Product Guide

McAfee® ePolicy Orchestrator® 4.6.0 Software
Contents

Configuring the template and location for exported reports .................................. 36
Using a proxy server ......................................................................................... 36
SSL certificates ............................................................................................... 37
Enabling System Tree sorting on the server ....................................................... 39
ePolicy Orchestrator server settings categories and their descriptions ............... 39

5 Creating user accounts .................................................................................. 43
About user accounts ......................................................................................... 43
Global administrators ....................................................................................... 43
Working with user accounts ............................................................................ 44
Creating user accounts ................................................................................... 44
Editing user accounts ...................................................................................... 44
Deleting user accounts .................................................................................... 45

6 Setting up permission sets ............................................................................. 47
How users, groups, and permission sets fit together .......................................... 47
Working with permission sets .......................................................................... 49
Creating a new permission set .......................................................................... 49
Modifying an existing permission set ................................................................ 50
Duplicating a permission set ........................................................................... 50
Exporting permission sets .............................................................................. 50
Importing permission sets ............................................................................... 51
Removing a permission set ............................................................................. 51
Deleting permission sets .................................................................................. 51

7 Configuring advanced server settings .......................................................... 53
Configuring Active Directory user login .......................................................... 53
Managing ePolicy Orchestrator users with Active Directory ......................... 53
Configuring Windows authentication and authorization ..................................... 56
Authenticating with certificates ....................................................................... 58
When to use certificate authentication ............................................................... 58
Configuring ePolicy Orchestrator for certificate authentication ....................... 58
Uploading server certificates .......................................................................... 59
Removing server certificates ......................................................................... 59
Configuring users for certificate authentication .............................................. 60
Problems with certificate authentication ......................................................... 60
Configuring Rogue System Detection server settings ..................................... 61
Configuring server settings for Rogue System Detection ................................ 61
Managing security keys ................................................................................... 64
Security keys and how they work .................................................................... 64
Master repository key pair .............................................................................. 65
Agent-server secure communication (ASSC) keys ............................................ 67
Backing up and restoring keys ........................................................................ 71
Configuring source and fallback sites ............................................................. 73
Working with source and fallback sites .......................................................... 73

8 Setting up repositories ................................................................................... 77
Repository types and what they do .................................................................... 78
Types of distributed repositories ...................................................................... 79
Repository branches and their purposes ........................................................... 80
Repository list file and its uses ........................................................................ 81
How repositories work together ...................................................................... 82
Ensuring access to the source site .................................................................... 82
Configuring proxy settings ............................................................................. 83
Configuring proxy settings for the McAfee Agent .......................................... 83
Configuring proxy settings for McAfee Labs Security Threats ....................... 84
Using SuperAgents as distributed repositories ........................................... 84
Creating SuperAgent repositories ........................................................... 85
Selecting which packages are replicated to SuperAgent repositories ................. 86
Deleting SuperAgent distributed repositories ............................................. 86
Creating and configuring FTP, HTTP, and UNC repositories .......................... 86
Creating a folder location on an FTP, HTTP server or UNC share ..................... 87
Avoiding replication of selected packages .................................................. 89
Disabling replication of selected packages .................................................. 89
Enabling folder sharing for UNC and HTTP repositories ............................... 90
Editing distributed repositories ................................................................... 90
Deleting distributed repositories ................................................................... 90
Using local distributed repositories that are not managed ................................. 91
Working with the repository list files ........................................................... 92
Exporting the repository list SiteList.xml file .............................................. 92
Exporting the repository list SiteMgr.xml file for backup or use by other servers 93
Importing distributed repositories from the SiteMgr.xml file ......................... 93
Importing source sites from the SiteMgr.xml file ......................................... 93
Changing credentials on multiple distributed repositories .............................. 94

9 Setting up registered servers ................................................................... 95
Registering servers ...................................................................................... 95
Registering McAfee ePO servers .................................................................. 95
Registering LDAP servers ........................................................................... 97
Registering SNMP servers ........................................................................... 98
Registering a database server ....................................................................... 99

10 Setting up Agent Handlers ..................................................................... 101
Agent Handlers and what they do ............................................................... 101
How Agent Handlers work .......................................................................... 101
Handler groups and priority ....................................................................... 102
Working with Agent Handlers ..................................................................... 103
Assigning agents to Agent Handlers ........................................................... 103
Managing Agent Handler assignments ......................................................... 104
Setting up Agent Handler groups ............................................................... 104
Managing Agent Handler groups ............................................................... 105
Moving agents between handlers ............................................................... 105

11 Other important server information ...................................................... 109
About Internet Protocols in managed environment ...................................... 109
Exporting objects from ePolicy Orchestrator .............................................. 110
Importing items into ePolicy Orchestrator .................................................. 110
Exporting objects and data from your ePolicy Orchestrator server ............... 111
ePolicy Orchestrator Log Files .................................................................... 112
The Audit Log ............................................................................................... 112
The Server Task log ...................................................................................... 114
The Threat Event log ..................................................................................... 116

Managing your network security with your ePolicy Orchestrator server

12 Organizing the System Tree .................................................................. 121
The System Tree structure .......................................................................... 121
Considerations when planning your System Tree ........................................ 123
Administrator access ................................................................................... 123
Environmental borders and their impact on system organization ................. 124
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnets and IP address ranges ..................................................</td>
</tr>
<tr>
<td>Tags and systems with similar characteristics ..............................</td>
</tr>
<tr>
<td>Operating systems and software ..................................................</td>
</tr>
<tr>
<td>Tags and how they work ..............................................................</td>
</tr>
<tr>
<td>Active Directory and NT domain synchronization ............................</td>
</tr>
<tr>
<td>Active Directory synchronization ...............................................</td>
</tr>
<tr>
<td>NT domain synchronization .........................................................</td>
</tr>
<tr>
<td>Criteria-based sorting ..............................................................</td>
</tr>
<tr>
<td>How settings affect sorting .......................................................</td>
</tr>
<tr>
<td>IP address sorting criteria .......................................................</td>
</tr>
<tr>
<td>Tag-based sorting criteria .........................................................</td>
</tr>
<tr>
<td>Group order and sorting .............................................................</td>
</tr>
<tr>
<td>Catch-all groups ............................................................................</td>
</tr>
<tr>
<td>How a system is added to the System Tree when sorted ......................</td>
</tr>
<tr>
<td>Working with tags ......................................................................</td>
</tr>
<tr>
<td>Creating tags with the Tag Builder ................................................</td>
</tr>
<tr>
<td>Excluding systems from automatic tagging ....................................</td>
</tr>
<tr>
<td>Applying tags to selected systems .................................................</td>
</tr>
<tr>
<td>Applying criteria-based tags automatically to all matching systems ....</td>
</tr>
<tr>
<td>Creating and populating groups ....................................................</td>
</tr>
<tr>
<td>Creating groups manually .............................................................</td>
</tr>
<tr>
<td>Adding systems manually to an existing group ................................</td>
</tr>
<tr>
<td>Exporting systems from the System Tree ........................................</td>
</tr>
<tr>
<td>Importing systems from a text file .................................................</td>
</tr>
<tr>
<td>Sorting systems into criteria-based groups ....................................</td>
</tr>
<tr>
<td>Importing Active Directory containers .........................................</td>
</tr>
<tr>
<td>Importing NT domains to an existing group ....................................</td>
</tr>
<tr>
<td>Synchronizing the System Tree on a schedule ................................</td>
</tr>
<tr>
<td>Updating the synchronized group with an NT domain manually ............</td>
</tr>
<tr>
<td>Moving systems manually within the System Tree ............................</td>
</tr>
<tr>
<td>Transferring systems between McAfee ePO servers ........................</td>
</tr>
</tbody>
</table>

**13 Working with the agent from the McAfee ePO server** 149

| Agent-server communication .................................................. | 149 |
| Agent-server communication interval ....................................... | 150 |
| Agent-server communication interruption handling ..................... | 150 |
| Wake-up calls and tasks ......................................................... | 151 |
| SuperAgents and broadcast wake-up calls .................................. | 151 |
| SuperAgent caching and communication interruptions .................... | 152 |
| Viewing agent and product properties ........................................ | 153 |
| Responding to policy events .................................................... | 153 |
| Running client tasks immediately .............................................. | 154 |
| Sending manual wake-up calls to systems ................................... | 155 |
| Sending manual wake-up calls to a group ................................... | 155 |
| Locate inactive agents .................................................................. | 156 |
| Queries provided by McAfee Agent ............................................ | 156 |
| Windows system and product properties reported by the agent .......... | 157 |

**14 Using the Software Manager to check in software** 159

| What’s in the Software Manager ................................................. | 159 |
| Checking in, updating, and removing software using the Software Manager | 160 |

**15 Using policies to manage products and systems** 163

| Policy management ................................................................. | 163 |
| Policy application ....................................................................... | 165 |
| How policy assignment rules work ............................................ | 166 |
Monitoring and reporting on your network security status

18 Responding to events in your network

About using Automatic Responses .......................................................................................... 212
Automatic Responses and how it works .................................................................................... 212
  Throttling, aggregation, and grouping ..................................................................................... 213
  Default rules ............................................................................................................................ 213
Planning ................................................................................................................................... 214
Determining how events are forwarded ..................................................................................... 214
  Determining which events are forwarded immediately ............................................................ 215
  Determining which events are forwarded ................................................................................. 215
Configuring Automatic Responses .......................................................................................... 216
  Assigning permission sets to access Automatic Responses ..................................................... 216
  Working with SNMP servers .................................................................................................... 217
  Working with registered executables and external commands .................................................. 220
Creating and editing Automatic Response rules ........................................................................ 216
  Describing the rule .................................................................................................................. 222
  Setting filters for the rule ......................................................................................................... 223
  Setting thresholds of the rule .................................................................................................... 223
  Configuring the action for Automatic Response rules ............................................................ 224
Frequently asked questions ........................................................................................................ 226

19 Monitoring with Dashboards

Working with dashboards ......................................................................................................... 229
  Creating dashboards ................................................................................................................ 230
  Adding monitors to dashboards ................................................................................................ 230
  Removing monitors from dashboards ....................................................................................... 231
  Duplicating dashboards .......................................................................................................... 231
  Deleting dashboards ................................................................................................................ 232
  Importing dashboards ............................................................................................................. 232
  Exporting dashboards ............................................................................................................. 232
  Changing the system default dashboard ............................................................................... 233
  Assigning permissions to dashboards ..................................................................................... 233
Working with dashboard monitors ............................................................................................ 234
  Configuring dashboard monitors ............................................................................................ 234
  Moving and resizing dashboard monitors .............................................................................. 235
Default dashboards and their monitors ..................................................................................... 235

20 Querying the database and reporting on system status

Query and report permissions ..................................................................................................... 240
About queries ............................................................................................................................. 240
  Query Builder .......................................................................................................................... 242
Working with queries ................................................................................................................ 243
  Creating custom queries .......................................................................................................... 243
  Running an existing query ........................................................................................................ 244
  Running a query on a schedule ............................................................................................... 245
  Creating a query group ............................................................................................................ 245
  Moving a query to a different group ....................................................................................... 246
Duplicating queries .................................................................................................................... 246
Deleting queries ........................................................................................................................ 246
Exporting a query ....................................................................................................................... 247
21 Detecting Rogue Systems 265

What are rogue systems ........................................ 265
Rogue System Detection states .................................. 266
Rogue Sensor Blacklist ........................................... 269
Rogue System Detection policy settings ....................... 269
Rogue System Detection permission sets ....................... 271
How the Rogue System Sensor works ......................... 272
Passive listening to layer-2 traffic ............................... 272
Intelligent filtering of network traffic ........................... 272
Data gathering and communications to the server .......... 273
Systems that host sensors ....................................... 273
How detected systems are matched and merged ............. 274
Working with detected systems ................................. 274
Configuring Rogue System Detection policy settings ...... 275
Adding systems to the Exceptions list ......................... 276
Adding systems to the Rogue Sensor Blacklist ............... 277
Adding detected systems to the System Tree .................. 277
Editing system comments ....................................... 277
Exporting the Exceptions list .................................. 278
Importing systems to the Exceptions list ...................... 278
Merging detected systems ....................................... 278
Pinging a detected system ....................................... 279
Querying detected system Agents ............................... 279
Removing systems from the Detected Systems list ........... 279
Removing systems from the Exceptions list ................... 280
Removing systems from the Rogue Sensor Blacklist ......... 280
Viewing detected systems and their details ................... 280
Working with sensors ............................................ 280
Installing sensors ............................................... 281
Editing sensor descriptions ..................................... 283
Removing sensors ............................................... 283
Working with subnets .......................................... 284
Preface

This guide provides the information you need to configure, use, and maintain your McAfee product.

Contents

- About this guide
- Finding product documentation

About this guide

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

Audience

McAfee documentation is carefully researched and written for the target audience. The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.
- **Users** — People who use the computer where the software is running and can access some or all of its features.
- **Security officers** — People who determine sensitive and confidential data, and define the corporate policy that protects the company's intellectual property.
- **Reviewers** — People who evaluate the product.

Conventions

This guide uses the following typographical conventions and icons.

- **Book title or Emphasis**: Title of a book, chapter, or topic; introduction of a new term; emphasis.
- **Bold**: Text that is strongly emphasized.
- **User input or Path**: Commands and other text that the user types; the path of a folder or program.
- **Code**: A code sample.
- **User interface**: Words in the user interface including options, menus, buttons, and dialog boxes.
- **Hypertext blue**: A live link to a topic or to a 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 is organized to help you find the information you need. It's divided into functional parts intended to support the goals you need to accomplish when using your McAfee ePolicy Orchestrator (McAfee ePO™) software. Each part is then further divided into chapters that group relevant information together by feature and associated tasks, so you can go directly to the topic you need to successfully accomplish your goals.

## Finding 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 <a href="http://mysupport.mcafee.com">Product Documentation</a>.</td>
</tr>
<tr>
<td></td>
<td>2 Select a <strong>Product</strong>, then select a <strong>Version</strong>.</td>
</tr>
<tr>
<td></td>
<td>3 Select a product document.</td>
</tr>
<tr>
<td>KnowledgeBase</td>
<td>• Click <a href="http://mysupport.mcafee.com">Search the KnowledgeBase</a> for answers to your product questions.</td>
</tr>
<tr>
<td></td>
<td>• Click <a href="http://mysupport.mcafee.com">Browse the KnowledgeBase</a> for articles listed by product and version.</td>
</tr>
</tbody>
</table>
Introducing McAfee ePolicy Orchestrator Software version 4.6.0

Get familiar with what ePolicy Orchestrator software is, the components of the software, and how they protect your environment. Then, review the configuration process overview.

Chapter 1  Introducing McAfee ePolicy Orchestrator Software version 4.6.0
Chapter 2  Planning your ePolicy Orchestrator configuration
Introducing McAfee ePolicy Orchestrator Software version 4.6.0

McAfee ePolicy Orchestrator software is a key component of the McAfee Security Management Platform which provides unified management of endpoint, network, and data security. It provides you with end-to-end visibility and powerful automation features that reduce incident response times, strengthens protection, and decreases the complexity of managing risk and security.

See also
What is ePolicy Orchestrator software on page 15
Components and what they do on page 16
How the software works on page 17
How to navigate the ePolicy Orchestrator interface on page 18

Contents
• What is ePolicy Orchestrator software
• Components and what they do
• How the software works
• How to navigate the ePolicy Orchestrator interface

What is ePolicy Orchestrator software

ePolicy Orchestrator software is a scalable, extensible management platform that enables centralized policy management and enforcement of your security products and the systems on which they reside. It also provides comprehensive reporting and product deployment capabilities, all through a single point of control.

Using an ePolicy Orchestrator server, you can:
• Deploy security products, patches, and service packs to the systems in your network.
• Manage the host and network security products deployed to your systems through the enforcement of security policies, client tasks, and server tasks.
• Update the DATs, Engines and other security content required by your security software to ensure your managed systems are secure.
Components and what they do

The ePolicy Orchestrator software is comprised of these components.

- McAfee ePO server — The center of your managed environment. The server delivers security policies and tasks, controls updates, and processes events for all managed systems. The ePolicy Orchestrator server includes these subcomponents:
  - Apache server — Along with the event parser, this component is responsible for communicating with the McAfee Agent. Together, these two components receive updated events and properties from agents, and send updated policies and tasks.
  - Application server — This component hosts the user interface and server task scheduler.
  - Event parser — This component works in conjunction with the apache server to communicate events and properties from the agent to the server, and send policies and tasks from the server to the agent.
- Database — The central storage component for all data created and used by ePolicy Orchestrator. You can choose whether to house the database on your McAfee ePO server or on a separate system, depending on the specific needs of your organization.
- McAfee Agent — A vehicle of information and enforcement between the ePolicy Orchestrator server and each managed system. The agent retrieves updates, ensures task implementation, enforces policies, and forwards events for each managed system. It uses a separate secure data channel to transfer data to the server. A McAfee Agent can also be configured as a SuperAgent.
- Master repository — The central location for all McAfee updates and signatures, residing on the ePolicy Orchestrator server. Master repository retrieves user-specified updates and signatures from McAfee or from user-defined source sites.
- Distributed repositories — Local access points strategically placed throughout your environment for agents to receive signatures, product updates, and product installations with minimal bandwidth impact. Depending on how your network is configured, you can set up SuperAgent, HTTP, FTP, or UNC share distributed repositories.
- Remote Agent Handlers — A server that you can install in various network locations to help manage agent communication, load balancing, and product updates. Remote Agent Handlers are comprised of an apache server and an event parser. They can help you manage the needs of large or complex network infrastructures by allowing you more control over agent-server communication.
- Registered servers — Used to register other servers with your ePolicy Orchestrator server. Registered server types include:
  - LDAP server — Used for Policy Assignment Rules and to enable automatic user account creation.
  - SNMP server — Used to receive an SNMP trap. You must add the SNMP server’s information so that ePolicy Orchestrator knows where to send the trap.
  - Database server — Used to extend the advanced reporting tools provided with ePolicy Orchestrator software.
  - Ticketing server — Before tickets can be associated with issues, you must have a registered ticketing server configured. The system running the ticketing extension must be able to resolve the address of the Service Desk system.

Depending on the needs of your organization and the complexity of your network, you might only need to use some of these components.
How the software works

McAfee ePO software is designed to be extremely flexible. It can be set up in many different ways, to meet your unique needs.

The software follows the classic client-server model, in which a client system (system) calls into your server for instructions. To facilitate this call to the server, a McAfee Agent is deployed to each system in your network. Once an agent is deployed to a system, the system can be managed by your ePolicy Orchestrator server. Secure communication between the server and managed system is the bond that connects all the components of your ePolicy Orchestrator software. The figure below shows an example of how your ePolicy Orchestrator server and components inter-relate in your secure network environment.
1. Your ePolicy Orchestrator server connects to the McAfee update server to pull down the latest security content.

2. The ePolicy Orchestrator database stores all the data about the managed systems on your network, including:
   - System properties
   - Policy information
   - Directory structure
   - All other relevant data the server needs to keep your systems up-to-date.

3. McAfee Agents are deployed to your systems to facilitate:
   - Policy enforcement
   - Product deployments and updates
   - Reporting on your managed systems

4. Agent-server secure communication (ASSC) occurs at regular intervals between your systems and server. If remote Agent Handlers are installed in your network, agents communicate with the server through their assigned Agent Handlers.

5. Users log onto the ePolicy Orchestrator console to perform security management tasks, such as running queries to report on security status or working with your managed software security policies.

6. The McAfee update server hosts the latest security content, so your ePolicy Orchestrator can pull the content at scheduled intervals.

7. Distributed repositories placed throughout your network host your security content locally, so agents can receive updates more quickly.

8. Remote Agent Handlers help to scale your network to handle more agents with a single ePolicy Orchestrator server.

9. Ticketing servers connect to your ePolicy Orchestrator server to help manage your issues and tickets.

10. Automatic Response notifications are sent to security administrators to notify them that an event has occurred.

---

**How to navigate the ePolicy Orchestrator interface**

The ePolicy Orchestrator interface uses a menu-based navigation model with a customizable favorites bar to ensure that you can get where you need to go quickly.

Menu sections represent the top-level features of your ePolicy Orchestrator server. As you add new managed products to your server, the associated interface pages are either added to an existing category, or a new category is created in the Menu.

**About the ePolicy Orchestrator navigation Menu**

The ePolicy Orchestrator **Menu** provides the primary navigation for your server.
The Menu uses categories that comprise the various features and functionality of your ePolicy Orchestrator server. Each category contains a list of primary feature pages associated with a unique icon. Select a category in Menu to view and navigate to the primary pages that make up that feature.

