9-4 Policy Catalog Agent-to-server communication interval configuration](image)

4. Click Save.

   If you need to send a policy change or add a client task immediately, you execute an agent wake-up call.

See also
Send a policy change immediately on page 49

Maintaining your SQL database

To help the McAfee ePO server to function correctly, you must have a well performing SQL database. It is the central storage place for all of the data your McAfee ePO server uses, and it requires maintenance.

Maintaining the McAfee ePO SQL database

The SQL database requires regular maintenance and backups to ensure that McAfee ePO functions correctly.

The McAfee ePO SQL database houses everything that McAfee ePO needs to function; your System Tree structure, policies, administrators, client tasks, and configuration settings.

Perform these tasks on a regular basis to maintain your SQL Server:
• Regularly back up the McAfee ePO SQL database and its transaction log.
• Reindex your database on a regular basis.
• Rebuild your database on a regular basis.
• Purge older events using server tasks as described in Purging events automatically.

Back up your SQL database regularly, in case your SQL database or your McAfee ePO server environment fails. These backups ensure that, if the McAfee ePO server needs to be rebuilt or restored, a safe and current copy is available to restore from. Plus, 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 backup 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 point to several pages scattered throughout the book. You must then scan each page for the specific information you are looking for.

This is significantly 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.

In the case 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 need to occasionally re-sort the data to re-create the phone book order. This is where re-indexing 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 on a daily basis.

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 re-indexing as part of your regular backup schedule to combine everything in one task.

Do not shrink your database. This is a common mistake that many administrators do when building their maintenance task.

Learn more

For details about creating your maintenance task, see KnowledgeBase article 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 website, found at http://www.sql-server-performance.com/articles/dba/dt_dbcc_showcontig_p1.aspx.

To learn more about maintaining and optimizing your SQL database, see the document Improving ePO Performance by Optimizing SQL.
Recommended tasks

McAfee recommends that you perform certain tasks daily, weekly, and monthly to ensure that your McAfee ePO 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

You should perform these McAfee recommended tasks at least once per day to ensure that your McAfee ePO server-managed network systems are safe from threats and your server is functioning normally.

![Diagram of daily operations tasks]

- **Threat tasks**
  - Check ePolicy Orchestrator Dashboards for threat events
  - Examine product specific reports, such as those for VSE 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

- **Security maintenance tasks**
  - 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 9-5 Suggested McAfee ePO daily tasks](image)

Each of the recommended daily tasks is described in more detail in this table.

> Where indicated, some of these tasks can be automated. Those instructions are included in this guide.

### Table 9-1 Recommended McAfee ePO daily tasks details

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat tasks to perform daily</td>
<td>Throughout the day review your dashboards for threats, detections, and trends. Setup automated responses to send emails to administrators when threat activity thresholds are met.</td>
</tr>
</tbody>
</table>
### Table 9-1  Recommended McAfee ePO daily tasks details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Examine product-specific reports for threat events, such as VSE or HIPS</td>
<td>Examine reports for any events that might point to 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 need to create new policies or edit existing policies. Examine reports to determine the status of HIPS services, and ensure that the VirusScan McShield service is enabled. See VirusScan Enterprise 8.8 Patch 1, 2, and 3 Hotfix 820636 to implement the proper On-Access Scan (OAS) status.</td>
</tr>
</tbody>
</table>
| 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. Run queries, or review dashboards periodically to check for alerts collected from you managed devices. Also watch for these threat signs:  
  • High CPU usage on undetermined processes  
  • Unusually high increases in network traffic  
  • Services added or deleted by someone other than you  
  • Inability to access network or administrative shares  
  • Applications or files that stop functioning  
  • Unknown registry keys added to launch an application  
  • Any browser home page that changed outside your control                                                        |
| Review the McAfee Labs Threat site once, or multiple times, per 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. This might reveal weaknesses in the network, where policies need to be adjusted. |

#### Security maintenance tasks

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Examine the DAT deployment reports</td>
<td>It is very 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 that attempts to update their DAT file frequently.</td>
</tr>
<tr>
<td>Check compliance queries and reports</td>
<td>In Queries &amp; Reports, find the compliance queries that identify systems that have not updated a product, such as VSE, with a hotfix or locate patch. Create a process to make sure that systems are up to date. For example, run an update or deployment task to ensure compliance.</td>
</tr>
</tbody>
</table>

> Out of compliance system numbers drop until all systems have checked in and updated their software.
Table 9-1 Recommended McAfee ePO daily tasks details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review the inactive agents log to see if systems are not reporting to McAfee ePO</td>
<td>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. For example, you can use this task to move the inactive systems to a new group in the System Tree, tag the systems, delete the systems, or email a report. If the systems are on the network, but having difficulty checking into the McAfee ePO server, you might need to perform one of these actions: • Re-install the McAfee Agent to ensure that the system is communicating with the McAfee ePO server. • 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.</td>
</tr>
<tr>
<td>Ensure that Active Directory or NT Synchronization is working</td>
<td>If you use Active Directory or NT Domain synchronization to pull in a list of new systems and containers that need to be managed by McAfee ePO, confirm that the Sync task can be configured to run at least once per day and is working. If the synchronization fails, systems are vulnerable on the network and pose a major risk for infection.</td>
</tr>
<tr>
<td>Confirm that a Memory Process Scan occurs at least daily</td>
<td>Using the Threats Dashboard, confirm the results of these scans don’t indicate an increase in threats. Run memory process scans frequently, because they are quick and unobtrusive.</td>
</tr>
<tr>
<td>Check Rogue System Detection</td>
<td>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.</td>
</tr>
</tbody>
</table>

See also
*Configure an Automatic Response if malware is detected in the test group on page 126*
*Finding inactive systems on page 114*
**Recommended weekly tasks**

You should perform the McAfee suggested tasks at least once per week to ensure that your McAfee ePO server-managed network systems are safe from threats and your server is functioning normally.

**Figure 9-6  Suggested McAfee ePO weekly tasks**

Each of the recommended weekly tasks is described in more detail in this table.

*Where indicated, some of these tasks can be automated. Those instructions are included in this guide.*

**Table 9-2  Recommended McAfee ePO weekly tasks details**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee ePO tasks</td>
<td>McAfee periodically releases patches and hotfixes in addition to DATs and Engines updates. Check the McAfee website and McAfee ePO Software Manager frequently for new updates to check into the McAfee ePO console for local environment testing. You can also use the Software Manager to download and check in these updates.</td>
</tr>
<tr>
<td>Check for McAfee Product hotfixes, extensions, and patch updates on the McAfee website or within the Software Manager.</td>
<td><strong>DAT and Engine files are not updated with the Software manager.</strong> See the <em>McAfee ePolicy Orchestrator Software Product Guide</em> for Software Manager details.</td>
</tr>
</tbody>
</table>
Table 9-2  Recommended McAfee ePO weekly tasks details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run a full replication to all distributed repositories.</td>
<td>Distributed repositories can become corrupt because of an incomplete replication task. To remove corrupt files in the repositories run a full replication to all distributed repositories once per week. Full replication tasks clear the existing repository contents and replace them with new files. Incremental replication tasks copy over only new or non-existent files and therefore will not fix any corrupt files. See the McAfee ePolicy Orchestrator Software Product Guide for replication details.</td>
</tr>
<tr>
<td>Schedule an On-Demand Scan of all systems in your environment.</td>
<td>Schedule an On-Demand Scan of all systems in your environment that runs during off-hours. See the Best Practices for On-Demand Scans in VirusScan Enterprise 8.8 and the Best Practices: On-Demand Scanning tutorial for details.</td>
</tr>
<tr>
<td>SQL database tasks</td>
<td><strong>Back up the McAfee ePO SQL database.</strong> Use the Microsoft SQL Enterprise Manager to back up the McAfee ePO database. Verify the backup was successful after it has completed. See How to create an ePO validation report for the event '1203. 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 re-install your software, if needed. See the McAfee ePolicy Orchestrator Software Product Guide for Disaster Recovery details.</td>
</tr>
<tr>
<td>Windows Server operating system tasks</td>
<td><strong>Remove inactive systems from Active Directory.</strong> If you use Active Directory to pull in a list of new systems and containers that need to be managed by McAfee ePO, confirm that Active Directory is clean and does not contain any systems that are no longer on the network.</td>
</tr>
</tbody>
</table>

See also

Finding inactive systems on page 114
Recommended monthly tasks

You should perform the McAfee suggested tasks at least once per month to ensure that your McAfee ePO server managed network systems are safe from threats and your server is functioning normally.

![Diagram of recommended monthly tasks]

Figure 9-7  Suggested McAfee ePO monthly tasks

Each of the recommended monthly tasks is described in more detail in this table.

Where indicated, some of these tasks can be automated. Those instructions are included in this guide.