**About the navigation bar**

Customize the navigation bar to provide quick access to the features and functionality you use most often.

You can decide which icons are displayed on the navigation bar by dragging any Menu item on or off the navigation bar. When you navigate to a page in the Menu, or click an icon in the navigation bar, the name of that page is displayed in the blue box next to the Menu.

On systems with 1024x768 screen resolution, the navigation bar can display six icons. When you place more than six icons on the navigation bar, an overflow menu is created on the right side of the bar. Click > to access the Menu items not displayed in the navigation bar. The icons displayed in the navigation bar are stored as user preferences, so each user's customized navigation bar is displayed regardless of which console they use to log on to the server.
Planning your ePolicy Orchestrator configuration

Getting started using your ePolicy Orchestrator server requires planning and consideration with regard to infrastructure and configuration.

How you setup your server infrastructure, and how much configuration you need to perform depends on the unique needs of your network environment. Considering these areas in advance can reduce the time it takes to get up-and-running.

Contents
- About scalability
- Server configuration overview

About scalability

How you manage your scalability needs depends on whether you use multiple ePolicy Orchestrator servers or multiple remote Agent Handlers.

With ePolicy Orchestrator software, you can scale your network vertically or horizontally.

- **Vertically scalability** — Adding and upgrading to bigger, faster hardware to manage larger and larger deployments. Scaling your ePolicy Orchestrator server infrastructure vertically is accomplished by upgrading your server hardware, and using multiple ePolicy Orchestrator servers throughout your network, each with its own database.

- **Horizontal scalability** — Accomplished by increasing the deployment size that a single ePolicy Orchestrator server can manage. Scaling your server horizontally is accomplished by installing multiple remote Agent Handlers, each reporting to a single database.

When to use multiple ePolicy Orchestrator servers

Depending on the needs of your organization, using multiple ePolicy Orchestrator servers might be required.

Some scenarios in which you might want to use multiple servers include:

- You want to maintain separate databases for distinct units within your organization.
- You require separate IT infrastructures, administrative groups, or test environments.
- Your organization is distributed over a large geographic area, and uses a network connection with relatively low bandwidth such as a WAN, VPN, or other slower connections typically found between remote sites. For more information about bandwidth requirements, see the McAfee ePolicy Orchestrator Hardware Usage and Bandwidth Sizing Guide.

Using multiple servers in your network requires that you maintain a separate database for each server. You can roll up information from each server to your main ePolicy Orchestrator server and database.
When to use multiple remote Agent Handlers

Multiple remote Agent Handlers can help you manage large deployments without adding additional ePolicy Orchestrator servers to your environment.

The Agent Handler is the component of your server responsible for managing agent requests. Each McAfee ePO server installation includes an Agent Handler by default. Some scenarios in which you might want to use multiple remote Agent Handlers include:

- You want to allow agents to choose between multiple physical devices, so they can continue to call in and receive policy, task, and product updates; even if the application server is unavailable, and you don’t want to cluster your ePolicy Orchestrator server.
- Your existing ePolicy Orchestrator infrastructure needs to be expanded to handle more agents, more products, or a higher load due to more frequent agent-server communication intervals (ASCI).
- You want to use your ePolicy Orchestrator server to manage disconnected network segments, such as systems that use Network Address Translation (NAT) or in an external network.

> This is functional as long as the Agent Handler has a high bandwidth connection to your ePolicy Orchestrator database.

Multiple Agent Handlers can provide added scalability and lowered complexity in managing large deployments. However, because Agent Handlers require a very fast network connection, there are some scenarios in which you should not use them, including:

- To replace distributed repositories. Distributed repositories are local file shares intended to keep agent communication traffic local. While Agent Handlers do have repository functionality built in, they require constant communication with your ePolicy Orchestrator database, and therefore consume a significantly larger amount of bandwidth.
- To improve repository replication across a WAN connection. The constant communication back your database required by repository replication can saturate the WAN connection.
- To connect a disconnected network segment where there is limited or irregular connectivity to the ePolicy Orchestrator database.

Server configuration overview

How you set up your ePolicy Orchestrator server depends on the unique needs of your environment. This process overview highlights the major setup and configuration required to use your ePolicy Orchestrator server. Each of the steps represents a chapter or section in this guide, where you can find the detailed information you need to understand the features and functionality of the software, along with the tasks needed to implement and use them.

> Depending on the size and complexity of your network, you might not need to configure all available features.
Process overview

This process is a high-level overview of the configuration process for your server. Many items represent specific feature sets or functional areas of the ePolicy Orchestrator software:

1. Configure essential features — ePolicy Orchestrator software has some essential features that you must configure for your server to function properly. Use the Guided Configuration tool to configure the essential features of your McAfee ePO server.

2. Configure general server settings — Server settings in this group affect functionality that you do not need to modify for your server to operate correctly, but you can customize some aspects of how your server works.

3. Create user accounts — User accounts provide a means for users to access the server.

4. Configure permission sets — Permission sets grant rights and access to ePolicy Orchestrator features.

5. Configure advanced server settings and features — Your ePolicy Orchestrator server provides advanced features and functionality to help you automate the management of your network security.

6. Setup additional components — Additional components such as distributed repositories, registered servers, and Agent Handlers are required to use many of the advanced features of your ePolicy Orchestrator software.
Setting up and configuring your ePolicy Orchestrator server

Setting up and configuring your ePolicy Orchestrator server is the first step to managing your network security.

Chapter 3  Configuring essential features
Chapter 4  Configuring general server settings
Chapter 5  Creating user accounts
Chapter 6  Setting up permission sets
Chapter 7  Configuring advanced server settings
Chapter 8  Setting up repositories
Chapter 9  Setting up registered servers
Chapter 10 Setting up Agent Handlers
Chapter 11 Other important server information
Configuring essential features

Get up-and-running quickly by configuring the essential features of your ePolicy Orchestrator server.

Contents

- About essential features
- Using the Guided Configuration to configure essential features

About essential features

Several of your ePolicy Orchestrator server features are essential for its use, and must be configured before you can deploy and manage security software on the systems in your network.

The essential features of your McAfee ePO server are:

- The Software Manager — Allows you to check in new and updated security software into your ePolicy Orchestrator server and Master Repository from within the console.

- The System Tree — Contains all of the systems managed by your ePolicy Orchestrator server.

- The Policy Catalog — Where you configure the security policies that control the security software deployed to your managed systems.

- The Client Task Catalog — Where you create, assign, and schedule client tasks to automate tasks that run on your managed systems.

- The McAfee Agent — Enables management of a system on your network. Once deployed, the agent communicates status and all associated data to and from your server and the managed system. It is the vehicle through which security software is deployed, policies are enforced, and tasks are assigned.

   ![](image)

   The McAfee Agent is an independent software product required for your ePolicy Orchestrator server to manage systems on your network. It is checked in to your Master Repository automatically when you install your McAfee ePO software.

This version of the software comes equipped with the ePolicy Orchestrator Guided Configuration tool. This tool is designed to help you configure these essential features, and to become familiar with the ePolicy Orchestrator interface. The Guided Configuration helps you complete the necessary steps to:

1. Get McAfee security software checked into your Master Repository, so it can be deployed to systems in your network.

2. Add your systems to the ePolicy Orchestrator System Tree, so you can bring them under management.

3. Create and assign at least one security policy to be enforced on your managed systems.
4 Schedule a client update task to keep your security software up-to-date.

5 Deploy your security software to your managed systems.

Using the Guided Configuration is not required. You can perform each of these steps manually. If you choose to perform these steps manually, McAfee recommends that you use a similar workflow during your configuration process. Regardless of the method you choose to configure these features, you can continue to modify and tune your server's configuration using the Guided Configuration tool or by navigating directly to each page from the McAfee ePO Menu.

---

Using the Guided Configuration to configure essential features

The Guided Configuration tool is designed to help you configure your ePolicy Orchestrator server by directing you through pages used to configure some essential features.

Work through each step in the task below to:

- Select the security software you want to deploy to systems on your network.
- Select the systems on your network you want manage with your McAfee ePO server, and add them to the System Tree.
- Configure a Default policy to be assigned and enforced on your managed systems.
- Schedule a product update task to ensure that your managed systems have the latest updates installed.
- Deploy your security software to your managed systems.

You don't have to complete each step, and you can revisit any step as often as you like. However, McAfee recommends that you use this configuration tool like a wizard, and complete each step in sequence. Doing so will help you get familiar with the individual interface pages that control these features, so you can use them without the configuration tool in the future.

**Task**

For option definitions, click ? in the interface.

1 In the ePolicy Orchestrator console click **Menu | Reporting | Dashboards**, then select **Guided Configuration** from the **Dashboard** drop-down and click **Start**.

2 Review the Guided Configuration overview and instructions, then click **Start**.

3 The **Software Selection** step opens. To complete this step:
   a Under the **Software Not Checked In** product category, click **Licensed** or **Evaluation** to display available products.
   b In the **Software** table, select the product you want to check in. The product description and all available components are displayed in the table below.
   c Click **Check In All** to check in product extensions to your ePolicy Orchestrator server, and product packages into your Master Repository.
   d Click **Next** at the top of the screen when you're finished checking in software and ready to move on to the next step.
4 The **System Selection** step opens. To complete this step:
   
   a Select the group in your **System Tree** where you want to add your systems. If you don't have any custom groups defined, select **My Organization**, then click **Next**. The **Adding your systems** dialogue box opens.
   
   b Select which method you want to use to add your systems to the **System Tree**:

<table>
<thead>
<tr>
<th>Add systems using…</th>
<th>To…</th>
<th>Then…</th>
</tr>
</thead>
</table>
   | AD Sync             | Synchronize your ePolicy Orchestrator server with your Active Directory (AD) server or Domain Controller (DC). If you're using one of these in your environment, AD Sync is the quickest way to add your systems to the System Tree. | 1 In the **AD Sync** dialog box, select the Synchronization type you want to use and specify the appropriate settings.  
   |                     |     | 2 Click Synchronize and Save to move on to the next step. |
   | Manual              | Manually add systems to your System Tree by specifying names or browsing a list of systems by domain. | 1 In the **New Systems** page, click **Browse** to add individual systems from a Domain and click **OK**, or type system names in the **Target systems** field.  
   |                     |     | 2 Click **Add Systems** to move on to the next step. |

5 The **Policy Configuration** step opens. To complete this step:

<table>
<thead>
<tr>
<th>Select…</th>
<th>To…</th>
<th>Then…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept Defaults</td>
<td>Use the <strong>My Default</strong> policy setting for the software you'll deploy and continue your configuration.</td>
<td>This step is complete.</td>
</tr>
</tbody>
</table>
   | Configure Policy | Specify custom policy settings now for each software product you checked in. | 1 In the **Policy Configuration** dialog box, click **OK**  
   |                |     | 2 Select a product from the **Product list** and click **My Default** to edit the default policy settings.  
   |                |     | 3 Click **Next** to move on to the next step. |
The **Software Updating** step opens. To complete this step:

<table>
<thead>
<tr>
<th>Select...</th>
<th>To...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Defaults</td>
<td>Automatically create a default product update client task that runs daily at 12:00 P.M.</td>
<td>This step is complete.</td>
</tr>
</tbody>
</table>

**Set Task Schedule**

Manually configure the schedule for your product update client task.

1. Using the **Client Task Assignment Builder**, specify a **Product** and **Task Name** for your product update task.
   - Do not change the **Task Type** selection. **Task Type** must be set to **Product Update**.
   - Configure the **Lock task inheritance** and **Tags** options, then click **Next**.
2. Specify the schedule for the update task, then click **Next**.
3. Review the summary and click **Save**.

7 The **Software Deployment** step opens. To complete this step:

a. Select the location in the **System Tree** that contains the systems where you want to deploy your software, then click **Next**. The **Software Deployment** dialog box opens. Click **OK** to continue.

b. Specify your settings for the McAfee Agent deployment, then click **Deploy**.
   - Click **Skip Agent Deployment** if you want to wait until later to perform this action. However, you must deploy agents in order to deploy your other security software.

c. The **Software Deployment** dialog box opens. Select the software packages you want to deploy to your managed systems, then click **Deploy**.

The **Configuration Summary** dialog box opens. Your configuration is complete. Click **Finish** to close the **Guided Configuration**.
Configuring general server settings

Configuring your software's general server settings is optional, but strongly recommended. Some features of your server rely on these settings to function properly.

Contents
- About general server settings
- Configuring general server settings

About general server settings
General server settings allow you to enable and customize some of your software's non-essential features and functionality.

Modify these server settings to customize some aspects of your server's behavior. For example, specifying an email server for use with your ePolicy Orchestrator server is not required. However, before your server can send an automatically generated email in response to an event in your network, you must configure the Email Server settings your McAfee ePO server needs to connect to your email server.

Configuring general server settings
General server settings control functionality that does not require specific configuration, or basic features that are not required for your server to function properly.

Use these tasks to configure your ePolicy Orchestrator server's general server settings.

Allowing agent deployment credentials to be cached
Users must provide client credentials to successfully deploy agents from your ePolicy Orchestrator server to systems in your network. You can choose whether to allow agent deployment credentials to be cached for each user.

Once a user's credentials are cached, that user can deploy agents without having to provide them again. Credentials are cached per user, so a user that has not previously provided credentials cannot deploy agents without providing their own credentials first.

Task
For option definitions, click ? in the interface.

1. Click Menu | Configuration | Server Settings, select Agent Deployment Credentials from the Setting Categories, then click Edit.

2. Select the checkbox to allow agent deployment credentials to be cached.
Specifying default dashboards and dashboard refresh intervals

The Dashboards server setting specifies the default dashboard a user sees when logging on to your server, as well as the rate at which all dashboards are refreshed.

You can specify which dashboard a user sees when they log on to your ePolicy Orchestrator server for the first time by mapping it to the user’s permission set. Mapping dashboards to permission sets ensures that users assigned a particular role are automatically presented with the information they need. Users with permission to view dashboards other than their default see the most recent dashboard they viewed each time they go to the Dashboards page.

Using the Dashboards server setting, you can also:

- Configure which dashboard is displayed to users who belong to a permission set that does not have a default dashboard assignment.
- Control the automatic refresh rate for dashboards.

Dashboards are refreshed automatically. Each time a refresh occurs, the underlying query is run, and the results displayed in the dashboard. When query results contain large amounts of data, a short refresh interval might impact available bandwidth. McAfee recommends that you choose a refresh interval (5 minutes by default) that is frequent enough to ensure accurate and timely information is displayed without consuming undue network resources.

Task

For option definitions, click ? in the interface.

1. Click Menu | Configuration | Server Settings, select Dashboards from the Setting Categories, then click Edit.
2. Select a permission set and default dashboard from the menus.
   Use + and − to add or remove multiple dashboards for each permission set, or to assignments for multiple permission sets.
3. Specify a value between 1 minute and 60 hours for the dashboard monitor refresh interval (5 minutes by default), then click Save.

Determining which events are forwarded to the server

Use this task to determine which events are forwarded to the server. This selection impacts the bandwidth used in your environment, as well as the results of event-based queries.

Task

For option definitions, click ? in the interface.

1. Click Menu | Configuration | Server Settings, select Event Filtering, then click Edit at the bottom of the page. The Edit Event Filtering page appears.
2. Select the events you want the agent to forward to the server, then click Save.

Changes to these settings take effect after all agents have communicated with the McAfee ePO server.
Choosing an ePO Notification Event interval

This setting determines how often ePO Notification Events are sent to the Automatic Response system.

There are three types of ePO Notification Events:

- **Client events** — Events that occur on managed systems. For example, "Product update succeeded."
- **Threat events** — Events that indicate a possible threat is detected. For example, "Virus detected."
- **Server events** — Events that occur on the server. For example, "Repository pull failed."

An automatic response can be triggered only after the Automatic Response system receives a notification. McAfee recommends that you specify a relatively short interval for sending these Notification events. McAfee recommends that you choose an evaluation interval that is frequent enough to ensure that the Automatic Response system can respond to an event in a timely manner, but infrequent enough to avoid excessive bandwidth consumption.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu** | **Configuration** | **Server Settings**, select **Event Notifications** from the **Setting Categories**, then click **Edit**.

2. Specify a value between 1 and 9,999 minutes for the **Evaluation Interval** (1 minute by default), then click **Save**.

Configuring settings for global updates

Global updates automate repository replication in your network. The content distributed to repositories during a global update, and whether global updates are enabled are configured using the Global Updating server setting.

Global updates are disabled by default. However, McAfee recommends that you enable and use them as part of your updating strategy. You can specify a randomization interval and package types to be distributed during the update. The randomization interval specifies the time period in which all systems are updated. Systems are updated randomly within the specified interval.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu** | **Configuration** | **Server Settings**, select **Global Updating** from the **Setting Categories**, then click **Edit**.

2. Set the status to **Enabled** and specify a **Randomization interval** between 0 and 32,767 minutes.

3. Specify which **Package types** to include in the global updates:
   - **All packages** — Select this option to include all signatures and engines, and all patches and service packs.
   - **Selected packages** — Select this option to limit the signatures and engines, and patches and service packs included in the global update.

When using global updating, McAfee recommends scheduling a regular pull task (to update the master repository) at a time when network traffic is minimal. Although global updating is much faster than other methods, it increases network traffic during the update. For more information about performing global updates, see **Global updating** under **Product and update deployment**.
Providing a license key
A license key entitles you to a full installation of the ePolicy Orchestrator software, and makes the other licensed McAfee software your company owns available in the ePolicy Orchestrator Software Manager.

Without a license key, your software runs in evaluation mode. Once the evaluation period is expired, the software ceases to function. You can add a license key at any time during the evaluation period.

Task
For option definitions, click ? in the interface.

1. Click Menu | Configuration | Server Settings, select License Key from the Setting Categories, then click Edit.
2. Type your License Key and click Save.

Creating a custom login message
Create and display a custom login message to be displayed on the Log On page.

Your message can be written in plain text, or formatted using HTML. If you create an HTML formatted message, you are responsible for all formatting and escaping.

Task
For option definitions, click ? in the interface.

1. Click Menu | Configuration | Server Settings, select Login Message from the Setting Categories, then click Edit.
2. Select Display custom login message, then type your message and click Save.

McAfee Labs Security Threats
The McAfee Labs Security Threats page informs you of the top ten medium-to-high-risk threats for corporate users. You no longer need to manually search for this information from the press (TV, radio,
newspapers), informational websites, mailing lists, or your peers. You are automatically notified of these threats from McAfee Labs.

**Protection status and risk assessment**

You can easily determine whether the DAT and engine files in the Current branch of the master repository provide protection against the top 10 threats and, if not, the highest risk level of any new threats.

**Protection available**

The DAT and engine files in the repository already provide protection against all threats that are known to McAfee Labs. To determine whether each managed system is protected, run a query against DAT and engine file coverage.

**Protection pending on Medium-to-Low Risk Threats**

The updated DAT file for threats assessed by McAfee Labs as medium risk is pending. However, updated protection is available in a supplemental virus definition (ExtraDAT) file, which you can manually download if you need protection before the next full DAT file is available, such as in an outbreak scenario.

**Protection Pending on High-Risk Threats**

The updated DAT file for threats assessed by McAfee Labs as high risk is pending. However, updated protection is available in a supplemental virus definition (ExtraDAT) file, which you can manually download if you need protection before the next full DAT file is available, such as in an outbreak scenario.

**Working with McAfee Labs Security Threats**

Use these task to mark threat notifications as read or unread or to delete them. Data is sorted by the date the threat was discovered. In addition, you can click the threat name to go to the McAfee Labs website to view information about each threat.

Each user views a McAfee Labs Security Threats page that is unique to their account. When one user deletes or marks threat notifications as read or unread, these actions are not represented in the table when another user account logs on.

**Controlling unsupported product policy visibility**

If you've been using your ePolicy Orchestrator server for a while, or you've recently updated from a previous version of the software, you might have some unsupported products installed on your server. You can control whether the policies associated with these products are visible in the Policy Catalog.

If you have unsupported products checked in to your server, you can choose whether the policies for those products are visible or hidden.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu | Configuration | Server Settings**, select **Policy Maintenance** from the **Setting Categories**, then click **Edit**.
2. Specify whether to show or hide policies for an unsupported product, optionally delete any unsupported products, then click **Save**.
Changing agent communication ports
You can change some of the ports used for agent communication on your ePolicy Orchestrator server.
You can modify the settings for these agent communication ports:

- Agent-to-server communication secure port
- Agent wake-up communication port
- Agent broadcast communication port

Task
For option definitions, click ? in the interface.