Table 9-3  Recommended McAfee ePO monthly tasks details

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee ePO tasks</td>
<td></td>
</tr>
<tr>
<td>Purge events to reduce database size.</td>
<td>Purge events automatically using the processes described in this guide.</td>
</tr>
<tr>
<td>Remove and update duplicate GUIDs.</td>
<td>Run the Duplicate Agent GUID Server tasks to find and fix any duplicate GUIDs in your environment. This process is described in this guide.</td>
</tr>
<tr>
<td>Review Audit Logs.</td>
<td>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 Software Product Guide for details.</td>
</tr>
</tbody>
</table>
Table 9-3  Recommended McAfee ePO monthly tasks details (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validate McAfee ePO Administrator and Reviewer IDs</td>
<td>Confirm that only employees authorized to have administrative access have properly configured IDs, with the proper permission sets in the McAfee ePO system.</td>
</tr>
<tr>
<td><strong>SQL database tasks</strong></td>
<td></td>
</tr>
<tr>
<td>Run your McAfee ePO SQL database Maintenance Plan</td>
<td>Set up and run your SQL Monthly Maintenance Plan. See Recommended maintenance plan for ePO database using SQL Server Management Studio for details.</td>
</tr>
<tr>
<td><strong>Windows Server operating system tasks</strong></td>
<td></td>
</tr>
<tr>
<td>Confirm that the Microsoft Operating System and other vendor patch levels on the McAfee ePO server are current.</td>
<td>Review and implement all Microsoft patches to eliminate vulnerabilities and mitigate risk. Other vendor patches might also be released and need updating to reduce vulnerabilities in the environment.</td>
</tr>
</tbody>
</table>

See also
*Find systems with the same GUID on page 105*
Automating and optimizing McAfee ePO workflow

You can create queries and tasks to automatically run to improve server performance, monitor threats, and ease maintenance.

Contents
- Find systems with the same GUID
- Purging events automatically
- Creating an automatic content pull and replication
- Confirm 1051 and 1059 events are filtered
- Finding systems that need a new agent
- Finding inactive systems
- Measuring malware events
- Finding malware events per subnet
- Automating DAT file testing
- Creating an automatic compliance query and report

Find systems with the same GUID

A common problem you might encounter is multiple agents with the same GUID. You can create a task to find these agents.

You can use a preconfigured server task that runs a query 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.

The steps in this task run the duplicate McAfee Agent GUID server task.

Task

For option definitions, click ? in the interface.

1. Click Menu | Automation | Server Tasks to open the Server Tasks Builder.
2. Click Edit for one of the following tasks.
   - Duplicate Agent GUID — Clear error count.
   - Duplicate Agent GUID — Remove systems that potentially use the same GUID.
3. In the Description page, select Enabled, then click:
   - Save — To enable the server task and run it from the Server Task page.
   - Next — To 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 impact performance of the McAfee ePO server and SQL Servers.

These 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 need to determine your event data retention rate. This 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 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.

There are two important event types in your database: client events and threat events. These two event types are the bulk of your event data in your database.

The following links describe reducing a McAfee ePO database by 90-95 percent from the default size. Follow the processes on these websites to Rebuild and Reorganize the SQL Indexes and Update Statistics task:

- [Database Maintenance: Part 1](#)
- [Database Maintenance: Part 2](#)

**See also**

*Reporting features on page 57*

**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, according to the retention settings for your organization.

**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 Plus Events — Purge after 10 days.

This is an example of the Actions list configuration.

![Server Task Builder with multiple Actions configured](image)

**Figure 10-1 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 that are visited by managed systems. This can result in a lot 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 clear client events.

Before you begin
You must have created a query to find the events you want purged before you start this task.

The 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.

4  Schedule the task to run every day during non-business hours, then click Save.

See also
Create custom event queries on page 59
Create custom table queries on page 70
Creating an automatic content pull and replication

To pull content daily from the public McAfee servers is one of the 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 is 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 119

Pull content automatically

Pull the McAfee content from the public McAfee servers. This keeps your protection signatures up to date.

You should schedule your pull tasks to run at least once per 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. This is aggressive and unnecessary because DAT files are typically released only once per day. Pulling two or three times per day is adequate.

Ideally, you should test your DAT files before deployment that requires a more 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 Server Task Builder dialog box with packages selected](image)

**Figure 10-3** 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 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 per day after 11 a.m. Eastern Time, then click **Next**.

![Server Task Builder Schedule configured](image)

**Figure 10-4** 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 119
Confirm 1051 and 1059 events are filtered

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 your 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? They have historic significance going back several years, and they were meant to give the administrator full disclosure that a file was not scanned by VirusScan Enterprise. This failure to scan the file could be for 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.

These events are still logged locally by VirusScan Enterprise 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 usually 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 64

Filter 1051 and 1059 events

Disable the 1051 and 1059 events if you find a significant number of these events 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.

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 with table output

Find systems with old McAfee Agent versions using a query to generate a list of all agents 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. In the Configure Chart: Table page, to configure the Sort by fields, select Product Version (Agent) under Agent Properties in the list, click Value (Descending), then click Next.

6. In the Columns tab, remove all the preconfigured columns, except System Name, and 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.

Now your new query can run from a product deployment to update the old McAfee Agent versions.

Create a Product Deployment project to update the McAfee Agents

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 you want installed on the systems.
   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.

Next to Select a start time, select Run Immediately from the list.

Click Save.

The Product Deployment project starts running and allows you to monitor the deployment process and status. See the McAfee ePolicy Orchestrator Software Product Guide for details.

See also
Create a new Agent Version Summary query with table output on page 112

Finding inactive systems

Most environments are constantly changing, new systems are added and old systems removed. This creates 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.

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 and 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 or move that system to a group in your tree that you can designate as, for example, Inactive Agents.

A preconfigured Inactive Agent Cleanup Task already 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 per 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 just 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.

```markdown
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 subaction 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 make changes 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 systems 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 Automatic Response to notify you if a threshold of systems is affected by malware.
This is an example of the dashboard created.

![Dashboard showing total infected systems cleaned per week](image)

**Figure 10-6  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**
   - **Event Category**
   - **Threat Severity**
• Threat Target IPv4 Address
• Threat Name
• Event Category

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, and click +.
• 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 if 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 flash drives.

This example shows the systems and their subnet generating the most malware events.

Figure 10-7 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 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 Target IP Address 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 just 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

   You don't need to 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 just 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 tests the content, such as DAT and engine files, before they are released on the public update servers. Because every organization is unique and contains proprietary applications, 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, you adjust this process to require that the administrator to 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.

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 only to a group of systems in a Test group.

3. An On-Demand Scan (ODS) task runs frequently on the test group.

4. Depending on the ODS scan output, one of these scenarios occurs:
   a. If malware is detected in the test group, an Automatic Response is triggered to email the appropriate 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 into the Current branch of the repository, then they 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 a pull task from the McAfee public website and a task to copy the DAT files into 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 with a small number of network segments or systems before deploying them 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 need to 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 additional DAT file, just in case the initial file, released at 11:00 a.m., was replaced later in the day.

• The other server task waits until after the test group of systems has been scanned for a few hours. Then, if not stopped by the Administrator, it automatically copies the DAT files from the Evaluation branch to the Current branch of the repository.

**Tasks**

- **Configure task to pull DAT into Evaluation branch on page 121**
  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 122**
  To automate your DAT file testing process, you must create a task to automatically copy DAT files from the Evaluation branch of the repository into the Current branch.

**Configure task to pull DAT into 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.

**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 the settings are correct in the Summary tab, then click Save.

   To confirm that the automatic DAT file pull is working, go to Menu | Reporting | Dashboards and select ePO Summary from the Dashboards list. In the Repository Package Status dashboard, in the Package Name list, confirm that the DAT (Evaluation) 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, you must create a task to automatically copy DAT files from the Evaluation branch of the repository into 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.

The daily server task to copy to the Current repository that you created runs four hours after another server task has pulled the same DAT into the Evaluation branch. This means you are validating the DATs 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 and your tolerance for risk.

Confirm 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 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 per day, at approximately 11:00 a.m. Eastern Time. In the rare case that a second DAT file is released later in the day, the additional release requires an administrator to disable the copy task into your Current Branch.

   • Click **Next**, confirm that all the settings are correct in the Summary tab, then click **Save**.

To confirm that the automatic DAT file copy is working, go to **Menu | Reporting | Dashboards**, then select **ePO Summary** from the Dashboards list. In the Repository Package Status dashboard, in the Package Name list, confirm that the DAT was updated within the last 24 hours.

**See also**
*Configure task to pull DAT into Evaluation branch on page 121*

---

**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 for the test group of systems you create should:

• Use a representative sampling of system server builds, workstation builds, and operating systems and service packs in your environment for validation.