1. Click **Menu** | **Configuration** | **Server Settings**, select **Ports** from the **Setting Categories**, then click **Edit**.
2. Select whether to enable port 443 as the secure port for agent-to-server communications, type the ports to be used for agent wake-up calls and agent broadcasts, then click **Save**.

Configuring the template and location for exported reports
You can define the appearance and storage location for tables and dashboards you export as documents.
Using the Printing and Exporting server setting, you can configure:
- Headers and footers, including a custom logo, name, page numbering, etc.
- Page size and orientation for printing.
- Directory where exported tables and dashboards are stored.

Task
For option definitions, click ? in the interface.

1. Click **Menu** | **Configuration** | **Server Settings**, then select **Printing and Exporting** in the Settings list.
2. Click **Edit**. The Edit Printing and Exporting page appears.
3. In the **Headers and footers for exported documents** section, click **Edit Logo** to open the Edit Logo page.
   a. Select **Text** and type the text you want included in the document header, or do one of the following:
      - Select **Image** and browse to the image file, such as your company logo.
      - Select the default McAfee logo.
   b. Click **OK** to return to the Edit Printing and Exporting page.
4. From the drop-down lists, select any metadata that you want displayed in the header and footer.
5. Select a **Page size** and **Page orientation**.
6. Type a new location or except the default location where exported documents will be saved.
7. Click **Save**.

Using a proxy server
If you use a proxy server in your network environment, you need to specify the proxy settings in the ePolicy Orchestrator server settings.
Task
For option definitions, click ? in the interface.

1 Click Menu | Configuration | Server Settings, select Proxy Settings from the Setting Categories, then click Edit.

2 Select Configure the proxy settings manually, provide the specific configuration information your proxy server uses for each set of options, then click Save.

SSL certificates
The browsers supported by McAfee ePO show a warning about a server’s SSL certificate if it cannot verify that the certificate is valid or signed by a source that the browser trusts. By default, the McAfee ePO server uses a self-signed certificate for SSL communication with the web browser, which, by default, the browser will not trust. This causes a warning message to display every time you visit the McAfee ePO console.

To stop this warning message from appearing you must do one of the following:

• Add the McAfee ePO server certificate to the collection of trusted certificates used by the browser.

  This must be done for every browser that interacts with McAfee ePO. If the browser certificate changes, you must add the McAfee ePO server certificate again since the certificate sent by the server no longer matches the one that the browser is configured to use.

• Replace the default McAfee ePO server certificate with a valid certificate that has been signed by a certificate authority (CA) that the browser trusts. This is the best option. Because the certificate is signed by a trusted CA, you do not need to add the certificate to all web browsers within your organization.

  If the server host name changes, you can replace the server certificate with a different one that has also been signed by a trusted CA.

To replace the McAfee ePO server certificate, you must first obtain the certificate — preferably a certificate that has been signed by a trusted CA. You must also obtain the certificate’s private key and its password (if it has one). Then you can use all of these files to replace the server’s certificate. For more information on replacing server certificates, see Security keys and how they work.

The McAfee ePO browser expects the linked files to use the following format:

• Server certificate — P7B or PEM
• Private key — PEM

If the server certificate or private key are not in these formats, they must be converted to one of the supported formats before they can be used to replace the server certificate.

Replacing the server certificate
Use this task to specify the server certificate and private key used by ePolicy Orchestrator.

For option definitions, click ? in the interface.

Task
1 Click Menu | Configuration | Server Settings, then click Server Certificate in the Settings Categories list.

2 Click Edit. The Edit Server Certificate page appears.

3 Browse to the server certificate file and click Open.
4 Browse to the private key file and click Open.

5 If needed, type the private key password.

6 Click Save.

> After applying the new certificate and private key, you need to restart ePolicy Orchestrator for the change to take effect.

### Installing a trusted security certificate for the McAfee ePO browser

Use these tasks to install a trusted security certificate for your McAfee ePO browser, to stop the server certificate warning from appearing every time you log on.

### Installing the security certificate when using Internet Explorer

Use this task to install the security certificate when using supported versions of Internet Explorer, so that the warning dialog box won’t appear every time you log on.

**Task**


2. Click Continue to this website (not recommended) to open the logon page. The address bar is red, indicating the browser cannot verify the security certificate.

3. To the right of the address bar, click Certificate Error to display the Certificate Invalid warning.

4. At the bottom of the warning, click View certificates to open the Certificate dialog box.

   > Do not click Install Certificate on the General tab. If you do, the process fails.

5. Select the Certification Path tab, then select Orion_CA_<servername>, and click View Certificate. Another Certificate dialog box opens to the General tab, displaying the Certificate Information.

6. Click Install certificate to open the Certificate Import Wizard.

7. Click Next to specify where the certificate is stored.

8. Select Place all certificates in the following store, then click Browse to select a location.

9. Select the Trusted Root Certificate Authorities folder from the list, click OK, then click Next.

10. Click Finish. In the Security Warning that appears, click Yes.

11. Close the browser.

12. Change the target of the ePolicy Orchestrator desktop shortcut to use the NetBIOS name of the ePolicy Orchestrator server instead of "localhost".


Now when you log on to ePolicy Orchestrator, you are no longer prompted to accept the certificate.

### Installing the security certificate when using Firefox 3.5 or higher

Use this task to install the security certificate when using Firefox 3.5 or higher, so that the warning dialog box won’t appear every time you log on.
Task
1. From your browser, start ePolicy Orchestrator. The Secure Connection Failed page appears.

2. Click **Or you can add an exception** at the bottom of the page. The page now displays the Add Exception button.

3. Click **Add Exception**. The Add Security Exception dialog appears.

4. Click **Get Certificate**. The Certification Status information is populated and the Confirm Security Exception button is enabled.

5. Make sure that **Permanently store this exception** is selected, then click **Confirm Security Exception**.

Now when you log on to ePolicy Orchestrator, you are no longer prompted to accept the certificate.

Enabling System Tree sorting on the server

Use this task to enable System Tree sorting on the server. System Tree sorting must be enabled on the server and the desired systems for systems to be sorted.

Task
For option definitions, click ? in the interface.

1. Click **Menu | Configuration | Server Settings**, then select **System Tree Sorting** in the Setting Categories list and click **Edit**.

2. Select whether to sort systems only on the first agent-server communication or on each agent-server communication.

   If you selected to sort only on the first agent-server communication, all enabled systems are sorted on their next agent-server communication and are never sorted again for as long as this option is selected. However, these systems can be sorted again manually by taking the Sort Now action, or by changing this setting to sort on each agent-server communication.

   If you selected to sort on each agent-server communication, all enabled systems are sorted at each agent-server communication as long as this option is selected.

**ePolicy Orchestrator server settings categories and their descriptions**

These are the default server settings categories available in ePolicy Orchestrator software.

When you check in additional software to your McAfee ePO server, product-specific server settings are added to the Server settings category list. For information on product-specific server settings, see the associated product documentation. You can modify server settings from the interface by navigating to the **Server Settings** page in the **Configuration** section of the ePolicy Orchestrator interface.

**Table 4-1 Default server settings categories and their descriptions**

<table>
<thead>
<tr>
<th>Server settings category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory User Login</td>
<td>Specifies whether members of your mapped Active Directory (AD) groups can log on to your server using their AD credentials once the Active Directory User Login feature has been fully configured.</td>
</tr>
<tr>
<td>Agent Deployment Credentials</td>
<td>Specifies whether users are allowed to cache agent deployment credentials.</td>
</tr>
</tbody>
</table>
### Table 4-1  Default server settings categories and their descriptions (continued)

<table>
<thead>
<tr>
<th>Server settings category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Based Authentication</td>
<td>Specifies whether Certificate Based Authentication is enabled, and the settings and configurations required for the Certificate Authority (CA) certificate being used.</td>
</tr>
<tr>
<td>Dashboards</td>
<td>Specifies the default active dashboard that is assigned to new users’ accounts at the time of account creation, and the default refresh rate (5 minutes) for dashboard monitors.</td>
</tr>
<tr>
<td>Detected System Compliance</td>
<td>Specifies the settings that affect how rogue systems in your network are identified and treated.</td>
</tr>
<tr>
<td>Detected System Exception Categories</td>
<td>Specifies the categories that can be used to mark systems in your environment as exceptions.</td>
</tr>
<tr>
<td>Detected System Matching</td>
<td>Specifies the settings used to match detected systems and system interfaces.</td>
</tr>
<tr>
<td>Detected System OUIs</td>
<td>Specifies how your OUI (Organizationally Unique Identifier) list is updated, and when the last update occurred.</td>
</tr>
<tr>
<td>Email Server</td>
<td>Specifies the email server that is used when ePolicy Orchestrator sends email messages.</td>
</tr>
<tr>
<td>Event Filtering</td>
<td>Specifies which events are forwarded by the agent.</td>
</tr>
<tr>
<td>Event Notifications</td>
<td>Specifies the interval at which you want ePolicy Orchestrator Notification Events to be sent to Automatic Responses.</td>
</tr>
<tr>
<td>Global Updating</td>
<td>Specifies whether and how global updating is enabled.</td>
</tr>
<tr>
<td>License Key</td>
<td>Specifies the license key used to register this ePolicy Orchestrator software.</td>
</tr>
<tr>
<td>Login Message</td>
<td>Specifies the custom login message displayed, if any, to users in your environment when they navigate to the ePolicy Orchestrator console log on screen.</td>
</tr>
<tr>
<td>McAfee Labs Security Threats</td>
<td>Specifies the update frequency for the McAfee Labs Security Threats service. If proxy settings are entered in Proxy Settings, they are used while collecting McAfee Labs security threats.</td>
</tr>
<tr>
<td>Policy Maintenance</td>
<td>Specifies whether policies for unsupported products are visible or hidden. This is needed only after ePolicy Orchestrator is upgraded from a previous version.</td>
</tr>
<tr>
<td>Ports</td>
<td>Specifies the ports used by the server when it communicates with agents and the database.</td>
</tr>
<tr>
<td>Printing and Exporting</td>
<td>Specifies how information is exported to other formats, and the template for PDF exports. It also specifies the default location where the exported files are stored.</td>
</tr>
<tr>
<td>Proxy Settings</td>
<td>Specifies the type of proxy settings configured for your McAfee ePO server.</td>
</tr>
<tr>
<td>Repository Packages</td>
<td>Specifies whether any package can be checked in to any branch. Only agents later than version 3.6 can retrieve packages other than updates from branches other than Current.</td>
</tr>
<tr>
<td>Rogue System Sensor</td>
<td>Specifies the settings that define behavior for Rogue System Sensors in your network.</td>
</tr>
<tr>
<td>Security Keys</td>
<td>Specifies and manages the agent-server secure communication keys, and repository keys.</td>
</tr>
<tr>
<td>Server Certificate</td>
<td>Specifies the server certificate that your McAfee ePO server uses for HTTPS communication with browsers.</td>
</tr>
<tr>
<td>Software Evaluation</td>
<td>Specifies the required information supplied to enable check in and deployment of trial software.</td>
</tr>
</tbody>
</table>
Table 4-1  Default server settings categories and their descriptions  (continued)

<table>
<thead>
<tr>
<th>Server settings category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source Sites</td>
<td>Specifies which source sites your server connects to for updates, as well as which sites should be used as a fallback.</td>
</tr>
<tr>
<td>System Details Settings</td>
<td>Specifies which queries and systems properties are displayed in the System Details page for your managed systems.</td>
</tr>
<tr>
<td>System Tree Sorting</td>
<td>Specifies whether and how System Tree sorting is enabled in your environment.</td>
</tr>
</tbody>
</table>
Creating user accounts

User accounts provide a means for users to access and use the software. Each account is associated with one or more permission sets, which define what the user allowed to do with the software.

Contents
- About user accounts
- Working with user accounts

About user accounts
There are two types of users, global administrators and users with limited permissions.

User accounts can be created and managed in several ways. You can:

- Create user accounts manually, then assign each account an appropriate permission set.
- Configure your ePolicy Orchestrator server to allow users to log on using Windows authentication.

Allowing users to log on using their Windows credentials is an advanced feature that requires configuration and set up of multiple settings and components. For more information on this option, see Managing ePolicy Orchestrator users with Active Directory.

While user accounts and permission sets are closely related, they are created and configured using separate steps. For more information on permission sets, see Setting up permission sets.

Global administrators
Global administrators have read and write permissions and rights to all operations.

When you install the server, a global administrator account is created automatically. By default, the user name for this account is admin. If the default value is changed during installation, this account is named accordingly.

You can create additional global administrator accounts for people who require global administrator rights.

Permissions exclusive to global administrators include:

- Create, edit, and delete source and fallback sites.
- Change server settings.
- Add and delete user accounts.
- Add, delete, and assign permission sets.
- Import events into ePolicy Orchestrator databases and limit events that are stored there.
Working with user accounts

You can create, edit, and delete user accounts manually with these tasks.

Tasks

- **Creating user accounts** on page 44
  Use this task to create a user account. You must be a global administrator to add, edit, or delete user accounts.

- **Editing user accounts** on page 44
  Use this task to edit a user account. Global administrators can change passwords on any user account. Other users can only change passwords on their own accounts.

- **Deleting user accounts** on page 45
  Use this task to delete a user account. You must be a global administrator to delete user accounts.

Creating user accounts

Use this task to create a user account. You must be a global administrator to add, edit, or delete user accounts.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu** | **User Management** | **Users**, then click **New User**. The New User page appears.

2. Type a user name.

3. Select whether to enable or disable the logon status of this account. If this account is for someone who is not yet a part of the organization, you might want to disable it.

4. Select whether the new account uses McAfee ePO authentication, Windows authentication, or Certificate Based Authentication and provide the required credentials or browse and select the certificate.

5. Optionally, provide the user's full name, email address, phone number, and a description in the Notes text box.

6. Choose to make the user a global administrator, or select the appropriate permission sets for the user.

7. Click **Save** to save the current entries and return to the Users tab. The new user should appear in the Users list.

Editing user accounts

Use this task to edit a user account. Global administrators can change passwords on any user account. Other users can only change passwords on their own accounts.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu** | **User Management** | **Users**.

2. From the Users list, select the user you want to edit, then click **Actions** | **Edit**.
3 Edit the account as needed.
4 Click Save.

Deleting user accounts
Use this task to delete a user account. You must be a global administrator to delete user accounts.

McAfee recommends disabling the Login status of an account instead of deleting it, until you are sure all valuable information associated with the account has been moved to other users.

Task
For option definitions, click ? in the interface.
1 Click Menu | User Management | Users.
2 From the Users list, select the user you want to delete, then click Actions | Delete.
3 Click OK.
Setting up permission sets

Permission sets control the level of access users have to the different features available in the software. Even the smallest of ePolicy Orchestrator installations needs to specify and control the access users have to different parts of the system.

Contents
- How users, groups, and permission sets fit together
- Working with permission sets

How users, groups, and permission sets fit together

Access to items within ePolicy Orchestrator is controlled by interactions between users, groups, and permission sets.

Users

Users fall into two general categories. Either they are administrators, having full rights throughout the system, or they are regular users. Regular users can be assigned any number of permission sets to define their access levels within ePolicy Orchestrator.

Groups

Queries and reports are assigned to groups. Each group can be private (to that user only), globally public (or "shared"), or shared to one or more permission sets.

Permission sets

A particular access profile is defined within a permission set. This usually involves a combination of access levels to various parts of ePolicy Orchestrator. For example, a single permission set might grant the ability to read the Audit log, use public and shared dashboards, and create and edit public reports or queries.

Permission sets can be assigned to individual users, or if you are using Active Directory, to all users from specific Active Directory servers.

Putting the pieces together

These three objects tightly interact. Understanding the interaction is the key to controlling access within ePolicy Orchestrator. Users do not have access to an object unless they are assigned a permission set that gives them that access. That same user does not have access to any reports or queries in a group unless the group is globally public or shared to a permission set assigned to that user. Due to the interwoven nature of these objects, you might have to create and modify permission sets, groups, and users multiple times to get everything set up the way you want.
An example access configuration

As an example, let's say you want to give all users from your "Dallas" Active Directory server access to a specific group of reports, and you want one particular engineer (let's call her "ElaineG") to be able to create and modify queries in that group. To accomplish this, you'll need to create two permission sets and one group, and edit ElaineG's user account.

1. Create a permission set called "Dallas Users."
2. Add the Dallas Active Directory server to the list called Active Directory groups mapped to this permission set.
3. Make sure they have the Queries and Reports permission Use all public groups and the shared groups below; create and edit personal queries/reports. as well as other permissions you want to grant.
4. Duplicate the "Dallas Users" permission set and call the new set "Dallas Report Creators".
5. Create a query group called "Dallas Reports" and give it By permission set (Shared Groups) visibility to the "Dallas Users" and "Dallas Report Creators" permission sets.
6. In the "Dallas Users" permission set, select the "Dallas Reports" group under Queries and Reports permissions. Do the same for the "Dallas Report Creators" permission set.
7. Change the Queries and Reports permission in this new permission set to Edit public groups and the shared groups below; create and edit personal queries/reports; make personal queries/reports public. The list of selected groups should not change.
8. Edit ElaineG's user account and assign her to the "Dallas Report Creators" group.

You've now got an entire class of users (members of the "Dallas" Active Directory server) with access to a specific query group, and an individual with the ability to create and modify queries and reports within that group.
Working with permission sets

Permission sets can be created, deleted, modified, imported and exported as you can with many other objects in an ePolicy Orchestrator server.

Tasks

- **Creating a new permission set on page 49**
  Providing access levels between seeing everything or nothing requires you to create a permission set.
- **Modifying an existing permission set on page 50**
  The permissions granted within a specific permission set can be modified at any time.
- **Duplicating a permission set on page 50**
  Occasionally, the easiest way to create a new permission set is to duplicate an existing one similar to what you want.
- **Exporting permission sets on page 50**
  Once you have fully defined your permission sets, the fastest way to migrate them to other ePolicy Orchestrator servers is to export them and import them onto other servers.
- **Importing permission sets on page 51**
  Permission sets can take some time to configure, so exporting and importing them is a quick way to move this configuration from one ePolicy Orchestrator server to another.
- **Removing a permission set on page 51**
  Permission sets can be deleted when they are no longer required.
- **Deleting permission sets on page 51**
  Use this task to delete a permission set. Only global administrators can delete permission sets.

Creating a new permission set

Providing access levels between seeing everything or nothing requires you to create a permission set.

If you want to create a new permission set that is unlike other permission sets you have created to this point, starting with this task is the best approach. If you want a new permission set that is similar to another existing permission set, it is easier to duplicate that permission set and modify the duplicate.

Task

For option definitions, click ? in the interface.

1. Open the permission sets page by clicking Menu | User Management | Permission Sets.
2. Click Actions | New.
3. Enter a name for the new permission set. ePolicy Orchestrator will not allow you to use a name that already exists. Each permission set name must be unique.
4. If you want to immediately assign specific users to this permission set, select their user names in the Users section.
5. If there are any Active Directory groups where you want all users from that group mapped to this permission set, select the server from the Server Name drop-down list and click Add.
6. If you have added any Active Directory servers you want to remove, select them in the Active Directory list box click Remove.
7. Click Save to create the permission set.

At this point, you have created the permission set but have not yet assigned permissions to it.
Modifying an existing permission set

The permissions granted within a specific permission set can be modified at any time.
The need to modify a permission set can come about immediately after creating it, or changingrequirements over time.

Task
For option definitions, click ? in the interface.

1. Select a permission set by clicking Menu | User Management | Permission Sets. Select a permission set to modify.
   If you have just created a new permission set, the newly-created permission set is already selected for you.

2. Select a category of permissions to modify by clicking Edit in that category’s row.
   The options appropriate to the selected permissions category will appear.

3. Change the permissions as desired, can click Save.
   This will commit the changes to the permission set into the database.

There is no need to click a Save button when you have completed modifying the permission set. Thechanges are saved for you when modifying each individual category. The changes you make areimmediately reflected in the system, and will be propagated to the remainder of your networkaccording to your policy configuration.

Duplicating a permission set

Occasionally, the easiest way to create a new permission set is to duplicate an existing one similar towhat you want.

Task
For option definitions, click ? in the interface.

1. Click Menu | User Management | Permission Sets and then select a permission set to duplicate from thePermission Sets list.

2. Click Actions | Duplicate.

3. Choose a new name for the duplicate. By default, ePolicy Orchestrator appends (copy) to theexisting name.
   ePolicy Orchestrator will not allow you to use a name that already exists. Each permission set namemust be unique.

4. Click OK.

The permission set is duplicated, but the original is still selected in the Permission Sets list.

Exporting permission sets

Once you have fully defined your permission sets, the fastest way to migrate them to other ePolicyOrchestrator servers is to export them and import them onto other servers.

Permission sets cannot be exported individually. You can only export the entire list of permission sets at one time.
**Task**
For option definitions, click ? in the interface.

1. Select **Menu | User Management | Permission Sets**.
2. Select the permission set(s) you want to export.
3. Click **Permission Sets Actions | Export All**

   The McAfee ePO server sends an XML file to your browser. What happens next depends on your browser settings. By default, most browsers ask you to save the file.

   The XML file only contains roles with some level of permission defined. If, for example, a particular permission set has no permissions for queries and reports, no entry will appear in the file.

**Importing permission sets**
Permission sets can take some time to configure, so exporting and importing them is a quick way to move this configuration from one ePolicy Orchestrator server to another.

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

1. Select **Menu | User Management | Permission Sets**
2. Click **Permission Sets Actions | Import**.
3. Click **Browse** to navigate to and select the XML file containing the permission set you want to import.
4. Choose whether you want to keep permission sets with the same name as an imported permission set or not by selecting the appropriate option. Click **OK**.
   
   If ePolicy Orchestrator cannot locate a valid permission set within the indicated file, an error message is displayed and the import process is aborted.

   The permission sets are added to the server and displayed in the **Permission Sets** list.

**Removing a permission set**
Permission sets can be deleted when they are no longer required.

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

1. Click **Menu | User Management | Permission Sets**, then select a permission set to delete.
2. Click **Actions | Delete**, then click **OK** in the verification dialog box.

   The permission set is deleted from the system, and any objects or users that had that permission set applied to them will no longer have the access the permission set granted unless granted otherwise.

**Deleting permission sets**
Use this task to delete a permission set. Only global administrators can delete permission sets.
**Task**

For option definitions, click ? in the interface.

1. Click **Menu | User Management | Permission Sets**, then select the permission set you want to delete in the Permission Sets list. Its details appear to the right.

2. Click **Actions | Delete**, then click **OK** in the Action pane. The permission set no longer appears in the Permission Sets list.
Configuring advanced server settings

Advanced server settings enable and control the behavior of your server’s advanced features. These features allow, and often require, configuration and tuning of multiple server settings to operate correctly in your managed environment.

Contents

- Configuring Active Directory user login
- Authenticating with certificates
- Configuring Rogue System Detection server settings
- Managing security keys
- Configuring source and fallback sites

Configuring Active Directory user login

When you have many users accessing your ePolicy Orchestrator server, managing user accounts manually can be overwhelming. You can reduce the overhead of managing user accounts and access by configuring Active Directory user login.

Contents

- Managing ePolicy Orchestrator users with Active Directory
- Configuring Windows authentication and authorization

Managing ePolicy Orchestrator users with Active Directory

ePolicy Orchestrator offers the ability to dynamically create McAfee ePO users and assign permission sets to them by automatically creating users based on Windows authenticated user credentials. This process is accomplished by mapping McAfee ePO permission sets to Active Directory groups in your environment. This feature can reduce the management overhead when you have a large number of McAfee ePO users in your organization. To complete the configuration, you must work though the following process:

1. Configure user authentication.
2. Register LDAP servers.
3. Assign permission sets to the Active Directory group.

User authentication

ePolicy Orchestrator users can be authenticated with McAfee ePO password authentication or Windows authentication. If you use Windows authentication, you can specify whether users authenticate:
• Against the domain that your McAfee ePO server is joined to (default).
• Against a list of one or more domain controllers.
• Against a list of one or more DNS-style domain names.
• Using a WINS server to look up the appropriate domain controller.

If you use domain controllers, DNS-style domain names, or a WINS server, you must configure the Windows authentication server setting.

Registered LDAP servers

It is necessary to register LDAP servers with your McAfee ePO server to permit dynamically assigned permission sets for Windows users. Dynamically assigned permission sets are permission sets assigned to users based on their Active Directory group memberships.

- Users trusted via one-way external trusts are not supported.

The user account used to register the LDAP server with ePolicy Orchestrator must be trusted via a bi-directional transitive trust, or must physically exist on the domain where the LDAP server belongs.

Windows authorization

The server setting for Windows authorization specifies which Active Directory (AD) server ePolicy Orchestrator uses to gather user and group information for a particular domain. You can specify multiple domain controllers and AD servers. This server setting supports the ability to dynamically assign permission sets to users that supply Windows credentials at login.

- ePolicy Orchestrator can dynamically assign permission sets Windows Authenticated users even if Active Directory User Login is not enabled.

Assign permissions

You must assign at least one permission set to an AD group other than a user’s Primary Group. Dynamically assigning permission sets to a user’s Primary Group is not supported, and results in application of only those permissions manually assigned to the individual user. The default Primary Group is "Domain Users."

Active Directory User Login

When you have configured the previously discussed sections, you can enable the User autodiscovery server setting. User autodiscovery allows user records to be automatically created when the following conditions are met:
• Users provide valid credentials, using the <domain\name> format. For example, a user with Windows credentials jsmith1, who is a member of the Windows domain named eng, would supply the following credentials: eng\jsmith1, along with the appropriate password.

• An Active Directory server that contains information about this user has been registered with ePolicy Orchestrator.

• The user is a member of at least one Domain Local or Domain Global group that maps to an McAfee ePO permission set.

Windows authentication and authorization strategies
There are a variety of approaches you can take when planning how to register your LDAP servers. Taking the time in advance to plan your server registration strategy will help you get it right the first time and reduce user authentication problems.

Ideally, this is a process you go through once, and only change if your overall network topology changes. Once servers are registered and Windows authentication configured, you shouldn’t need to modify these settings very often.

Authentication versus authorization
Authentication involves verifying the user’s identity. This is the process of matching the credentials supplied by the user to something the system trusts as authentic. This could be an ePolicy Orchestrator server account, Active Directory credentials, or a certificate. If you want to use Windows authentication, you will need to examine how the domains (or servers) containing your user accounts are organized.

Authorization is after you’ve verified the user’s credentials. This is where permission sets are applied, determining what the user can do within the system. When using Windows authentication, you can determine what users from different domains should be authorized to do. This is done by attaching permission sets to groups contained within these domains.

User account network topology
How much effort will be required to fully configure Windows authentication and authorization depends on your network topology, and the distribution of user accounts across your network.

• If the credentials for your prospective users are all contained in a small set of domains (or servers) contained within a single domain tree, merely register the root of that tree, and you’re done.

• If your user accounts are more spread out, you will need to register a number of servers or domains. Determine the minimum number of domain (or server) sub-trees you will need and register the roots of those trees. Try to register them in the order they’ll be most used. As the authentication process goes down the list of domains (or servers) in the order they’re listed, putting the most commonly used domains at the top of the list will improve average authentication performance.

Permission structure
For users to be able to log on to an ePolicy Orchestrator server using Windows authentication, a permission set must be attached to the Active Directory group their account belongs to on their domain. When determining how permission sets should be assigned, keep in mind the following capabilities:

• Permission sets can be assigned to multiple Active Directory groups.

• Permission sets can be dynamically assigned only to an entire Active Directory group. They cannot be assigned to just some users within a group.
If you need to assign special permissions to an individual user, you can do so by creating an Active Directory group that contains only that user.

**Configuring Windows authentication and authorization**

Use these tasks to set up Active Directory User Login.

**Tasks**

- **Enabling Windows authentication in ePO Server on page 56**
  Before more advanced Windows authentication can be used, the server must be prepared.

  - **Configuring Windows authentication on page 56**
    There are multiple ways to allow users to use existing Windows account credentials within ePolicy Orchestrator.

  - **Configuring Windows authorization on page 57**
    Users attempting to log on to an ePolicy Orchestrator server using Windows authentication need a permission set assigned to one of their Active Directory groups to log on successfully.

**Enabling Windows authentication in ePO Server**

Before more advanced Windows authentication can be used, the server must be prepared.

To activate the Windows Authentication page in the server settings, you must first stop the ePolicy Orchestrator service. This task must be performed on the McAfee ePO server itself.

**Task**

For option definitions, click ? in the interface.

1. From the server console, select **Start** | **Settings** | **Control Panel** | **Administrative Tools**

2. Select **Services**.

3. In the **Services** window, right-click **McAfee ePolicy Orchestrator Applications Server** and select **Stop**.

4. Rename **Winauth.dll** to **Winauth.bak**.
   In a default installation, this file is found in `C:\Program Files\McAfee\ePolicy Orchestrator\Server\bin`.

5. Restart the server.

When you next open the **Server Settings** page, a **Windows Authentication** option appears.

**Configuring Windows authentication**

There are multiple ways to allow users to use existing Windows account credentials within ePolicy Orchestrator.

**Before you begin**

You must have first prepared your server for Windows authentication. See **Enabling Windows authentication in ePO server**.

How you configure these settings depends on several issues:
• Do you want to use multiple domain controllers?
• Do you have users spread across multiple domains?
• Do you want to use a WINS server to look up which domain your users are authenticating against?

Without any special configuration, users can authenticate using Windows credentials for the domain that the McAfee ePO server is joined to, or any domain that has a two-way trust relationship with the McAfee ePO server's domain. If you have users in domains that don't meet that criteria, you must configure Windows authentication.

For option definitions, click ? in the interface.

**Task**
1. Click Menu | Configuration | Server Settings, then select Windows Authentication from the Settings Categories list.
2. Click Edit.
3. Specify whether you want to use one or more Domains, one or more Domain controllers, or a WINS server.
   Domains must be provided in DNS format. (e.g. internaldomain.com) Domain controllers and WINS servers must have fully-qualified domain names. (e.g. dc.internaldomain.com)

   You can specify multiple domains or domain controllers, but only one WINS server. Click + to add additional domains or domain controllers to the list.

4. Click Save when you are finished adding servers.

   If you specify domains or domain controllers, the McAfee ePO server will attempt to authenticate users with servers in the order they are listed. It starts at the first server in the list and continues down the list until the user authenticates successfully.

**Configuring Windows authorization**
Users attempting to log on to an ePolicy Orchestrator server using Windows authentication need a permission set assigned to one of their Active Directory groups to log on successfully.

**Task**
For option definitions, click ? in the interface.
1. Click Menu | User Management | Permission Sets.
2. Either choose an existing permission set from the Permission Sets list and click Edit in the Name and users section, or click Actions | New.
3. Select any individual users the permission set should apply to.
4. Select a Server name from the list and click Add.
5. In the LDAP browser, navigate through the groups and select the groups to which this permission set should apply.
   Selecting an item in the Browse pane will display the members of that item in the Groups pane. You can select any number of those groups to receive the permission set dynamically. Only members from one item at a time may be added. If you need to add more, repeat steps 4 and 5 until you are finished.
6. Click Save.

   The permission set will now be applied to all users from the groups you specified logging on to the server using Windows authentication.
**Authenticating with certificates**

Client-side certificate authentication allows a client to use a digital certificate as their authentication credentials when logging on to an ePolicy Orchestrator server.

This chapter details how and when certificate authentication should be used.

**Contents**

- When to use certificate authentication
- Configuring ePolicy Orchestrator for certificate authentication
- Uploading server certificates
- Removing server certificates
- Configuring users for certificate authentication
- Problems with certificate authentication

**When to use certificate authentication**

Certificate authentication is the most secure method available. However, it is not the best choice for all environments.

Certificate authentication is an extension of public-key authentication. It uses public keys as a basis, but differs from public-key authentication in that you only need to trust a trusted third party known as a *certification authority* (or CA). Certificates are digital documents containing a combination of identity information and public keys, and are digitally signed by the CA who verifies that the information is accurate.

**Advantages of certificate-based authentication**

Certificate-based authentication has a number of advantages over password authentication:

- Certificates have predefined lifetimes. This allows for a forced, periodic review of a user's permissions when their certificate expires.

- If a user's access must be suspended or terminated, the certificate can be added to a *certificate revocation list*, or CRL, which is checked on each logon attempt to prevent unauthorized access.

- Certificate authentication is more manageable and scalable in large institutions than other forms of authentication because only a small number of CAs (frequently only one) must be trusted.

**Disadvantages of certificate-based authentication**

Not every environment is best for certificate-based authentication. Disadvantages of this method include:

- A public-key infrastructure is required. This can add additional cost that in some cases may not be worth the additional security.

- Additional overhead in maintaining certificates is required when comparing to password-based authentication.

**Configuring ePolicy Orchestrator for certificate authentication**

Before users can log on with certificate authentication, ePolicy Orchestrator must be configured properly.

**Before you begin**

You must have already received a signed certificate in P7B, PKCS12, DER, or PEM format.
Task
1 Click Menu | Configuration | Server Settings.
2 Select Certificate Based Authentication and click Edit.
3 Click Browse next to CA certificate for client certificate (P7B, PEM).
4 Navigate to and select the certificate file, then click OK.
5 If you have a Certificate Revoked List (CRL) file, click Browse next to this edit box, navigate to the CRL file, and click OK.
6 Click Save to save all changes.
7 Restart ePolicy Orchestrator to activate certificate authentication.

Uploading server certificates
Servers require certificates for SSL connections providing increased security than standard HTTP sessions.

Before you begin
To upload a signed certificate, you must have already received a server certificate from a Certificate Authority (CA).

It is possible to create self-signed certificates instead of using externally signed ones, though this carries slightly higher risk. This task can be used to initially configure certificate-based authentication, or modify an existing configuration with an updated certificate.

Task
For option definitions, click ? in the interface.
1 Click Menu | Configuration | Server Settings.
2 Select Certificate Based Authentication and click Edit.
3 Select Enable Certificate Based Authentication.
4 Click Browse next to CA certificate for client certificate (PKCS7, PEM encoded, DER encoded, or PKCS12 file with extension like .cer, .crt, . pem, .der, .p12, .p7b). Navigate to and select the certificate file and click OK.
5 If you have provided a PKCS12 certificate file, enter a password and alias name as appropriate.
6 If you want to provide a Certificate Revoked List (CRL) file, click Browse next to Certificate Revoked List file (PEM). Navigate to and select the CRL file and click OK.
   The CRL file must be in PEM format.
7 Click Save to save all changes.
8 Restart the server to enable the Certificate Based Authentication settings changes.

Removing server certificates
Server certificates can and should be removed if they are no longer used.

Before you begin
The server must already be configured for certificate authentication before you can remove server certificates.
To remove the server certificate, you must disable certificate based authentication. Once a server certificate is uploaded it can only be changed, not removed.

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

1. Open the Server Settings page by selecting **Menu | Configuration | Server Settings**.
2. Select **Certificate Based Authentication** and click **Edit**.
3. Deselect **Enable Certificate Based Authentication**, then click **Save**.

The server settings have been changed, but you must restart the server in order to complete the configuration change.

**Configuring users for certificate authentication**

Users must have certificate authentication configured before they can authenticate with their digital certificate.

Certificates used for user authentication are typically acquired with a smart card or similar device. Software bundled with the smart card hardware can extract the certificate file. This extracted certificate file is usually the file uploaded in this procedure.

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

1. Click **Menu | User Management | Users**.
2. Select a user and click **Actions | Edit**.
3. Select **Change authentication or credentials**, then select **Certificate Based Authentication**.
4. Use one of these methods to provide credentials.
   - Copy the DN field from the certificate file and paste it into the **Personal Certificate Subject DN Field** edit box.
   - Upload a certificate file. Click **Browse**, navigate to and select the certificate file on your computer, and click **OK**.

   User certificates can be PEM- or DER-encoded. The actual certificate format does not matter as long as the format is X.509 or PKCS12 compliant.

5. Click **Save** to save changes to the user's configuration.

The certificate information provided is verified, and a warning is issued if found invalid. From this point on, when the user attempts to log on to ePolicy Orchestrator from a browser that has the user's certificate installed, the log on form is greyed out and the user is immediately authenticated.

**Problems with certificate authentication**

Most authentication problems using certificates are caused by one of a small number of problems. If a user cannot log on to ePolicy Orchestrator with their certificate, try one of the following options to resolve the problem:

- Verify the user has not been disabled.
- Verify the certificate has not expired or been revoked.
- Verify the certificate is signed with the correct certificate authority.
• Verify the DN field is correct on the user configuration page.
• Verify the browser is providing the correct certificate.
• Check the audit log for authentication messages.

Configuring Rogue System Detection server settings
Rogue System Detection server settings determine how information about subnets and detected systems is displayed in the Detected Systems page within your ePolicy Orchestrator console.

Configuring server settings for Rogue System Detection
These server settings allow you to customize Rogue System Detection to meet the specific needs of your organization.

These settings control important behavior, including:
• Whether a detected system is compliant (based on last agent communication).
• The categories for system exceptions (systems that don't need an agent).
• How detected system interfaces are matched.
• The list of OUIs used to identify vendor specific NICs used by systems connecting to your network.
• How your Rogue System Sensors are configured.

Use these tasks to configure server settings for Rogue System Detection.

Tasks
• Editing Detected System Compliance on page 61
  Use this task to edit the Detected System Compliance settings. These settings are user-configured and have two important functions:
• Editing Detected System Exception Categories on page 62
• Editing Detected Systems Matching on page 62
  Use this task to edit the matching settings for Rogue System Detection. Matching settings are user-configured and have these important functions:
• Editing Detected System OUIs on page 63
  Use this task to edit the settings that specify the method and location used to update Detected System OUIs (Organizationally Unique Identifiers). Rogue System Detection uses OUIs to provide details about the systems on your network.
• Editing Rogue System Sensor settings on page 63
  Use this task to edit the sensor settings for Rogue System Detection. Sensor settings are user-configured and specify:

Editing Detected System Compliance
Use this task to edit the Detected System Compliance settings. These settings are user-configured and have two important functions:
• They specify the time-frame that determines the state of detected systems (Managed, Rogue, Exception, Inactive).
• They control the visual feedback of the Rogue System Detection status monitors on the Detected Systems page.

For option definitions, click ? in the interface.
Configuring advanced server settings
Configuring Rogue System Detection server settings

Task
1. Click Menu | Configuration | Server Settings, then in the Settings Categories list, click Detected System Compliance.
2. In the details pane, click Edit.
3. Edit the number of days to categorize Detected Systems as Managed or Inactive.

```markdown
The number of days in Rogue | Has Agent in McAfee ePO Database, but is older than__days is controlled by the number of days set in the Managed field.
```
4. Edit the percentage levels for these options, so that the color codes represent your requirements:
   - **Covered Subnets** — Required coverage.
   - **Compliant Systems** — Required compliance status.
   - **Sensor Health** — Ratio of active to missing sensors.
5. **ePO Servers** — Configure additional McAfee ePO servers whose detected systems should not be considered rogue systems.
6. Click Save.

**Editing Detected System Exception Categories**
Use this task to configure and edit the categories to use to manage exception systems in your network. Exceptions are systems that you know are unmanaged (don’t have a McAfee Agent on them).

Task
For option definitions, click ? in the interface.

1. Click Menu | Configuration | Server Settings, then from the Settings Categories list, select Detected System Exception Categories and click Edit.
2. Add or subtract exception categories using + and -.

```markdown
Use the Delete and Change links to modify existing exceptions categories.
```
3. Specify a name and description for each exception category. For example, you might want to create a category named "Printers-US-NW" to contain all the printers on your network in your company’s Northwest regional offices. This way you can keep track of these systems without receiving reports about them being rogue.
4. Click Save.

**Editing Detected Systems Matching**
Use this task to edit the matching settings for Rogue System Detection. Matching settings are user-configured and have these important functions:

- They define the properties that determine how newly detected interfaces are matched with existing systems.
- They specify static IP ranges for matching.
- They specify which ports to check for a McAfee Agent.

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

1. Click **Menu | Configuration | Server Settings**, then in the Settings Categories list select **Detected System Matching** and click **Edit**.

2. Use the **Matching Detected Systems** table to define the properties that determine when to match detected systems.

3. Use the **Matching Managed Systems** table to define the properties that determine when a newly detected interface belongs to an existing managed system.

4. In **Static IP Ranges for Matching**, type the static IP ranges to use when matching on static IP addresses.

5. In **Alternative McAfee Agent Ports**, specify any alternate ports you want to use when querying detected systems to check for a McAfee Agent.

6. Click **Save**.

**Editing Detected System OUIs**

Use this task to edit the settings that specify the method and location used to update Detected System OUIs (Organizationally Unique Identifiers). Rogue System Detection uses OUIs to provide details about the systems on your network.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu | Configuration | Server Settings**, then from the server settings Categories list, select **Detected System OUIs** and click **Edit**.

2. Choose one of the following options to specify where to update your list of OUIs:
   - **URL** — Specifies the location of an OUI.txt file to be read. The McAfee ePO server must have access to this location in order to pull the file directly from the path specified in the URL.
   - **Server location** — Specifies a location on this McAfee ePO server where the OUI.txt file is located.
   - **File upload** — Type or browse to an OUI.txt file to upload to this McAfee ePO server for processing, then click **Update**.