• Use 20 to 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. This 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 new System Tree group, click **Menu | Systems | 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 into your System Tree, add new systems, or add virtual machine systems.

After creating this test group as an isolated group of systems, you can use it to test new DAT and engine updates before you deploy the updates to all the other systems in your organization.
Configure an agent policy for the test group
You must create a McAfee Agent policy that, used with an update task, automatically copies the 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 | 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 In 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 new policy, named Update from Evaluation, to the Policy Catalog.

4 Click the new policy you just created and 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 (ODS) 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.

Task
For option definitions, click ? in the interface.

1 To create a new ODS 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 To copy the existing ODS task, click Actions | New Task, then, click OK from the New Task dialog box.
   Now you can modify the copy of the existing ODS task to create the new task.

3 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 Windows folder.
   b As time permits, you can also scan the Program Files folder or All local disks.

5 Click the Scan options, click Include subfolders and Scan boot sectors.

6 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.

7 Do not configure any Exclusions.

8 Click the Actions tab, configure When a threat is found as Clean files, then Delete files.

9 Click the Performance tab and configure System utilization as Low and Artemis as Very Low.

10 Do not change any settings on the Reports tab.

11 Click Save.

Now the ODS 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 (ODS) task to run five minutes after each McAfee Agent policy update from the Evaluation repository to the test group.

Task
For option definitions, click ? in the interface.

1 Click Menu | Policy | Client Task Assignments.
   The System Tree page appears with the Assigned Client Tasks tab selected.

2 In the System Tree groups list, select the test group of systems where you want to run the ODS task.

3 To start the Client task Assignment Builder, click Actions | New Client Task Assignment, then in the Select Task tab, configure these settings:
   a For the Product list, select VirusScan Enterprise.
   b For the Task Type list, select On Demand Scan.
c For the Task Name list, select the ODS task you created in Configure On Demand Scan of test group.

d Click Next, to configure the schedule.

4 In the Schedule tab, configure these settings:
   a For the Schedule status, click Enabled.
   b For the Schedule type, select Daily from the list.
   c For the Effective period, select today’s date as the Start date, then click No end date.
   d For the Start time, configure these settings:
      • Select 9:05 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.

5 Click Next, check the Summary page, then click Save.

Your ODS 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 if malware is detected in the test group

If malware is found by the on-demand scan (ODS) 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 ODS 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 Response, click New Response, then configure these settings in the Descriptions tab:
   a For Name, 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, select ePO Notification Events from the list.
   d For Status, click Enabled.
   e Click Next.

2 Configure these settings in the Filter tab:
   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.

d Click Next.

3 Configure these settings in the Aggregation tab:
   a For Aggregation, click Trigger this response for every event.
   b Do not configure any Grouping or Throttling settings.
   c Click Next.

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 124

Creating 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 do not have the latest DATs or have not contacted the McAfee ePO server in over 30 days.

To find this very important information automatically, you must:
1 Create and schedule a server task that runs these queries:
   - **VSE: Compliance Over the Last 30 Days** — Displays the computers per day that are out of compliance based on McAfee anti-virus software DAT, engine, and service pack version.
   - **Inactive Agents** — Displays the agents that have not communicated with the McAfee ePO server in the last 30 days.

2 Create a report that includes the output of these queries.

3 Create and schedule a server task to run the report, then send it to the Administration team.

Following is an example of the report created using the query output and automatically delivered to the Administration team.

Figure 10-9  Sample automatic compliance query and report output

**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 Monday 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**.
      
      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**.
      - 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:
      - 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**.
   c. Click **Next**.

4. In the **Schedule** tab, change these settings.
   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. Click **Next**, confirm that all the 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

You need to create a report to contain the information from the queries you ran before you can send it to the administrator team, once you have the query data saved.

**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 in the **Configure Query Chart** dialog box **Query** setting, 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 in the **Configure Query Chart** dialog box **Query** setting, 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 and uses 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:
   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. For Actions list, select Run Report, then configure these settings:
      • For Select a report to run, select the compliance report you configured in Create report to include query output.
      • Select your language.
      • For Sub-Actions, select Email file.
      • For Recipients, type the email addresses of your administrators.
         Separate multiple email addresses with commas.
      • For Subject, type the information you want to appear in the subject line of the email.
   b. Click Next.

4. In the Schedule tab, change these settings:
   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. Click Next, confirm that all the 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.
Automating and optimizing McAfee ePO workflow
Creating an automatic compliance query and report
Plan your disaster recovery

You should set up McAfee ePO for a disaster recovery scenario as soon as possible after you complete your installation.

Contents

- Use Disaster Recovery
- Use server clusters for disaster recovery
- Use cold and hot spares on one physical site
- Use cold and hot spares on two physical sites

Use Disaster Recovery

The Disaster Recovery feature helps you quickly recover or re-install 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.

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 restore SQL server.
4. Re-install the McAfee ePO software using the Restore option when the McAfee ePO software Setup.exe launches.

Use server clusters for disaster recovery

If you require zero downtime when a hardware failure occurs, you can cluster your McAfee ePO and SQL servers. However, this 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 hardware failure, you can re-install 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 server, and then 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 is completely transparent to all of the agents and provides the least downtime in a disaster situation.

You must have a good SQL database backup for this to work.

See the 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 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 pointing to your secondary SQL Server. See the Microsoft article, Types of Replication Overview for details.

If the primary site fails, make all of the agents previously communicating with the primary McAfee ePO server start communicating 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 see that the primary site's IP address is not available, they query the DNS where you have changed the IP address for the primary McAfee ePO server to point to the IP address of the secondary McAfee ePO server. All agents then start trying to connect to the secondary McAfee ePO server and SQL database.
See the *McAfee ePolicy Orchestrator Product Guide* for full restore procedures.
Plan your disaster recovery
Use cold and hot spares on two physical sites
Getting more information

Use these links to find several informative and valuable links for 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 ePO processes.
- **McAfee Video Library** — This video McAfee library provides videos describing the value of McAfee products and includes technical tips.

**Documentation and support**
- **Product Documentation** — These links, on the Technical Support ServicePortal page, provide all McAfee products and includes product guides, installation guides, and release notes.
- **KnowledgeBase Search** — This page on the Technical Support ServicePortal page allows you to search the official McAfee KnowledgeBase.
- **McAfee Community for Business** — This public community allows you to ask, and answer, questions and participate in discussions with other McAfee users.

**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.

**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 the 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

A

about this guide 7
Active Directory
   organizing the System Tree 42
   synchronization 38, 42
   used to organize System Tree 41
AD, See Active Directory
administrators
   access through the System Tree 41
   contacted automatically to stop DAT release 126
   contacted automatically with compliance report 130
   recommended monthly task to review IDs 102
Agent Handlers
   component in ePolicy Orchestrator 10
   increased node count 15
agent-server secure communication
   about 10
   default interval 31
   exporting keys 31
agent-to-server communication interval
   about 49
   adjusting 93
   change default 93
   using with agent wake-up call 49
agents
   adding it to your image file 40
   and SuperAgent repositories 77
   copying the agent file 36
   deploying with third-party tools 41
   finding inactive agents 114
   finding older versions 112
   functionality 33
   GUID 40
   missing from shell systems 38
   moving between ePolicy Orchestrator servers 31
   policies 48
   revision numbers 29
   troubleshooting deployment 37
   updating using Product Deployment 113
   upgrade strategy 29
Apache server 76
ASCI, See agent-server communication interval 40
ASSC, See agent-server secure communication
Audit Logs
   purge automatically 106
   recommended monthly task 102
automatic responses
   component in ePolicy Orchestrator 10
   used to automate DAT file testing 126
automation
   copy files from Evaluation branch into Current 122
   create compliance query and report 127
   pull and copy DAT updates from McAfee 120
   pulling content into repositories 109
   purge events server task 106
B

back ups
   database 94
   required with spare database 134
   Secure Sockets Layer certificates 30
   using a SAN 25
   when moving ePolicy Orchestrator server 30
   with Disaster Recovery feature 133
   your infrastructure 27
bandwidth
   calculate for client updates 84
   calculation for repository updates 79
   calculation needed to update repositories 52
BMC Client Automation third part tool 41

C

client events
   create custom queries 70
   create summary queries 65
   purge automatically 106
clients
   calculating update bandwidth 84
   converting to SuperAgents 77