**Editing Rogue System Sensor settings**

Use this task to edit the sensor settings for Rogue System Detection. Sensor settings are user-configured and specify:

- The amount of time sensors are active.
- The maximum number of sensors active in each subnet.
- How long the server waits to hear from a sensor before categorizing it as missing.

For option definitions, click ? in the interface.

**Task**

1. Click **Menu | Configuration | Server Settings**, then in the Settings Categories list, select **Rogue System Sensor** and click **Edit**.

2. Edit the **Sensor Timeout** field to set the maximum amount of time the server waits for a sensor to call in before marking it as missing.
Configuring advanced server settings
Managing security keys

3. Edit the Sensors per Subnet field to set the maximum number of sensors active in each subnet, or select All sensors active.

4. Add a list of Sensor Scanning MAC addresses and OUIs that the sensors should not actively probe, regardless of the configured policy.

5. Edit the Active Period time field to set the maximum amount of time that passes before the server tells a sensor to sleep, to allow a new sensor to become active.

   The Active Period setting does not set the communication times for the active and inactive sensors. Communication time is configured using communication policy settings for Rogue System Detection.

6. Click Save.

Managing security keys

Security keys are used to verify and authenticate communications and content within your ePolicy Orchestrator managed environment.

Contents

- Security keys and how they work
- Master repository key pair
- Agent-server secure communication (ASSC) keys
- Backing up and restoring keys

Security keys and how they work

The ePolicy Orchestrator server relies on three security key pairs.

The three security pairs are used to:
- Authenticate agent-server communication.
- Verify the contents of local repositories.
- Verify the contents of remote repositories.

Each pair’s secret key signs messages or packages at their source, while the pair’s public key verifies the messages or packages at their target.

Agent-server secure communication (ASSC) keys

- The first time the agent communicates with the server, it sends its public key to the server.
- From then on, the server uses the agent public key to verify messages signed with the agent’s secret key.
- The server uses its own secret key to sign its message to the agent.
- The agent uses the server’s public key to verify the agent’s message.
- You can have multiple secure communication key pairs, but only one can be designated as the master key.
When the client agent key updater task runs (McAfee ePO Agent Key Updater), agents using different public keys receive the current public key.

If you are upgrading from ePolicy Orchestrator 4.0, the master key is unchanged. Whether or not you upgrade from version 4.0 or 4.5, the existing keys are migrated to your McAfee ePO 4.6 server.

**Local master repository key pairs**
- The repository secret key signs the package before it is checked in to the repository.
- The repository public key verifies the contents of packages in the master repository and distributed repository.
- The agent retrieves available new content each time the client update task runs.
- This key pair is unique to each server.
- By exporting and importing keys among servers, you can use the same key pair in a multi-server environment.

**Other repository key pairs**
- The secret key of a trusted source signs its content when posting that content to its remote repository. Trusted sources include the McAfee download site and the McAfee Security Innovation Alliance (SIA) repository.

  If this key is deleted, you cannot perform a pull, even if you import a key from another server. Before you overwrite or delete this key, make sure to back it up in a secure location.

- The agent public key verifies content that is retrieved from the remote repository.

**Master repository key pair**
The master repository private key signs all unsigned content in the master repository. This key is a feature of agents 4.0 and later.

Agents 4.0 and later use the public key to verify the repository content that originates from the master repository on this McAfee ePO server. If the content is unsigned, or signed with an unknown repository private key, the downloaded content is considered invalid and deleted.

This key pair is unique to each server installation. However, by exporting and importing keys, you can use the same key pair in a multi-server environment. This is a fallback measure that can help to ensure that agents can always connect to one of your master repositories, even when another repository is down.

**Other repository public keys**
Keys other than the master key pair are the public keys that agents use to verify content from other master repositories in your environment or from McAfee source sites. Each agent reporting to this server uses the keys in the **Other repository public keys** list to verify content that originates from other McAfee ePO servers in your organization, or from McAfee-owned sources.

If an agent downloads content that originated from a source where the agent does not have the appropriate public key, the agent discards the content.

These keys are a new feature, and only agents 4.0 and later are able to use the new protocols.

**Working with repository keys**
Use these tasks to work with and manage repository keys.
### Tasks

- **Using one master repository key pair for all servers on page 66**
  Use this task to ensure that all McAfee ePO servers and agents use the same master repository key pair in a multi-server environment.

- **Using master repository keys in multi-server environments on page 66**
  Use this task to ensure that agents can use content originating from any McAfee ePO server in your environment.

### Using one master repository key pair for all servers

Use this task to ensure that all McAfee ePO servers and agents use the same master repository key pair in a multi-server environment.

This consists of first exporting the key pair you want all servers to use, then importing the key pair into all other servers in your environment.

#### Task

For option definitions, click ? in the interface.

1. Click **Menu | Configuration | Server Settings**, select **Security Keys** from the Setting Categories list, then click **Edit**.
   
   The Edit Security Keys page appears.

2. Next to **Local master repository key pair**, click **Export Key Pair**.
   
   The Export Master Repository Key Pair dialog box appears.

3. Click **OK**. The File Download dialog box appears.

4. Click **Save**, browse to a location that is accessible by the other servers, where you want to save the zip file containing the secure-communication key files, then click **Save**.

5. Next to **Import and back up keys**, click **Import**.
   
   The Import Keys wizard opens.

6. Browse to the zip file containing the exported master repository key files, then click **Next**.

7. Verify that these are the keys you want to import, then click **Save**.

   The imported master repository key pair replaces the existing key pair on this server. Agents begin using the new key pair after the next agent update task runs. Once the master repository key pair is changed, an ASSC must be performed before the agent can use the new key.

### Using master repository keys in multi-server environments

Use this task to ensure that agents can use content originating from any McAfee ePO server in your environment.

The server signs all unsigned content that is checked in to the repository with the master repository private key. Agents use repository public keys to validate content that is retrieved from repositories in your organization or from McAfee source sites.

The master repository key pair is unique for each installation of ePolicy Orchestrator. If you use multiple servers, each uses a different key. If your agents can download content that originates from different master repositories, you must ensure that agents recognize the content as valid.

You can ensure this in two ways:

- Use the same master repository key pair for all servers and agents.
- Ensure agents are configured to recognize any repository public key that is used in your environment.
The following process exports the key pair from one McAfee ePO server to a target McAfee ePO server, then, at the target McAfee ePO server, imports and overwrites the existing key pair.

For option definitions, click ? in the interface.

**Task**

1. On the McAfee ePO server with the master repository key pair, click **Menu** | **Configuration** | **Server Settings**, select **Security Keys** from the Setting Categories list, then click **Edit**.
   The Edit Security Keys page appears.

2. Next to **Local master repository key pair**, click **Export Key Pair**.
   The Export Master Repository Key Pair dialog box appears.

3. Click **OK**.
   The File Download dialog box appears.

4. Click **Save**, then browse to a location on the target McAfee ePO server to save the zip file.

5. Change the name of the file if needed, then click **Save**.

6. On the target McAfee ePO server where you want to load the master repository key pair, click **Menu** | **Configuration** | **Server Settings**, select **Security Keys** from the Setting Categories list, then click **Edit**.
   The Edit Security Keys page appears.

7. Next to **Import and back up keys**, click **Import**.
   The Import Keys dialog box appears.

8. Next to **Select file**, browse to and select the master key pair file you saved, then click **Next**.
   The summary dialog box appears.

9. If the summary information appears correct, click **Save**. The new master key pair appears in the list next to **Agent-server secure communication keys**.

10. From the list, select the file you imported in the previous steps and click **Make Master**. This changes the existing master key pair to the new key pair you just imported.

11. Click **Save** to complete the process.

**Agent-server secure communication (ASSC) keys**

Agent-server secure communication (ASSC) keys are used by the agents to communicate securely with the server.

You can make any ASSC key pair the master, which is the key pair currently assigned to all deployed agents. Existing agents that use other keys in the **Agent-server secure communication keys** list do not change to the new master key unless there is a client agent key updater task scheduled and run.

- Be sure to wait until all agents have updated to the new master before deleting older keys.
- Windows agents older than version 3.6 are not supported.

**Working with ASSC keys**

Use these tasks to work with and manage ASSC keys in your environment.
Tasks

- **Deleting agent-server secure communication (ASSC) keys on page 68**
  Use this task to delete unused keys in the Agent-server secure communication keys list. Make sure that the selected key is not being used by any agent that is managed by this McAfee ePO server.

- **Exporting ASSC keys on page 68**
  Use this task to export agent-server secure communication keys from one McAfee ePO server to a different McAfee ePO server, to allow agents to access that new McAfee ePO server.

- **Importing ASSC keys on page 69**
  Use this task to import agent-server secure communication keys that were exported from a different McAfee ePO server. This procedure allows agents from that server to access this McAfee ePO server.

- **Generating and using new ASSC key pairs on page 69**
  Use this task to generate new agent-server secure communication key pairs.

- **Designating an ASSC key pair as the master on page 70**
  Use this task to change which key pair, listed in the Agent-server secure communication keys list, is specified as the master. Do this after importing or generating a new key pair.

- **Using the same ASSC key pair for all servers and agents on page 70**
  Follow this process to ensure that all McAfee ePO servers and agents use the same agent-server secure communication (ASSC) key pair.

- **Using a different ASSC key pair for each McAfee ePO server on page 71**
  Use this task to ensure that all agents can communicate with the required McAfee ePO servers in an environment where each McAfee ePO server must have a unique agent-server secure communication key pair.

- **Viewing systems that use an ASSC key pair on page 71**
  Use this task to view the systems whose agents use a specific agent-server secure communication key pair, which appears in the Agent-server secure communication keys list.

### Deleting agent-server secure communication (ASSC) keys

Use this task to delete unused keys in the Agent-server secure communication keys list. Make sure that the selected key is not being used by any agent that is managed by this McAfee ePO server.

- **Task**
  1. Click **Menu** | **Configuration** | **Server Settings**, select **Security Keys** from the Setting Categories list, then click **Edit**. The Edit Security Keys page appears.
  2. From the Agent-server secure communication keys list, select the key you want to remove, then click **Delete**. The Delete Key dialog box appears.
  3. Click **OK** to delete the key pair from this server.

### Exporting ASSC keys

Use this task to export agent-server secure communication keys from one McAfee ePO server to a different McAfee ePO server, to allow agents to access that new McAfee ePO server.

For option definitions, click ? in the interface.
Task
1. Click Menu | Configuration | Server Settings, select Security Keys from the Setting Categories list, then click Edit.
   The Edit Security Keys page appears.

2. In the Agent-server secure communication keys list, select a key, then click Export.
   The Export Agent-Server Communication Keys dialog box appears.

3. Click OK.
   Your browser prompts you to take action to download the sr<ServerName>.zip file to the specified location.

   Depending on the internet browser you are using, if you have specified a default location for all downloads this file might be automatically saved to that location.

Importing ASSC keys
Use this task to import agent-server secure communication keys that were exported from a different McAfee ePO server. This procedure allows agents from that server to access this McAfee ePO server.

For option definitions, click ? in the interface.

Task
1. Click Menu | Configuration | Server Settings, select Security Keys from the Setting Categories list, then click Edit.
   The Edit Security Keys page appears.

2. Click Import. The Import Keys page appears.

3. Browse to and select the key from the location where you saved it (by default, on the desktop), then click Open.

4. Click Next and review the information on the Import Keys page.

5. Click Save.

Generating and using new ASSC key pairs
Use this task to generate new agent-server secure communication key pairs.

For option definitions, click ? in the interface.

Task
1. Click Menu | Configuration | Server Settings, select Security Keys from the Setting Categories list, then click Edit.
   The Edit Security Keys page appears.

2. Next to the Agent-server secure communication keys list, click New Key. In the dialog box, type the name of the security key.
3 If you want existing agents to use the new key, select the key in the list, then click Make Master. Agents begin using the new key after the next agent update task is complete. If the server manages 4.6 agents, make sure the 4.6 Agent Key Updater package has been checked into the master repository.

![Warning]

In large installations, generating and using new master key pairs should be performed only when you have specific reason to do so. McAfee recommends performing this procedure in phases so you can more closely monitor progress.

4 After all agents have stopped using the old key, delete it. In the list of keys, the number of agents currently using that key is displayed to the right of every key.

5 Back up all keys.

**Designating an ASSC key pair as the master**

Use this task to change which key pair, listed in the Agent-server secure communication keys list, is specified as the master. Do this after importing or generating a new key pair.

For option definitions, click ? in the interface.

**Task**

1. Click Menu | Configuration | Server Settings, select Security Keys from the Setting Categories list, then click Edit.
   
   The Edit Security Keys page appears.

2. From the Agent-server secure communication keys list, select a key, then click Make Master.

3. Create an update task for the agents to run immediately, so that agents update after the next agent-server communication.

   Ensure that the agent key updater package is checked in to the master repository and has been replicated to all distributed repositories that are managed by ePolicy Orchestrator. Agents begin using the new key pair after the next update task for the agent is complete. At any time, you can see which agents are using any of the agent-server secure communication key pairs in the list.

4. Back up all keys.

**Using the same ASSC key pair for all servers and agents**

Follow this process to ensure that all McAfee ePO servers and agents use the same agent-server secure communication (ASSC) key pair.

![Tip]

If you have a large number of managed systems in your environment, McAfee recommends performing this process in phases so you can monitor agent updates.

1. Create an agent update task.

2. Export the keys chosen from the selected McAfee ePO server.

3. Import the exported keys to all other servers.

4. Designate the imported key as the master on all servers.

5. Perform two agent wake-up calls
6. When all agents are using the new keys, delete any unused keys.

7. Back up all keys.

---

**Using a different ASSC key pair for each McAfee ePO server**

Use this task to ensure that all agents can communicate with the required McAfee ePO servers in an environment where each McAfee ePO server must have a unique agent-server secure communication key pair.

Agents can communicate with only one server at a time. The McAfee ePO server can have multiple keys to communicate with different agents, but the opposite is not true. Agents cannot have multiple keys to communicate with multiple McAfee ePO servers.

For option definitions, click ? in the interface.

**Task**

1. From each McAfee ePO server in your environment, export the master agent-server secure communication key pair to a temporary location.

2. Import each of these key pairs into every McAfee ePO server.

---

**Viewing systems that use an ASSC key pair**

Use this task to view the systems whose agents use a specific agent-server secure communication key pair, which appears in the *Agent-server secure communication keys* list.

After making a specific key pair the master, you might want to view the systems that are still using the previous key pair. Do not delete a key pair until you know that no agents are still using it.

For option definitions, click ? in the interface.

**Task**

1. Click *Menu | Configuration | Server Settings*, select *Security Keys* from the Setting Categories list, then click *Edit*.
   
   The Edit Security Keys page appears.

2. In the *Agent-server secure communication keys* list, select a key, then click *View Agents*. The *Systems using this key* page appears.

This page lists all systems whose agents are using the selected key.

---

**Backing up and restoring keys**

Use these tasks to back up and restore security keys.
Tasks

- **Backing up all security keys on page 72**
  
  McAfee recommends periodically backing up all security keys, and always creating a backup before making any changes to the key management settings.

- **Restoring security keys on page 72**
  
  McAfee recommends periodically backing up all security keys. In the unexpected event any security keys are lost from the McAfee ePO server, you can restore them from the backup that you have stored in a secure network location.

- **Restoring security keys from a backup file on page 73**
  
  Use this task to restore all security keys from a backup file.

**Backing up all security keys**

McAfee recommends periodically backing up all security keys, and always creating a backup before making any changes to the key management settings.

Store the backup in a secure network location, so that the keys can be restored easily in the unexpected event any are lost from the McAfee ePO server.

Use this task to back up all security keys that are currently managed on this McAfee ePO server.

For option definitions, click ? in the interface.

**Task**

1. Click **Menu | Configuration | Server Settings**, select **Security Keys** from the Setting Categories list, then click **Edit**.
   
   The Edit Security Keys page appears.

2. Click **Back Up All** near the bottom of the page.
   
   The Backup Keystore dialog box appears.

3. You can optionally enter a password to encrypt the keystore ZIP file or click **OK** to save the files as unencrypted text.

4. From the File Download dialog box, click **Save** to create a zip file of all security keys.
   
   The Save As dialog box appears.

5. Browse to a secure network location to store the zip file, then click **Save**.

**Restoring security keys**

McAfee recommends periodically backing up all security keys. In the unexpected event any security keys are lost from the McAfee ePO server, you can restore them from the backup that you have stored in a secure network location.

Use this task to restore the security keys on the McAfee ePO server.

For option definitions, click ? in the interface.

**Task**

1. Click **Menu | Configuration | Server Settings**, select **Security Keys** from the Setting Categories list, then click **Edit**.
   
   The Edit Security Keys page appears.

2. Click **Restore All** near the bottom of the page.
   
   The Restore Security Keys page appears.
3. Browse to the zip file containing the security keys, select it, and click **Next**. The Restore Security Keys wizard opens to the Summary page.

4. Browse to the keys you want to replace your existing key with, then click **Next**.

5. Click **Restore**. The Edit Security Keys page reappears.

6. Browse to a secure network location to store the zip file, then click **Save**.

**Restoring security keys from a backup file**

Use this task to restore all security keys from a backup file.

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

**Task**

1. Click **Menu | Configuration | Server Settings**, select **Security Keys** from the Setting Categories list, then click **Edit**. The Edit Security Keys page appears.

2. Click **Restore All** at the bottom of the page. The Restore Security Keys wizard opens.

3. Browse to and select the backup zip file, then click **Next**.

4. Verify that the keys in this file are the ones you want to overwrite your existing keys, then click **Restore All**.

---

**Configuring source and fallback sites**

You need to configure the source and fallback sites from which your ePolicy Orchestrator server retrieves updates and signatures needed to keep your security software up-to-date.

**Working with source and fallback sites**

Use these tasks to change the default source and fallback sites. You must be a global administrator or have appropriate permissions to define, change, or delete source or fallback sites. You can edit settings, delete existing source and fallback sites, or switch between them.

McAfee recommends using the default source and fallback sites. If you require different sites for this purpose, you can create new ones.

**Tasks**

- **Creating source sites on page 74**
  Use this task to create a new source site.

- **Switching source and fallback sites on page 75**
  Use this task to change which sites are the source and fallback sites. Depending on your network configuration, you might find that HTTP or FTP updating works better. Therefore, you might want to switch the source and fallback sites.

- **Editing source and fallback sites on page 75**
  Use this task to edit the settings of source or fallback sites, such as URL address, port number, and download authentication credentials.

- **Deleting source sites or disabling fallback sites on page 75**
  Use this task to delete source sites or disable fallback sites.
Creating source sites

Use this task to create a new source site.

For option definitions, click ? in the interface.

Task

1. Click Menu | Configuration | Server Settings, then select Source Sites.

2. Click Add Source Site. The Source Site Builder wizard appears.

3. On the Description page, type a unique repository name and select HTTP, UNC, or FTP, then click Next.

4. On the Server page, provide the web address and port information of the site, then click Next.

HTTP or FTP server type:

- From the URL drop-down list, select DNS Name, IPv4, or IPv6 as the type of server address, then enter the address.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Name</td>
<td>Specifies the DNS name of the server.</td>
</tr>
<tr>
<td>IPv4</td>
<td>Specifies the IPv4 address of the server.</td>
</tr>
<tr>
<td>IPv6</td>
<td>Specifies the IPv6 address of the server.</td>
</tr>
</tbody>
</table>

- Enter the port number of the server: FTP default is 21; HTTP default is 80.

UNC server type:

- Enter the network directory path where the repository resides. Use this format: \\<COMPUTER>\<FOLDER>.

5. On the Credentials page, provide the Download Credentials used by managed systems to connect to this repository.

Use credentials with read-only permissions to the HTTP server, FTP server, or UNC share that hosts the repository.

HTTP or FTP server type:

- Select Anonymous to use an unknown user account.

- Select FTP or HTTP authentication (if the server requires authentication), then enter the user account information.

UNC server type:

- Enter domain and user account information.

6. Click Test Credentials. After a few seconds, a confirmation message appears that the site is accessible to systems using the authentication information. If credentials are incorrect, check the:

- User name and password.

- URL or path on the previous panel of the wizard.

- The HTTP, FTP or UNC site on the system.

7. Click Next.

8. Review the Summary page, then click Save to add the site to the list.
**Switching source and fallback sites**
Use this task to change which sites are the source and fallback sites. Depending on your network configuration, you might find that HTTP or FTP updating works better. Therefore, you might want to switch the source and fallback sites.

For option definitions, click ? in the interface.

**Task**
1. Click **Menu** | **Configuration** | **Server Settings**.
2. Select **Source Sites**, then click **Edit**. The Edit Source Sites page appears.
3. From the list, locate the site that you want to set as fallback, then click **Enable Fallback**.

**Editing source and fallback sites**
Use this task to edit the settings of source or fallback sites, such as URL address, port number, and download authentication credentials.

For option definitions, click ? in the interface.

**Task**
1. Click **Menu** | **Configuration** | **Server Settings**.
2. Select **Source Sites**, then click **Edit**. The Edit Source Sites page appears.
3. Locate the site in the list, then click on the name of the site. The **Source Site Builder** wizard opens.
4. Edit the settings on the wizard pages as needed, then click **Save**.

**Deleting source sites or disabling fallback sites**
Use this task to delete source sites or disable fallback sites.

For option definitions, click ? in the interface.

**Task**
1. Click **Menu** | **Configuration** | **Server Settings**.
2. Select **Source Sites**, then click **Edit**. The Edit Source Sites page appears.
3. Click **Delete** next to the required source site. The **Delete Source Site** dialog box appears.
4. Click **OK**.

The site is removed from the **Source Sites** page.
Setting up repositories

Repositories house your security software packages and updates for distribution to your managed systems.

Security software is only as effective as the latest installed updates. For example, if your DAT files are out-of-date, even the best anti-virus software cannot detect new threats. It is critical that you develop a robust updating strategy to keep your security software as current as possible.

The ePolicy Orchestrator repository architecture offers flexibility to ensure that deploying and updating software is as easy and automated as your environment allows. Once your repository infrastructure is in place, create update tasks that determine how, where, and when your software is updated.

Are you setting up repositories for the first time?

When creating and setting up repositories for the first time:

1. Decide which types of repositories to use and their locations.
2. Create and populate your repositories.

Contents

- Repository types and what they do
- How repositories work together
- Ensuring access to the source site
- Using SuperAgents as distributed repositories
- Creating and configuring FTP, HTTP, and UNC repositories
- Using local distributed repositories that are not managed
- Working with the repository list files
- Changing credentials on multiple distributed repositories
Repository types and what they do

To deliver products and updates throughout your network, the ePolicy Orchestrator software offers several types of repositories that create a robust update infrastructure when used together. These provide the flexibility to develop an updating strategy to ensure your systems stay up-to-date.

Master repository

The master repository maintains the latest versions of security software and updates for your environment. This repository is the source for the rest of your environment.

By default, ePolicy Orchestrator uses Microsoft Internet Explorer proxy settings.

Distributed repositories

Distributed repositories host copies of your master repository’s contents. Consider using distributed repositories and placing them throughout your network strategically to ensure managed systems are updated while network traffic is minimized, especially across slow connections.

As you update your master repository, ePolicy Orchestrator replicates the contents to the distributed repositories.

Replication can occur:

- Automatically when specified package types are checked in to the master repository, as long as global updating is enabled.
- On a recurring schedule with Replication tasks.
- Manually, by running a Replicate Now task.

A large organization can have multiple locations with limited bandwidth connections between them. Distributed repositories help reduce updating traffic across low bandwidth connections, or at remote sites with a large number of client systems. If you create a distributed repository in the remote location and configure the systems within that location to update from this distributed repository, the updates are copied across the slow connection only once — to the distributed repository — instead of once to each system in the remote location.

If global updating is enabled, distributed repositories update managed systems automatically, as soon as selected updates and packages are checked in to the master repository. Update tasks are not necessary. However, you do need to be running SuperAgents in your environment if you want automatic updating. You must still create and configure repositories and the update tasks.

If distributed repositories are set up to replicate only selected packages, your newly checked-in package is replicated by default. To avoid replicating a newly checked-in package, deselect it from each distributed repository or disable the replication task before checking in the package. For additional information, see Avoiding replication of selected packages and Disabling replication of selected packages.

Do not configure distributed repositories to reference the same directory as your master repository. Doing so causes the files on the master repository to become locked by users of the distributed repository, which can cause pulls and package check-ins to fail and leave the master repository in an unusable state.
**Source site**

The source site provides all updates for your master repository. The default source site is the McAfeeHttp update site, but you can change the source site or create multiple source sites if you require. McAfee recommends using the McAfeeHttp or McAfeeFtp update sites as your source site.

Source sites are not required. You can download updates manually and check them in to your master repository. However, using a source site automates this process.

McAfee posts software updates to these sites regularly. For example, DAT files are posted daily. Update your master repository with updates as they are available.

Use pull tasks to copy source site contents to the master repository.

McAfee update sites provide updates to detection definition (DAT) and scanning engine files, as well as some language packs. You must check in all other packages and updates, including service packs and patches, to the master repository manually.

**Fallback site**

The fallback site is a source site that’s been enabled as the backup site, from which managed systems can retrieve updates when their usual repositories are inaccessible. For example, when network outages or virus outbreaks occur, accessing the established location might be difficult. Therefore, managed systems can remain up-to-date in such situations. The default fallback site is the McAfeeHttp update site. You can enable only one fallback site.

If managed systems use a proxy server to access the Internet, you must configure agent policy settings for those systems to use proxy servers when accessing this fallback site.

**Types of distributed repositories**

The ePolicy Orchestrator software supports four types of distributed repositories. Consider your environment and needs when determining which type of distributed repository to use. You are not limited to using one type, and might need several, depending on your network.

**SuperAgent repositories**

Use systems hosting SuperAgents as distributed repositories. SuperAgent repositories have several advantages over other types of distributed repositories:

- Folder locations are created automatically on the host system before adding the repository to the repository list.
- File sharing is enabled automatically on the SuperAgent repository folder.
- SuperAgent repositories don’t require additional replication or updating credentials — account permissions are created when the agent is converted to a SuperAgent.

Although functionality of SuperAgent broadcast wake-up calls requires a SuperAgent in each broadcast segment, this is not a requirement for functionality of the SuperAgent repository. Managed systems only need to "see" the system hosting the repository.
FTP repositories
You can use an FTP server to host a distributed repository. Use FTP server software, such as Microsoft Internet Information Services (IIS), to create a new folder and site location for the distributed repository. See your web server documentation for details.

HTTP repositories
You can use an HTTP server to host a distributed repository. Use HTTP server software, such as Microsoft IIS, to create a new folder and site location for the distributed repository. See your web server documentation for details.

UNC share repositories
You can create a UNC shared folder to host a distributed repository on an existing server. Be sure to enable sharing across the network for the folder, so that the McAfee ePO server can copy files to it and agents can access it for updates.

Unmanaged repositories
If you are unable to use managed distributed repositories, ePolicy Orchestrator administrators can create and maintain distributed repositories that are not managed by ePolicy Orchestrator.

If a distributed repository is not managed, a local administrator must keep it up-to-date manually. Once the distributed repository is created, use ePolicy Orchestrator to configure managed systems of a specific System Tree group to update from it.

Refer to Enabling the agent on unmanaged McAfee products so that they work with ePolicy Orchestrator for configuration of unmanaged systems.

McAfee recommends that you manage all distributed repositories through ePolicy Orchestrator. This and using global updating, or scheduled replication tasks frequently, ensures your managed environment is up-to-date. Use unmanaged distributed repositories only if your network or organizational policy do not allow managed distributed repositories.

Repository branches and their purposes
The ePolicy Orchestrator software provides three repository branches, allowing you to maintain three versions of all packages in your master and distributed repositories.

The repository branches are Current, Previous, and Evaluation. By default, ePolicy Orchestrator uses only the Current branch. You can specify branches when adding packages to your master repository. You can also specify branches when running or scheduling update and deployment tasks, to distribute different versions to different parts of your network.

Update tasks can retrieve updates from any branch of the repository, but you must select a branch other than the Current branch when checking in packages to the master repository. If a non-Current branch is not configured, the option to select a branch other than Current does not appear.

To use the Evaluation and Previous branches for packages other than updates, you must configure this in the Repository Packages server settings. Agent versions 3.6 and earlier can retrieve update packages only from the Evaluation and Previous branches.
Current branch

The Current branch is the main repository branch for the latest packages and updates. Product deployment packages can be added only to the Current branch, unless support for the other branches has been enabled.

Evaluation branch

You might want to test new DAT and engine updates with a small number of network segments or systems before deploying them to your entire organization. Specify the Evaluation branch when checking in new DATs and engines to the master repository, then deploy them to a small number of test systems. After monitoring the test systems for several hours, you can add the new DATs to your Current branch and deploy them to your entire organization.

Previous branch

Use the Previous branch to save and store prior DAT and engine files before adding the new ones to the Current branch. In the event that you experience an issue with new DAT or engine files in your environment, you have a copy of a previous version that you can redeploy to your systems if necessary. ePolicy Orchestrator saves only the most immediate previous version of each file type.

You can populate the Previous branch by selecting Move existing packages to Previous branch when you add new packages to your master repository. The option is available when you pull updates from a source site and, when you manually check in packages to the Current branch.

Repository list file and its uses

The repository list (SiteList.xml and SiteMgr.xml) file contains the names of all the repositories you are managing.

The repository list includes the location and encrypted network credentials that managed systems use to select the repository and retrieve updates. The server sends the repository list to the agent during agent-server communication.

If needed, you can export the repository list to external files (SiteList.xml or SiteMgr.xml).

Use an exported SiteList.xml file to:

- Import to an agent during installation.

Use an exported SiteMgr.xml file to:

- Backup and restore your distributed repositories and source sites if you need to reinstall the server.
- Import the distributed repositories and source sites from a previous installation of the ePolicy Orchestrator software.
How repositories work together

The repositories work together in your environment to deliver updates and software to managed systems. Depending on the size and geography of your network, you might need distributed repositories.

1. The master repository regularly pulls DAT and engine update files from the source site.
2. The master repository replicates the packages to distributed repositories in the network.
3. The managed systems in the network retrieve updates from a distributed repository. If managed systems can’t access the distributed repositories or the master repository, they retrieve updates from the fallback site.

Figure 8-1 Sites and repositories delivering packages to systems

Ensuring access to the source site

Use these tasks to ensure that the McAfee ePO master repository, managed systems, and the McAfee Labs Security Threats dashboard monitor can access the Internet when using the McAfeeHttp and the McAfeeFtp sites as source and fallback sites.

This section describes the steps for configuring the McAfee ePO master repository, the McAfee Agent, and McAfee Labs Security Threats to connect to the download site directly or via a proxy. The default selection is Do not use proxy.

Tasks

- **Configuring proxy settings on page 83**
  Use this task to configure proxy settings to pull DATs for updating your repositories and to update McAfee Labs Security threats.
- **Configuring proxy settings for the McAfee Agent on page 83**
- **Configuring proxy settings for McAfee Labs Security Threats on page 84**
  Use this task to configure proxy settings for the McAfee Labs Security Threats.
Configuring proxy settings

Use this task to configure proxy settings to pull DATs for updating your repositories and to update McAfee Labs Security threats.

For option definitions, click ? in the interface.

**Task**

1. Click **Menu | Configuration | Server Settings**. The **Server Settings** page appears.

2. From the list of setting categories, select **Proxy Settings**, then click **Edit**. The **Edit Proxy Settings** page appears.

3. Select **Configure the proxy settings manually**.

4. Next to **Proxy server settings**, select whether to use one proxy server for all communication, or different proxy servers for HTTP and FTP proxy servers. Then type the IP address or fully-qualified domain name and the **Port** number of the proxy server.

   If you are using the default source and fallback sites, or if you configure another HTTP source site and FTP fallback site (or vice versa), configure both HTTP and FTP proxy authentication information here.

5. Next to **Proxy authentication**, configure the settings as appropriate, depending on whether you pull updates from HTTP repositories, FTP repositories, or both.

6. Next to **Exclusions**, select **Bypass Local Addresses**, then specify distributed repositories the server can connect to directly by typing the IP addresses or fully-qualified domain name of those systems, separated by semi-colons.

7. Click **Save**.

Configuring proxy settings for the McAfee Agent

Use this task to configure proxy settings for the McAfee Agent.

For option definitions, click ? in the interface.

**Task**

1. Click **Menu | Policy | Policy Catalog**, then from the **Product** list click **McAfee Agent**, and from the **Category** list, select **Repository**.

   A list of agents configured for the McAfee ePO server appears.

2. On the **My Default** agent, click **Edit Settings**.

   The **edit settings** page for the **My Default** agent appears.

3. Click the **Proxy** tab.

   The **Proxy Settings** page appears.

4. Select **Use Internet Explorer settings (Windows only)** for Windows systems, and select **Allow user to configure proxy settings**, if appropriate.

   There are multiple methods to configuring Internet Explorer for use with proxies. McAfee provides instructions for configuring and using McAfee products, but does not provide instructions for non-McAfee products. For information on configuring proxy settings, see Internet Explorer Help and http://support.microsoft.com/kb/226473.

5. Select **Configure the proxy settings manually** to configure the proxy settings for the agent manually.
6 Type the IP address or fully-qualified domain name and the port number of the HTTP and/or FTP source where the agent pulls updates. Select **Use these settings for all proxy types** to make these the default settings for all the proxy types.

7 Select **Specify exceptions** to designate systems that do not require access to the proxy. Use a semicolon to separate the exceptions.

8 Select **Use HTTP proxy authentication** and/or **Use FTP proxy authentication**, then provide a user name and credentials.

9 Click **Save**.

**Configuring proxy settings for McAfee Labs Security Threats**

Use this task to configure proxy settings for the McAfee Labs Security Threats.

For option definitions, click ? in the interface.

**Task**

1 Click **Menu | Configuration | Server Settings**.

2 Select **Proxy Settings** and click **Edit**.

The **Edit Proxy Settings** page appears.

3 Select **Configure the proxy settings manually**.

4 Next to **Proxy server settings**, select whether to use one proxy server for all communication, or different proxy servers for HTTP and FTP proxy servers. Then type the IP address or fully-qualified domain name and the **Port** number of the proxy server.

   If you are using the default source and fallback sites, or if you configure another HTTP source site and FTP fallback site (or vice versa), configure both HTTP and FTP proxy authentication information here.

5 Next to **Proxy authentication**, configure the settings as appropriate, depending on whether you pull updates from HTTP repositories, FTP repositories, or both.

6 Next to **Exclusions**, select **Bypass Local Addresses**, then specify any distributed repositories where the server can connect to directly by typing the IP addresses or fully-qualified domain name of those systems, separated by semicolons.

7 Click **Save**.

---

**Using SuperAgents as distributed repositories**

Use these tasks to create and configure repositories on systems that host SuperAgents. You cannot create these SuperAgents until agents have been distributed to the target systems.
Creating SuperAgent repositories on page 85

Use this task to create a SuperAgent repository. The desired system must have an McAfee ePO agent installed and running. McAfee recommends using SuperAgent repositories with global updating.

Selecting which packages are replicated to SuperAgent repositories on page 86

Use this task to select which repository-specific packages are replicated to any distributed repository.

Deleting SuperAgent distributed repositories on page 86

Use the task to remove SuperAgent distributed repositories from the host system and the repository list (SiteList.xml). New configurations take effect during the next agent-server communication.

Creating SuperAgent repositories

Use this task to create a SuperAgent repository. The desired system must have an McAfee ePO agent installed and running. McAfee recommends using SuperAgent repositories with global updating.

This task assumes that you know where the desired systems are located in the System Tree. McAfee recommends that you create a “SuperAgent” tag so that you can easily locate the systems with the Tag Catalog page, or by running a query.

For option definitions, click ? in the interface.

Task

1. Click Menu | Policy | Policy Catalog, then from the Product list click McAfee Agent, and from the Category list, select General.
   A list of agents configured for the McAfee ePO server appears.

2. Create a new policy, duplicate an existing one, or open one that’s already applied to systems that host a SuperAgent where you want to host SuperAgent repositories.

3. Select the General tab, then ensure Convert agents to SuperAgents (Windows only) is selected.

4. Select Use systems running SuperAgents as distributed repositories, then type a folder path location for the repository. This is the location where the master repository copies updates during replication. You can use standard Windows variables, such as <PROGRAM_FILES_DIR>.

   Managed systems updating from this SuperAgent repository are able to access this folder. You do not need to manually enable file sharing.

5. Click Save.

6. Assign this policy to each system that you want to host a SuperAgent repository.

The next time the agent calls in to the server, the new configuration is retrieved. When the distributed repository is created, the folder you specified is created on the system if it did not already exist. If the folder you specify cannot be created, one of two folders is created:

- <DOCUMENTS AND SETTINGS>\ ALL USERS\APPLICATION DATA\MCAFEE\FRAMEWORK\DB\SOFTWARE
- <AGENT INSTALLATION PATH>\DATA\DB\SOFTWARE

In addition, the location is added to the repository list (SiteList.xml) file. This makes the site available for updating by systems throughout your managed environment.

If you do not want to wait for the next agent-server communication, you can send an agent wake-up call to the systems.
Selecting which packages are replicated to SuperAgent repositories

Use this task to select which repository-specific packages are replicated to any distributed repository.
For option definitions, click ? in the interface

**Task**

1. Click Menu | Software | Distributed Repositories.
   A list of all distributed repositories appears.

2. Locate and click on the desired SuperAgent repository.
   The Distributed Repository Builder wizard opens.

3. On the Package Types page, select the required package types.

   Ensure that all packages required by any managed system using this repository are selected. Managed systems go to one repository for all packages — the task fails for systems that are expecting to find a package type that is not present. This feature ensures packages that are used only by a few systems are not replicated throughout your entire environment.

4. Click Save.

Deleting SuperAgent distributed repositories

Use the task to remove SuperAgent distributed repositories from the host system and the repository list (SiteList.xml). New configurations take effect during the next agent-server communication.
For option definitions, click ? in the interface.

**Task**

1. Open the desired McAfee Agent policy pages (in edit mode) from the desired assignment point in the System Tree or from the Policy Catalog page.

2. On the General tab, deselect Use systems running SuperAgents as distributed repositories, then click Save.

   To delete a limited number of your existing SuperAgent distributed repositories, duplicate the McAfee Agent policy assigned to these systems and deselect Use systems running SuperAgents as distributed repositories before saving it. Assign this new policy as needed.

   The SuperAgent repository is deleted and removed from the repository list. However, the agent still functions as a SuperAgent as long as you leave the Convert agents to SuperAgents option selected.

Creating and configuring FTP, HTTP, and UNC repositories

Use these tasks to host distributed repositories on existing FTP, HTTP servers or UNC shares. Although you do not need to use a dedicated server, the system should be powerful enough for the desired number of managed systems to connect for updates.
Tasks

- Creating a folder location on an FTP, HTTP server or UNC share on page 87
  Use this task to create the folder that hosts repository contents on the distributed repository system.

- Adding the distributed repository to ePolicy Orchestrator on page 87
  Use this task to add the new distributed repository to the repository list and configure it to use the folder you created.

- Avoiding replication of selected packages on page 89
  If distributed repositories are set up to replicate only selected packages, your newly checked-in package is replicated by default. Depending on your requirements for testing and validating, you might want to avoid replicating some packages to your distributed repositories.

- Disabling replication of selected packages on page 89

- Enabling folder sharing for UNC and HTTP repositories on page 90
  Use this task to share a folder on an HTTP or UNC distributed repository.

- Editing distributed repositories on page 90
  Use this task to edit a distributed repository.

- Deleting distributed repositories on page 90
  Use this task to delete HTTP, FTP, or UNC distributed repositories. Doing this removes them from the repository list, and removes the distributed repository contents.

Creating a folder location on an FTP, HTTP server or UNC share

Use this task to create the folder that hosts repository contents on the distributed repository system.

- For UNC share repositories, create the folder on the system and enable sharing.

- For FTP or HTTP repositories, use your existing FTP or HTTP server software, such as Microsoft Internet Information Services (IIS), to create a new folder and site location. See your web server documentation for details.

Adding the distributed repository to ePolicy Orchestrator

Use this task to add the new distributed repository to the repository list and configure it to use the folder you created.

Do not configure distributed repositories to reference the same directory as your master repository. Doing so causes the files on the master repository to become locked by users of the distributed repository, which can cause pulls and package check-ins to fail and leave the master repository in an unusable state.

Task

For option definitions, click ? in the interface.

1. Click Menu | Software | Distributed Repositories, then click Actions | New Repository. The Distributed Repository Builder wizard opens.

2. On the Description page, type a unique name and select HTTP, UNC, or FTP, then click Next. The name of the repository does not need to be the name of the system hosting the repository.
3 On the Server page, provide the web address and port information of the site.