   moving with Transfer Systems 31
   tasks, about 51
   tasks, deploying products 51
compliance
   automate query and report processes 127
   create server task to run compliance queries 128
   ensure with agent in image 40
compliance (continued)
  report part of daily tasks 97
  reports 130
  run run task to deliver report 130
configuration
  agent to server communication interval 93
  automatic updates of DAT and product files 109
  client event summary queries 65
  custom queries 58, 59
  disabling 1051 and 1059 events 111
  event purging 106
  event purging with a query 108
  Global Updating limitations 85
  hard disks 22
  product deployment 52
  queries with tables 70
  threat event summary queries 66
console, See ePolicy Orchestrator
conventions and icons used in this guide 7
CPUs
  assign priority in virtual machines 21
  needed for node count 80
  over-utilized 89, 91
  recommended hardware 15
dat files
  automatic DAT file testing 120, 124
  average size 84
  creating a compliance query 127
  deploying to repositories 79
  overview of automatic testing process 119
  replicating and repositories 83
  test before deployment 123
  update with Global Updating 85
  updating automatically 109
  using repositories 76
databases
  64-bit operating systems 15
  back up and restore 27, 30
  backup part of weekly tasks 100
  component in ePolicy Orchestrator 10
  configuring hard disks 22
  dedicated hard disk 21
  deployed on storage area networks 25
  installed with ePolicy Orchestrator 21
  maintaining 94
  purge events automatically 106
  recommended hardware 15
  reindex 94
  server clusters for disaster recovery 133
  sharing hardware with ePolicy Orchestrator 22
  spares on physical sites 134
deployment
  agents overview and troubleshooting 37
  agents with third-party tools 41
  calculating repository bandwidth 84
  databases on storage area networks 25
  packages 50
  products 51
  to repositories 79
  using client tasks 51
  using randomization 52
detection definition files, See DAT files
disaster recovery
  feature used to move ePolicy Orchestrator configuration 30
  using cold and hot spares 134
  using server clusters 133
  using the Disaster Recovery feature 133
distributed repositories
  automatically pull and copy DAT updates from McAfee 120
  component in ePolicy Orchestrator 10
  creating in SuperAgents 78
  different types 76
  part of weekly tasks 100
  replicated with an automatic content pull 109
  used to deploy packages 50
dns
  changing ePolicy Orchestrator name 30
  used to find the ePolicy Orchestrator server 35, 134
documentation
  audience for this guide 7
  product-specific, finding 8
  typographical conventions and icons 7
drives, See hard disks
duplicate GUID
  recommended monthly task 102
  run server task 105
e
  ePolicy Orchestrator
    about 10
    back up your infrastructure 27
    components 10
    configuring hard disks 22
    console 10
    dedicated hard disk 21
    disable server as repository 80
    disaster recovery 133
    event processing 92
    functions 10
    installed with database 21
    installing the software 27
    moving agents between servers 30, 31
    node count 21
    Performance Monitor 90
    products list 47
ePolicy Orchestrator (continued)

- recommended hardware 15
- repository branches 50
- server 10
- server best practices 96
- server clusters for disaster recovery 133
- sharing hardware with database 22
- spares on physical sites 134
- support information 137
- understanding agent version 29
- updating the software 27
- upgrade strategy 29

events
- 1051 and 1059 filtering 111
- causing ePolicy Orchestrator performance problems 89, 91
- create client event summary queries 65
- creating custom queries 59
- creating queries 70
- disabling 1051 and 1059 events 111
- measuring malware events 116
- per subnet counted using a query 119
- processing 92
- purge automatically 106
- purge with a query 108
- purging form database 94
- threat event summary queries 66

extension, definition 47

F

- Force complete policy and task update parameter note 49
- Force installation over existing version parameter note 37
- fragmentation in the database 94
- FramePkg.exe, agent installation application 41
- FTP repositories 76

G

- global unique identifier, See GUID 40
- Global Updating, about 85
- groups
  - in the System Tree 42
  - of SuperAgents 77
  - sending a policy change 49
  - used to deploy products 51
- GTI, See McAfee Global Threat Intelligence 97
- GUIDs
  - deleting from the image file 40
  - finding duplicates 105

H

- hard disks
  - configuring 22
  - dedicated 21
  - recommended hardware 15
  - moving ePolicy Orchestrator 30
  - questions 21
- recommended configurations 22
- sharing with ePolicy Orchestrator and database 22
- used for repositories 80
- HIPS, See Host Intrusion Prevention 15
- Host Intrusion Prevention, example product 15
- hotfixes 29
- HTTP repositories 77

I

- IBM Tivoli third part tool 41
- IIS, See Microsoft IIS server
- image file, adding the agent 40
- inactive agent
  - finding 114
  - query 114
  - removed as part of weekly tasks 100
- installation
  - ePolicy Orchestrator 27
  - use Disaster Recovery after installation 133
- IP address
  - change to move your ePolicy Orchestrator server 30
  - used to find the ePolicy Orchestrator server 35
  - used to sort the System Tree 42

L

- lazy caching, SuperAgent configuration 77
- LDF file 22

M

- Maintenance Plan, See database maintaining 94
- malware events
  - count systems cleaned per week 117
  - create query to find malware events per subnet 119
  - measuring 116
  - per subnet 118
  - send Automatic Response 126
- Master Repository
  - default 80
  - on ePolicy Orchestrator 76
- McAfee Agents, See agents
- McAfee Global Threat Intelligence suggested daily task 97
- McAfee Security Innovation Alliance 47
- McAfee ServicePortal, accessing 8
- MDF file 22
- Microsoft
  - System Center Configuration Manager 41
  - Windows Reliability and Performance Monitor 89
  - Windows Task Manager 89
- Microsoft Developer Network, deploying to a SAN 25
- Microsoft IIS server 76