**HTTP or FTP server type:**

- From the URL drop-down list, select **DNS Name, IPv4, or IPv6** as the type of server address, then enter the address.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Name</td>
<td>Specifies the DNS name of the server.</td>
</tr>
<tr>
<td>IPv4</td>
<td>Specifies the IPv4 address of the server.</td>
</tr>
<tr>
<td>IPv6</td>
<td>Specifies the IPv6 address of the server.</td>
</tr>
</tbody>
</table>

- Enter the port number of the server: FTP default is 21; HTTP default is 80.
- Specify the Replication UNC path for your HTTP folder.

**UNC server type**

- Enter the network directory path where the repository resides. Use this format: `\<COMPUTER>\<FOLDER>`.

4 Click **Next**.

5 On the Credentials page:

a Enter **Download credentials**. Use credentials with read-only permissions to the HTTP server, FTP server, or UNC share that hosts the repository.

**HTTP or FTP server type:**

- Select **Anonymous** to use an unknown user account.
- Select **FTP or HTTP authentication** (if the server requires authentication), then enter the user account information.

**UNC server type:**

- Select **Use credentials of logged-on account** to use the credentials of the currently logged-on user.
- Select **Enter the download credentials**, then enter domain and user account information.

b Click **Test Credentials**. After a few seconds, a confirmation message appears, stating that the site is accessible to systems using the authentication information. If credentials are incorrect, check the following:

- User name and password
- URL or path on the previous panel of the wizard
- HTTP, FTP, or UNC site on the system
Enter Replication credentials.
The server uses these credentials when it replicates DAT files, engine files, or other product updates from the master repository to the distributed repository. These credentials must have both read and write permissions for the distributed repository:

- For FTP, enter the user account information.
- For HTTP or UNC, enter domain and user account information.
- Click Test Credentials. After a few seconds, a confirmation message appears that the site is accessible to systems using the authentication information. If credentials are incorrect, check the following:
  - User name and password
  - URL or path on the previous panel of the wizard
  - HTTP, FTP, or UNC site on the system

Click Next. The Package Types page appears.

Select whether to replicate all packages or selected packages to this distributed repository, then click Next.

- If you choose the Selected packages option, you must manually select the Signatures and engines and Products, patches, service packs, etc. you want to replicate.
- Optionally select to Replicate legacy DATs.

Review the Summary page, then click Save to add the repository. The ePolicy Orchestrator software adds the new distributed repository to its database.

Avoiding replication of selected packages

If distributed repositories are set up to replicate only selected packages, your newly checked-in package is replicated by default. Depending on your requirements for testing and validating, you might want to avoid replicating some packages to your distributed repositories.

Use this task to avoid replicating a newly checked-in package.

For option definitions, click ? in the interface.

Task
1. Click Menu | Software | Distributed Repositories, then click on the desired repository. The Distributed Repository Builder wizard opens.
2. On the Package Types page, deselect the package that you want to avoid being replicated.
3. Click Save.

Disabling replication of selected packages

If distributed repositories are set up to replicate only selected packages, your newly checked-in package is replicated by default. To disable the impending replication of a package, disable the replication task before checking in the package.

Use this task to disable replication before checking in the new package.
Task
For option definitions, click ? in the interface.

1. Click Menu | Automation | Server Tasks, then select Edit next to the desired replication server task. The Server Task Builder wizard opens.

2. On the Description page, select the Schedule status as Disabled, then click Save.

**Enabling folder sharing for UNC and HTTP repositories**
Use this task to share a folder on an HTTP or UNC distributed repository.

For these repositories, the ePolicy Orchestrator software requires that the folder is enabled for sharing across the network, so that your ePolicy Orchestrator server can copy files to it. This is for replication purposes only. Managed systems configured to use the distributed repository use the appropriate protocol (HTTP, FTP, or Windows file sharing) and do not require folder sharing.

Task
1. On the managed system, locate the folder you created using Windows Explorer.
2. Right-click the folder, then select Sharing.
3. On the Sharing tab, select Share this folder.
4. Configure share permissions as needed.
   Systems updating from the repository require only read access, but administrator accounts, including the account used by the ePolicy Orchestrator server service, require write access. See your Microsoft Windows documentation to configure appropriate security settings for shared folders.
5. Click OK.

**Editing distributed repositories**
Use this task to edit a distributed repository.

Task
For option definitions, click ? in the interface.

1. Click Menu | Software | Distributed Repositories, then click the desired repository. The Distributed Repository Builder wizard opens, displaying the details of the distributed repository.
2. Change configuration, authentication, and package selection options as needed.
3. Click Save.

**Deleting distributed repositories**
Use this task to delete HTTP, FTP, or UNC distributed repositories. Doing this removes them from the repository list, and removes the distributed repository contents.
**Task**
For option definitions, click ? in the interface.

1. Click **Menu | Software | Distributed Repositories**, then click **Delete** next to the desired repository.

2. On the **Delete Repository** dialog box, click **OK**.

   - Deleting the repository does not delete the packages on the system hosting the repository.

---

**Using local distributed repositories that are not managed**

Use this task to copy contents from the master repository into the unmanaged distributed repository. Once created, you must manually configure managed systems to go to the unmanaged repository for files.

For option definitions, click ? in the interface.

**Task**

1. Copy all files and subdirectories in the master repository folder from the server.
   By default, this is in the following location on your server: `C:\Program Files\McAfee\ePO\4.6.0\DB\Software`

2. Paste the copied files and subfolders in your repository folder on the distributed repository system.

3. Configure an agent policy for managed systems to use the new unmanaged distributed repository:
   a. Click **Menu | Policy | Policy Catalog**, then select the **Product** as **McAfee Agent** and **Category** as **Repository**.

   - Policy inheritance cannot be broken for tabs of a policy. Therefore, when you apply this policy to systems, ensure that only the desired systems receive and inherit the policy to use the unmanaged distributed repository.

   b. Click on an existing agent policy or create a new agent policy.

   c. On the Repositories tab, click **Add**.
      The Add Repository window appears.

   d. Type a name in the **Repository Name** text field.
      The name does not have to be the name of the system hosting the repository.

   e. Under **Retrieve Files From**, select the type of repository.

   f. Under **Configuration**, type the location of the repository using appropriate syntax for the repository type.

   g. Type a port number or keep the default port.

   h. Configure authentication credentials as needed.

   i. Click **OK** to add the new distributed repository to the list.

   j. Select the new repository in the list.
      The type **Local** indicates it is not managed by the ePolicy Orchestrator software. When an unmanaged repository is selected in the **Repository list**, the **Edit** and **Delete** buttons are enabled.

   k. Click **Save**.

Any system where this policy is applied receives the new policy at the next agent-server communication.
Working with the repository list files

Use these tasks to export repository list files.

- SiteList.xml — For use by the agent and supported products.
- SiteMgr.xml — For use when reinstalling the McAfee ePO server, or for importing into other McAfee ePO servers that use the same distributed repositories or source sites.

Tasks

- **Exporting the repository list SiteList.xml file on page 92**
  Use this task to export the repository list (SiteList.xml) file for manual delivery to systems, or for import during the installation of supported products.

- **Exporting the repository list SiteMgr.xml file for backup or use by other servers on page 93**
  Use this task to export the list of distributed repositories and source sites as the SiteMgr.xml file. Use this file to restore the distributed repositories and source sites when you reinstall the McAfee ePO server, or when you want to share distributed repositories or source sites with another McAfee ePO server.

- **Importing distributed repositories from the SiteMgr.xml file on page 93**
  Use this task to import distributed repositories from a repository list file. This is valuable after reinstalling a server, or if you want one server to use the same distributed repositories as another server.

- **Importing source sites from the SiteMgr.xml file on page 93**
  Use this task to import source sites from a repository list file. This is valuable after reinstalling a server, or if you want one server to use the same distributed repositories as another server.

**Exporting the repository list SiteList.xml file**

Use this task to export the repository list (SiteList.xml) file for manual delivery to systems, or for import during the installation of supported products.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu | Software | Master Repository**, then click **Actions | Export Sitelist**. The File Download dialog box appears.

2. Click **Save**, browse to the location to save the SiteList.xml file, then click **Save**.

Once you have exported this file, you can import it during the installation of supported products. For instructions, see the *Installation Guide* for that product.

You can also distribute the repository list to managed systems, then apply the repository list to the agent.
Exporting the repository list SiteMgr.xml file for backup or use by other servers

Use this task to export the list of distributed repositories and source sites as the SiteMgr.xml file. Use this file to restore the distributed repositories and source sites when you reinstall the McAfee ePO server, or when you want to share distributed repositories or source sites with another McAfee ePO server.

You can export this file from either the Distributed Repositories or Source Sites pages. However, when you import this file to either page, it imports only the items from the file that are listed on that page. For example, when this file is imported to the Distributed Repositories page, only the distributed repositories in the file are imported. Therefore, if you want to import both distributed repositories and source sites, you must import the file twice, once from each page.

For option definitions, click ? in the interface.

Task
1. Click Menu | Software | Distributed Repositories (or Source Sites), then click Actions | Export Repositories (or Export Source Sites).
   The File Download dialog box appears.
2. Click Save, browse to the location to save the file, then click Save.

Importing distributed repositories from the SiteMgr.xml file

Use this task to import distributed repositories from a repository list file. This is valuable after reinstalling a server, or if you want one server to use the same distributed repositories as another server.

Task
For option definitions, click ? in the interface.
1. Click Menu | Software | Distributed Repositories, then click Actions | Import Repositories.
   The Import Repositories page appears.
2. Browse to select the exported SiteMgr.xml file, then click OK. The distributed repository is imported into the server.
3. Click OK.

The selected repositories are added to the list of repositories on this server.

Importing source sites from the SiteMgr.xml file

Use this task to import source sites from a repository list file. This is valuable after reinstalling a server, or if you want one server to use the same distributed repositories as another server.

Task
For option definitions, click ? in the interface.
1. Click Menu | Configuration | Server Settings, then from the Setting Categories list select Source Sites and click Edit.
   The Edit Source Sites page appears.
2. Click Import. The Import repositories page appears.
3. Browse to and select the exported SiteMgr.xml file, then click **OK**. The **Import Source Sites** page appears.

4. Select the desired source sites to import into this server, then click **OK**. The selected source sites are added to the list of repositories on this server.

---

**Changing credentials on multiple distributed repositories**

Use this task to change credentials on multiple distributed repositories of the same type. This task is valuable in environments where there are many distributed repositories.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu** | **Distributed Repositories**.
   The **Distributed Repositories** page appears.

2. Click **Actions** and select **Change Credentials**.
   The **Change Credentials** wizard opens to the **Repository Type** page.

3. Select the type of distributed repository for which you want to change credentials, then click **Next**. The **Repository Selection** page appears.

4. Select the desired distributed repositories, then click **Next**. The **Credentials** page appears.

5. Edit the credentials as needed, then click **Next**. The **Summary** page appears.

6. Review the information, then click **Save**.
Setting up registered servers

You can access additional servers by registering them with your McAfee ePO server. Registered servers allow you to integrate your software with other, external servers. For example, register an LDAP server to connect with your Active Directory server.

McAfee ePolicy Orchestrator can communicate with:

- Other McAfee ePO servers
- Additional, remote, database servers
- LDAP servers
- HTTP servers
- Ticketing servers

Each type of registered server supports or supplements the functionality of ePolicy Orchestrator and other McAfee and third-party extensions and products.

Registering servers

Use these tasks to register additional servers to work with ePolicy Orchestrator.

Tasks

- **Registering McAfee ePO servers on page 95**
  You can register additional McAfee ePO servers for use with your main McAfee ePO server to collect or aggregate data.

- **Registering LDAP servers on page 97**
  You must have a registered LDAP (Lightweight Directory Access Protocol) server to use Policy Assignment Rules, to enable dynamically assigned permission sets, and to enable Active Directory User Login.

- **Registering SNMP servers on page 98**
  To receive an SNMP trap, you must add the SNMP server’s information, so that ePolicy Orchestrator knows where to send the trap.

- **Registering a database server on page 99**
  Before you can retrieve data from a database server, you must register it with ePolicy Orchestrator.

Registering McAfee ePO servers

You can register additional McAfee ePO servers for use with your main McAfee ePO server to collect or aggregate data.
Setting up registered servers
Registering servers

Task
For option definitions, click ? in the interface.

1. Select Menu | Configuration | Registered Servers and click New Server.

2. From the Server type menu on the Description page, select ePO, specify a unique name and any notes, then click Next.

3. Specify the following options to configure the server:

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication type</td>
<td>Specifies the type of authentication to use for this database, including:</td>
</tr>
<tr>
<td></td>
<td>• Windows authentication</td>
</tr>
<tr>
<td></td>
<td>• SQL authentication</td>
</tr>
<tr>
<td>Client task sharing</td>
<td>Specifies whether to enable or disable client task for this server.</td>
</tr>
<tr>
<td>Database name</td>
<td>Specifies the name for this database.</td>
</tr>
<tr>
<td>Database port</td>
<td>Specifies the port for this database.</td>
</tr>
<tr>
<td>Database server</td>
<td>Specifies the name of the database for this server. You can specify a database using DNS Name or IP address (IPv4 or IPv6).</td>
</tr>
<tr>
<td>ePO Version</td>
<td>Specifies the version of the ePO server being registered.</td>
</tr>
<tr>
<td>Password</td>
<td>Specifies the password for this server.</td>
</tr>
<tr>
<td>Policy sharing</td>
<td>Specifies whether to enable or disable policy sharing for this server.</td>
</tr>
<tr>
<td>SQL Server instance</td>
<td>Allows you to specify whether this is the default server or a specific instance, by providing the Instance name.</td>
</tr>
</tbody>
</table>

Ensure that the SQL browser service is running before connecting to a specific SQL instance using its instance name. Specify the port number if the SQL browser service is not running. Select the Default SQL server instance and type the port number to connect to the SQL server instance.

<table>
<thead>
<tr>
<th>SSL communication with database server</th>
<th>Specifies whether ePolicy Orchestrator uses SSL (Secure Socket Layer) communication with this database server including:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Try to use SSL</td>
</tr>
<tr>
<td></td>
<td>• Always use SSL</td>
</tr>
<tr>
<td></td>
<td>• Never use SSL</td>
</tr>
<tr>
<td>Test connection</td>
<td>Verifies the connection for the detailed server.</td>
</tr>
</tbody>
</table>
### Option | Definition
--- | ---
**Transfer systems** | Specifies whether to enable or disable the ability to transfer systems for this server. When enabled, select **Automatic sitelist import** or **Manual sitelist import**. When choosing **Manual sitelist import**, it is possible to cause older versions of McAfee Agent (version 4.0 and earlier) to be unable to contact their Agent Handler. This may happen when:
- Transferring systems from this McAfee ePO server to the registered McAfee ePO server
- and an Agent Handler name appears alpha-numerically earlier than the ePO Server name in the supplied sitelist
- and the older Agents use that Agent Handler

**Use NTLMv2** | Optionally choose to use NT LAN Manager authentication protocol. Select this option when the server you are registering employs this protocol.

**User name** | Specifies the user name for this server.

4 Click **Save**.

### Registering LDAP servers
You must have a registered LDAP (Lightweight Directory Access Protocol) server to use Policy Assignment Rules, to enable dynamically assigned permission sets, and to enable Active Directory User Login.

**Task**

For option definitions, click ? in the interface.

1 Select **Menu | Configuration | Registered Servers**, then click **New Server**.

2 From the **Server type** menu on the **Description** page, select **LDAP Server**, specify a unique name and any details, then click **Next**.

3 Choose whether you are registering an OpenLDAP or Active Directory server in the **LDAP server type** list.

   The rest of these instructions will assume an Active Directory server is being configured. OpenLDAP-specific information is included where required.

4 Choose if you are specifying a Domain name or a specific server name in the **Server name** section. Use DNS-style domain names (e.g. internaldomain.com) and fully-qualified domain names or IP addresses for servers. (e.g. server1.internaldomain.com or 192.168.75.101)

   Using domain names gives fail-over support, and allows you to choose only servers from a specific site if desired.

   OpenLDAP servers can only use server names. They cannot be specified by domain.
5 Choose if you want to Use Global Catalog. This is deselected by default. Selecting it can provide significant performance benefits. It should only be selected if the registered domain is the parent of only local domains. If non-local domains are included, chasing referrals could cause significant non-local network traffic, possibly severely impacting performance.

Use Global Catalog is not available for OpenLDAP servers.

6 If you have chosen to not use the Global Catalog, choose whether to Chase referrals or not. Chasing referrals can cause performance problems if it leads to non-local network traffic, whether or not a Global Catalog is used.

7 Choose whether to Use SSL when communicating with this server or not.

8 If you are configuring an OpenLDAP server, enter the Port.

9 Enter a User name and Password as indicated. These credentials should be for an admin account on the server. Use domain\username format on Active Directory servers and cn=User,dc=realm,dc=com format on OpenLDAP servers.

10 Either enter a Site name for the server, or select it by clicking Browse and navigating to it.

11 Click Test Connection to verify communication with the server as specified. Alter information as necessary.

12 Click Save to register the server.

**Registering SNMP servers**

To receive an SNMP trap, you must add the SNMP server’s information, so that ePolicy Orchestrator knows where to send the trap.

For option definitions click ? in the interface.

**Task**

1 Click Menu | Configuration | Registered Servers, then click New Server.

2 From the Server type menu on the Description page, select SNMP Server, provide the name and any additional information about the server, then click Next.

3 From the URL drop-down list, select one of these types of server address, then enter the address:

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Name</td>
<td>Specifies the DNS name of the registered server.</td>
</tr>
<tr>
<td>IPv4</td>
<td>Specifies the IPv4 address of the registered server.</td>
</tr>
<tr>
<td>IPv6</td>
<td>Specifies the DNS name of the registered server which has an IPv6 address.</td>
</tr>
</tbody>
</table>

4 Select the SNMP version that your server uses:
   - If you select SNMPv1 or SNMPv2c as the SNMP server version, type the community string of the server under Security.
   - If you select SNMPv3, provide the SNMPv3 Security details.

5 Click Send Test Trap to test your configuration.

6 Click Save.
The added SNMP server appears on the Registered Server page.

**Registering a database server**
Before you can retrieve data from a database server, you must register it with ePolicy Orchestrator.

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

1. Open the Registered Servers page: select **Menu** | **Configuration** | **Registered Servers**, then click **New Server**.

2. Select **Database server** in the **Server type** drop-down list, enter a server name and an optional description, then click **Next**.

3. Choose a **Database type** from the drop-down list of registered types. Indicate if you want this database type to be as the default. If there is already a default database assigned for this database type, it is indicated in the **Current Default database for database type** row.

4. Indicate the **Database Vendor**. Currently only Microsoft SQL Server and MySQL are supported.

5. Enter the connection specifics and login credentials for the database server.

6. To verify that all connection information and login credentials are entered correctly, click **Test Connection**.
   
   A status message indicates success or failure.

7. Click **Save**.
Setting up Agent Handlers

You can create and configure multiple, remote Agent Handlers for use in your network.

Contents
- Agent Handlers and what they do
- How Agent Handlers work
- Handler groups and priority
- Working with Agent Handlers

Agent Handlers and what they do
Agent Handlers handle communication between agents and your McAfee ePO server.
Each ePolicy Orchestrator server contains a master Agent Handler. Additional Agent Handlers can be installed independently of your main McAfee ePO server on systems throughout your network.

Setting up additional Agent handlers can:
- Help manage an increased number of products and systems managed by a single, logical ePolicy Orchestrator server in situations where the CPU on the database server is not overloaded.
- Provide fault tolerant and load-balanced communication with a large number of agents, including geographically distributed agents.

How Agent Handlers work
Agent Handlers distribute network traffic, which is generated by an agent-to-server communication interval (ASCI), by assigning managed systems or groups of systems to report to a specific Agent Handler. Once assigned, a managed system performs regular agent-server communication to its Agent Handler instead of to the main McAfee ePO server.
The handler provides updated sitelists, policies, and policy assignment rules, just as the McAfee ePO server does. The handler also caches the contents of the master repository, so that agents can pull product update packages, DATs, and other necessary information.

When an agent checks in with its handler, if the handler does not have the updates needed, the handler retrieves them from the assigned repository and caches them, while passing the update through to the agent.

The Systems per agent handler chart displays all the agent handlers installed and the number of agents managed by each agent handler.
When an agent handler is uninstalled it is not displayed in this chart. If an agent handler assignment rule exclusively assigns agents to an agent handler and if the particular agent handler is uninstalled, then it is displayed in the chart as Uninstalled agent handler along with the number of agents still trying to contact this.

If the Agent Handlers are not installed correctly, then the Uninstalled Agent Handler message is displayed which indicates that the handler cannot communicate with few agents. Click on the list to view the agents which cannot communicate with the handler.