Microsoft SQL database, See database
MSDN, See Microsoft Developer Network 25

N
node counts
  and repositories 77
hard disks 22
questions 21
recommended hardware 15
repository hardware 80
setting agent to server communication interval 49
sharing hardware 22
using virtual machines 21
Novell Zenworks third part tool 41

O
OAS, See On-Access Scan 97
ODS, See On Demand Scan 97
On Demand Scan
  recommended daily task 97
  recommended weekly task 100
  used to automate DAT file testing 124
On-Access Scan, recommended daily task 97
On-Demand Scan
  part of weekly tasks 100
  schedule for the test group 125
operating systems
  64-bit 15
  configuring hard disks 22
  for repositories 76

P
packages
  about 47
  deploying 50
patches
  revision numbers 29
  using repositories 76
perfmon, See Performance Monitor 90
Performance Monitor, starting 90
policies
  about 47
  create new SuperAgent policy 78
  creating SuperAgent 77
  disabling the Master Repository 82
  for agents 48
  inherited from System Tree 47
  McAfee Agent policy for a DAT test group 124
  sending changes immediately 49
  sending immediately 49
  set the ASCI 93
policy enforcement interval 51
Product Deployment
  create project to update McAfee Agents 113
Product Deployment (continued)
  feature 51
products
  adding using Software Manager 47
  deployment 51
  updating automatically 109
  version numbers 29
  videos 137
purge events
  automatically 106
  recommended monthly task 102

Q
queries
  client event summary 65
  creating custom 58, 59
  creating reports 57
  DAT file compliance 127
  event summary overview 64
  find Agent Version Summary 112
  Inactive Agents 114
  malware events 116
  threat event summary 66
  to count systems cleaned per week 117
  to display compliance 128
  to find malware events per subnet 119
  use report input 130
  used to purge events 108
  using tables 70

R
RAID 22
RAM
  recommended hardware 15
  repository servers 80
randomization, product deployment 51
reference information 137
reports
  creating 57
  creating custom queries 58, 59
  include query output 130
repositories
  about 76, 79
  automatically pull and copy DAT updates from McAfee 120
  branches 50
  calculating bandwidth use 79
  calculating update bandwidth 84
  calculation bandwidth needed to update 52
  DAT file replication 83
  determine how many and location 79, 80
  disabling the Master Repository 82
  FTP servers 76
  global updating 85
  HTTP servers 77
repositories (continued)
- pull content automatically 109
- SuperAgent 77
- UNC shares 77
- update with Global Updating 85
- used to automate DAT file testing 124
- what they do 75

S
SAN, See storage area networks
Scheduling
- automatic updates of DAT and product files 109
- event purging 106, 108
- product deployment 52
Secure Sockets Layer certificate back ups 30
Secure Sockets Layer certificates 30
Server clusters
- for disaster recovery 133
- for SQL database hardware 22
Server tasks
- about 56
- purge the logs 106
Servers
- combining ePolicy Orchestrator and database 21
- disabling the Master Repository 82
- disaster recovery 133
- finding performance problems 89, 91
- platform, questions 21
- recommended best practices 96
- recommended hardware 15
ServicePortal, finding product documentation 8
Shell systems, about 38
SIA, See McAfee Security Innovation Alliance 47
SMS, See Microsoft System Center Configuration Manager 41
SMS, See Systems Management Server 31
Snapshot, with Disaster Recovery feature 133
Software Manager 47
- part of weekly tasks 100
- recommended weekly task 100
SQL database, See databases
SQL replication, required with spare database 134
SSL, See Secure Sockets Layer certificates
SSL, See Secure Sockets Layer 30
Storage area networks, configuring 25
SuperAgents
- assign SuperAgents policy to SuperAgents group 78
- configuring 77
- convert client systems into SuperAgents 79
- create group in System Tree 78
- create new policy 78
- lazy caching 77
- sharing hardware 80
- synchronization, Active Directory 38

System Tree
- configuring SuperAgent group 77
- create group for DAT file testing 123
- create SuperAgents group 78
- deleting inactive systems 115
- inherited policies 47
- organizing with Active Directory 41
- showing shell systems 38
- wake up agents immediately 49
Systems Management Server tool 31

T
Tasks
- added with new products 51
- automatically pull and copy DAT updates from McAfee 120
- find inactive agents 114
- Inactive Agents task 114
- pull content automatically 109
- purge events 102
- purge events automatically 106
- purge events with a query 108
- recommended daily 97
- recommended monthly 102
- recommended weekly 100
- to copy files from Evaluation branch into Current 122
- to deploy products 51
- to modify ePolicy Orchestrator 56
- to run and deliver a report 130
- to run compliance queries 128
- to schedule On-Demand Scan of test group 125
Technical Support, finding product information 8
ticketing system 10
Tools, third party
- use Windows Explorer to check ePolicy Orchestrator events 92
- used to deploy agents 35, 36, 41
- Windows Performance Monitor 90
Transfer Systems, used to move clients 31
troubleshooting agent deployment 37

U
UNC share repositories 77
Universal Naming Convention, See UNC share repositories
Updates
- calculating required bandwidth 84
- DAT files and products automatically 109
- ePolicy Orchestrator 27
Upgrade Compatibility Utility 27
Upgrading product strategy 29

V
VDI, See Virtual Desktop Infrastructure 40
Virtual Desktop Infrastructure mode 40
virtual machines
  configuring hard disks 22
  node count 21
  testing ePolicy Orchestrator 27
  used for automatic DAT file testing 123
  with database 21
  with ePolicy Orchestrator 21
VirusScan Enterprise
  downloaded as part of your image 40
  example product 15
  On-Demand Scan as part of suggested weekly tasks 100

VirusScan Enterprise (continued)
  policies added automatically to ePolicy Orchestrator 47
  restriction for Global Updating 85
VMs, See virtual machines
VSE, See VirusScan Enterprise 15

W
what’s in this guide 8
Windows Reliability and Performance Monitor 89, 91
Windows Task Manager 89