**Multiple Agent Handlers**

You can have more than one Agent Handler in you network. You might have a large number of managed systems spread across multiple geographic areas or political boundaries. Whatever the case, you can add an organization to your managed systems by assigning distinct groups to different handlers.

---

**Handler groups and priority**

When using multiple Agent Handlers in your network, you can group and prioritize them to help ensure network connectivity. Configure your handler groups to meet the specific needs of your environment. For example, you might choose to create a group of handlers in which the handlers are dispersed over a wide geographic area. With handlers dispersed, you can configure the handler priority so that agents first communicate to the handler nearest them. However, if the system in that handler area fails, the next priority handler takes over to ensure that agents can communicate.

**Handler groups**

With multiple Agent Handlers in your network, you can create handler groups. You can also apply priority to handlers in a group. Handler priority tells the agents which handler to communicate with first. If the handler with the highest priority is unavailable, the agent falls back to the next handler in the list. This priority information is contained in the repository list (sitelist.xml file) in each agent. When you change handler assignments, this file is updated as part of the agent-server commutation process. Once the assignments are received, the agent waits until the next regularly scheduled communication to implement them. You can perform an immediate agent wake-up call to update the agent immediately.

Grouping handlers and assigning priority is customizable, so you can meet the needs of your specific environment. Two common scenarios for grouping handlers are:

- **Using multiple handlers for load balancing**
  You might have a large number of managed systems in your network, for which you want to distribute the workload of agent-server communications and policy enforcement. You can configure the handler list so that agents randomly pick the handler communicate with.

- **Setting up a fallback plan to ensure agent-server communication**
  You might have systems distributed over a wide geographic area. By assigning a priority to each handler dispersed throughout this area, you can specify which handler the agents communicate with, and in what order. This can help ensure that managed systems on your network stay up-to-date by creating a fallback agent communication, much the same as fallback repositories ensure that new updates are available to your agents. If the handler with the highest priority is unavailable, the agent will fall back to the handler with the next highest priority.

In addition to assigning handler priority within a group of handlers, you can also set handler assignment priority across several groups of handlers. This adds an additional layer of redundancy to your environment to further ensure that your agents can always receive the information they need.
**Sitelist files**

The agent uses the sitelist.xml and sitelist.info files to decide which handler to communicate with. Each time handler assignments and priorities are updated, these files are updated on the managed system. Once these files are updated, the agent implements the new assignment or priority on the next scheduled agent-server communication.

---

**Working with Agent Handlers**

Use these tasks to configure and manage Agent Handlers.

**Tasks**

- **Assigning agents to Agent Handlers on page 103**
  Use this task to assign agents to specific handlers. You can assign systems individually, by group, and by subnet. Handler assignments can specify an individual handler or a list of handlers to use. The list that you specify can be made up of individual handlers or groups of handlers.

- **Managing Agent Handler assignments on page 104**
  Use this table to complete common management tasks for Agent Handler assignments. To perform these actions, click **Menu | Configuration | Agent Handlers**, then in Handler Assignment Rules, click **Actions**.

- **Setting up Agent Handler groups on page 104**
  Use this task to set up Agent Handler groups. Handler groups can make it easier to manage multiple handlers throughout your network, and can play a role in your fallback strategy.

- **Managing Agent Handler groups on page 105**
  Use this table to complete common management tasks for Agent Handler groups. To perform these actions, click **Menu | Configuration | Agent Handlers**, then click the **Handler Groups** monitor.

- **Moving agents between handlers on page 105**
  Use these tasks to assign agents to specific handlers. You can assign systems using Agent Handler assignment rules, Agent Handler assignment priority, or individually using the System Tree. Handler assignments can specify an individual handler or a list of handlers to use. The list that you specify can be made up of individual handlers or groups of handlers.

**Assigning agents to Agent Handlers**

Use this task to assign agents to specific handlers. You can assign systems individually, by group, and by subnet. Handler assignments can specify an individual handler or a list of handlers to use. The list that you specify can be made up of individual handlers or groups of handlers.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu | Configuration | Agent Handlers**, then click **Actions | New Assignment**.
2. Specify a unique name for this assignment.
3 Specify the agents for this assignment using one or both of the following **Agent Criteria** options:

- Browse to a **System Tree location**.
- Type the IP address, IP range, or subnet mask of managed systems in the **Agent Subnet** field.

4 Specify **Handler Priority** by deciding whether to:

- **Use all Agent Handlers** — Agents randomly select which handler to communicate with.
- **Use custom handler list** — When using a custom handler list, select the handler or handler group from the drop-down menu.

When using a custom handler list, use + and - to add and remove additional Agent Handlers to the list (an Agent Handler can be included in more than one group). Use the drag-and-drop handle to change the priority of handlers. Priority determines which handler the agents try to communicate with first.

### Managing Agent Handler assignments

Use this table to complete common management tasks for Agent Handler assignments. To perform these actions, click **Menu | Configuration | Agent Handlers**, then in Handler Assignment Rules, click **Actions**.

<table>
<thead>
<tr>
<th>To do this...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete a handler assignment</td>
<td>Click <strong>Delete</strong> in the selected assignment row.</td>
</tr>
<tr>
<td>Edit a handler assignment</td>
<td>Click <strong>Edit</strong> for the selected assignment. The Agent Handler Assignment page opens, where you can specify:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Assignment name</strong> — The unique name that identifies this handler assignment.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Agent criteria</strong> — The systems that are included in this assignment. You can add and remove System Tree groups, or modify the list of systems in the text box.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Handler priority</strong> — Choose whether to use all Agent Handlers or a custom handler list. Agents randomly select which handler to communicate with when <strong>Use all Agent Handlers</strong> is selected.</td>
</tr>
<tr>
<td></td>
<td>Use the drag-and-drop handle to quickly change the priority of handlers in your custom handler list.</td>
</tr>
<tr>
<td>Export handler assignments</td>
<td>Click <strong>Export</strong>. The Download Agent Handler Assignments page opens, where you can view or download the AgentHandlerAssignments.xml file.</td>
</tr>
<tr>
<td>Import handler assignments</td>
<td>Click <strong>Import</strong>. The Import Agent Handler Assignments dialog box opens, where you can browse to a previously downloaded AgentHandlerAssignments.xml file.</td>
</tr>
<tr>
<td>Edit the priority of handler assignments</td>
<td>Click <strong>Edit Priority</strong>. The Agent Handler Assignment</td>
</tr>
<tr>
<td>View the summary of a handler assignments details</td>
<td>Click &gt; in the selected assignment row.</td>
</tr>
</tbody>
</table>

### Setting up Agent Handler groups

Use this task to set up Agent Handler groups. Handler groups can make it easier to manage multiple handlers throughout your network, and can play a role in your fallback strategy.
Task
For option definitions, click ? in the interface.

1 Click Menu | Configuration | Agent Handlers, then in Handler Groups, click New Group. The Add/Edit Group page appears.

2 Specify the group name and the Included Handlers details, including:
   • Click Use load balancer to use a third-party load balancer, then type the Virtual DNS Name and Virtual IP address fields (both are required).
   • Click Use custom handler list to specify which Agent Handlers are included in this group.

   When using a custom handler list, select the handlers from the Included Handlers drop-down list. Use + and - to add and remove additional Agent Handlers to the list (an Agent Handler can be included in more than one group). Use the drag-and-drop handle to change the priority of handlers. Priority determines which handler the agents try to communicate with first.

3 Click Save.

Managing Agent Handler groups
Use this table to complete common management tasks for Agent Handler groups. To perform these actions, click Menu | Configuration | Agent Handlers, then click the Handler Groups monitor.

<table>
<thead>
<tr>
<th>To do this...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete a handler group</td>
<td>Click Delete in the selected group row.</td>
</tr>
<tr>
<td>Edit a handler group</td>
<td>Click on the handler group. The Agent Handler Group Settings page opens, where you can specify:</td>
</tr>
<tr>
<td></td>
<td>• Virtual DNS Name — The unique name that identifies this handler group.</td>
</tr>
<tr>
<td></td>
<td>• Virtual IP address — The IP address associated with this group.</td>
</tr>
<tr>
<td></td>
<td>• Included handlers — Choose whether to use a third-party load balancer or a custom handler list.</td>
</tr>
</tbody>
</table>

   Use a custom handler list to specify which handlers, and in what order, agents assigned to this group communicate with.

| Enable or disable a handler group | Click Enable or Disable in the selected group row. |

Moving agents between handlers
Use these tasks to assign agents to specific handlers. You can assign systems using Agent Handler assignment rules, Agent Handler assignment priority, or individually using the System Tree. Handler assignments can specify an individual handler or a list of handlers to use. The list that you specify can be made up of individual handlers or groups of handlers.
Tasks

- **Grouping agents using Agent Handler assignments on page 106**
  Group agents together by creating Agent Handler assignments.

- **Grouping agents by assignment priority on page 107**
  Group agents together and assigning them to an Agent Handler that is using assignment priority.

- **Grouping agents using the System Tree on page 107**
  Group agents together and assign them to an Agent Handler using the System Tree.

**Grouping agents using Agent Handler assignments**

Group agents together by creating Agent Handler assignments.

Handler assignments can specify an individual handler or a list of handlers to use. The list that you specify can be made up of individual handlers or groups of handlers.

When assigning agents to Agent Handlers, consider geographic proximity to reduce unnecessary network traffic.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu | Configuration | Agent Handlers**, then click on the required Handler Assignment Rule. The Agent Handler Assignment page appears.

   If the Default Assignment Rules is the only assignment in the list, you must create a new assignment. Refer to **Assigning agents to Agent Handlers**.

2. Type a name for the **Assignment Name**.

3. You can configure **Agent Criteria** by System Tree locations, by agent subnet, or individually using the following:
   - **System Tree Locations** — Select the group from the **System Tree location**.
     
     You can browse to select other groups from the Select System Tree and use + and - to add and remove System Tree groups that are displayed.
   - **Agent Subnet** — In the text field, type IP addresses, IP ranges, or subnet masks in the text box.
   - **Individually** — In the text field, type the IPv4/IPv6 address for a specific system.

4. You can configure Handler Priority to **Use all Agent Handlers** or **Use custom handler list**. Click **Use custom handler list**, then change the handler in one of these ways:
   - Change the associated handler by adding another handler to the list and deleting the previously associated handler.
   - Add additional handlers to the list and set the priority that the agent uses to communicate with the handlers.

   When using a custom handler list, use + and - to add and remove additional Agent Handlers from the list (an Agent Handler can be included in more than one group). Use the drag-and-drop handle to change the priority of handlers. Priority determines which handler the agents try to communicate with first.

5. Click **Save**.
**Grouping agents by assignment priority**

Group agents together and assigning them to an Agent Handler that is using assignment priority.

Handler assignments can specify an individual handler or a list of handlers to use. The list that you specify can be made up of individual handlers or groups of handlers. This list defines the order in which agents attempt to communicate using a particular Agent Handler.

> When assigning systems to Agent Handlers, consider geographic proximity to reduce unnecessary network traffic.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu | Configuration | Agent Handlers**. The Agent Handler page appears.

> If the Default Assignment Rules is the only assignment in the list, you must create a new assignment.

2. Edit assignments using the steps in the task **Grouping agents by assignment rules**.

3. As needed, modify the priority or hierarchy of the assignments by clicking **Actions | Edit Priority**.

> Moving one assignment to a priority lower than another assignment creates a hierarchy where the lower assignment is actually part of the higher assignment.

4. To change the priority of an assignment, which is shown in the Priority column on the left, do one of the following:
   - Use drag-and-drop — Use the drag-and-drop handle to drag the assignment row up or down to another position in the Priority column.
   - Click **Move to Top** — In the Quick Actions, click **Move to Top** to automatically move the selected assignment to the top priority.

5. When the priorities of the assignments are configured correctly, click **Save**.

**Grouping agents using the System Tree**

Group agents together and assign them to an Agent Handler using the System Tree.

Handler assignments can specify an individual handler or a list of handlers to use. The list that you specify can be made up of individual handlers or groups of handlers.

> When assigning systems to Agent Handlers, consider geographic proximity to reduce unnecessary network traffic.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu | Systems | System Tree | Systems**.

2. In the **System Tree** column, navigate to the system or group you want to move.

3. Use the drag-and-drop handle to move systems from the currently configured system group to the target system group.

4. Click **OK**.
11 Other important server information

Review these topics for details about other important server information.

Contents
- About Internet Protocols in managed environment
- Exporting objects from ePolicy Orchestrator
- Importing items into ePolicy Orchestrator
- Exporting objects and data from your ePolicy Orchestrator server
- ePolicy Orchestrator Log Files

About Internet Protocols in managed environment

ePolicy Orchestrator software is compatible with both Internet Protocol versions 4 and 6 (IPv4, IPv6).

ePolicy Orchestrator servers work in three different modes:
- Only IPv4 — Supports only IPv4 address format
- Only IPv6 — Supports only IPv6 address format
- Mixed mode — Supports both IPv4 and IPv6 address formats

The mode in which your ePolicy Orchestrator server works depends on your network configuration. For example, if your network is configured to use only IPv4 addresses, your server works in Only IPv4 mode. Similarly, if your network is configured to use both IPv4 and IPv6 addresses, your server works in Mixed mode.

Until IPv6 is installed and enabled, your ePolicy Orchestrator server listens only on IPv4 addresses. When IPv6 is enabled, it works in the mode in which it is configured.

When the McAfee ePO server communicates with an Agent Handler or Rogue System Sensor on IPv6, address-related properties such as IP address, subnet address, and subnet mask are reported in IPv6 format. When transmitted between client and ePolicy Orchestrator server, or when displayed in the user interface or log file, IPv6-related properties are displayed in the expanded form and are enclosed in brackets.

For example, 3FFE:85B:1F1F::A9:1234 is displayed as [3FFE:085B:1F1F:0000:0000:00A9:1234].

When setting an IPv6 address for FTP or HTTP sources, no modifications to the address are needed. However, when setting a Literal IPv6 address for a UNC source, you must use the Microsoft Literal IPv6 format. See Microsoft documentation for additional information.
Exporting objects from ePolicy Orchestrator

Frequently, the easiest and fastest way to replicate behavior from one ePolicy Orchestrator server to another is to export the item describing the behavior and import it onto the other server.

Items exported from ePolicy Orchestrator are stored in XML files that describe the exported items in detail. Objects exported from an McAfee ePO server are displayed in your browser as XML. Your browser settings determine how the XML is displayed and saved.

Exported file contents

An exported file usually contains an outer containing element named `<list>` in the event multiple items are being exported. If only a single object is exported, this outer containing element may be named after the object. (e.g. `<query>`). Any more detailed contents are variable depending on the exported item type.

Exportable items

The following items can be exported. Installed extensions may add items to this list. Please check the extension's documentation for details.

- Dashboards
- Permission Sets
- Queries
- Reports
- Server Tasks
- Users
- Automatic Responses

The following items can have a table of their current contents exported.

- Audit Log
- Issues

Importing items into ePolicy Orchestrator

Items exported from a ePolicy Orchestrator server can be imported into another server. ePolicy Orchestrator exports items into XML. These XML files contain exact descriptions of the exported items.

Importing items

When importing items into ePolicy Orchestrator, certain rules are followed:

- All items except users are imported with private visibility by default. You may apply other permissions either during or after import.
- If an item already exists with the same name, "(imported)" or "(copy)" is appended to the imported item's name.
- Imported items requiring an extension or product that does not exist on the new server will be marked invalid.
ePolicy Orchestrator will only import XML files exported by ePolicy Orchestrator.

Specific details on how to import different kinds of items can be found in the documentation for the individual items.

Exporting objects and data from your ePolicy Orchestrator server

Exported objects and data can be used for backing up important data, and to restore or configure the ePolicy Orchestrator servers in your environment.

Most objects and data used in your server can be exported or downloaded for viewing, transforming, or importing into another server or applications. The following table lists the various items you can act on. You can export to HTML and PDF files for viewing formats, or to CSV or XML files for using and transforming the data in other applications.

<table>
<thead>
<tr>
<th>Object type</th>
<th>Can be exported</th>
<th>Can be imported</th>
<th>Export format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic responses</td>
<td>X</td>
<td>X</td>
<td>xml</td>
</tr>
<tr>
<td>Client task objects</td>
<td>X</td>
<td>X</td>
<td>xml</td>
</tr>
<tr>
<td>Dashboards</td>
<td>X</td>
<td>X</td>
<td>xml</td>
</tr>
<tr>
<td>Detected System Exceptions</td>
<td>X</td>
<td>X</td>
<td>txt</td>
</tr>
<tr>
<td>Permission set definitions</td>
<td>X</td>
<td>X</td>
<td>xml</td>
</tr>
<tr>
<td>Policy objects</td>
<td>X</td>
<td>X</td>
<td>xml</td>
</tr>
<tr>
<td>Policy assignments</td>
<td>X</td>
<td>X</td>
<td>xml</td>
</tr>
<tr>
<td>Query definitions</td>
<td>X</td>
<td>X</td>
<td>xml</td>
</tr>
<tr>
<td>Query data</td>
<td>X</td>
<td></td>
<td>multiple</td>
</tr>
<tr>
<td>Reports</td>
<td>X</td>
<td>X</td>
<td>xml</td>
</tr>
<tr>
<td>Repositories</td>
<td>X</td>
<td>X</td>
<td>xml</td>
</tr>
<tr>
<td>Server tasks</td>
<td>X</td>
<td>X</td>
<td>xml</td>
</tr>
<tr>
<td>Site lists</td>
<td>X</td>
<td>X</td>
<td>xml</td>
</tr>
<tr>
<td>Subnets (in the form of a list)</td>
<td>X</td>
<td>X</td>
<td>txt</td>
</tr>
<tr>
<td>Systems (in the form of a list, from the System Tree)</td>
<td>X</td>
<td>X</td>
<td>txt</td>
</tr>
<tr>
<td>Tables (in the form of a report or list)</td>
<td>X</td>
<td></td>
<td>multiple</td>
</tr>
<tr>
<td>Tags</td>
<td>X</td>
<td>X</td>
<td>xml</td>
</tr>
</tbody>
</table>

Task

1. From the page displaying the objects or data, click Actions and select the desired option. For example, when exporting a table, select Export Table and click next.

2. When exporting content that can be downloaded in multiple formats, such as Query data, an Export page with configuration options is opened. Specify your preferences and click Export.

3. When exporting objects or definitions, such as client task objects or definitions one of the following occurs:
   - A browser dialog box opens where you can choose whether to Open or Save the file.
   - An Export page containing a link to the file opens. Left-click the link to view the file in your browser. Right-click the link to Save the file.
ePolicy Orchestrator Log Files

Your ePolicy Orchestrator server maintains log files that chronicle various kinds of events and actions going on within the system.

Contents
  ▶ The Audit Log
  ▶ The Server Task log
  ▶ The Threat Event Log

The Audit Log

Use the Audit Log to maintain and access a record of all McAfee ePO user actions. The Audit Log entries are displayed in a sortable table. For added flexibility, you can also filter the log so that it displays only failed actions, or only entries that are within a certain age.

The Audit Log displays seven columns:

- **Action** — The name of the action the McAfee ePO user attempted.
- **Completion Time** — The time the action finished.
- **Details** — More information about the action.
- **Priority** — Importance of the action.
- **Start Time** — The time the action was initiated.
- **Success** — Whether the action was successfully completed.
- **UserName** — User name of the logged-on user account that was used to take the action.

Audit Log entries can be queried against. You can create queries with the Query Builder wizard that target this data, or you can use the default queries that target this data. For example, the Failed Logon Attempts query retrieves a table of all failed logon attempts.

Working with the Audit Log

Use these tasks to view and purge the Audit Log. The Audit Log records actions taken by McAfee ePO users.

Tasks

- **Viewing the Audit Log on page 112**
  Use this task to view a history of administrator actions. Available data depends on how often and by what age the Audit Log is purged.

- **Purging the Audit Log on page 113**
  Use this task to purge the Audit Log. You can only purge Audit Log records by age. When you purge the Audit Log, the records are deleted permanently.

- **Purging the Audit Log on a schedule on page 113**
  Use this task to purge the Audit Log with a scheduled server task.

Viewing the Audit Log

Use this task to view a history of administrator actions. Available data depends on how often and by what age the Audit Log is purged.
**Task**

For option definitions, click ? in the interface.

1. Click Menu | User Management | Audit Log. The details of administrator actions are displayed in a table.
2. Click any of the column titles to sort the table by that column (alphabetically).
3. From the Filter drop-down list, select an option to narrow the amount of visible data. You can remove all but the failed actions, or show only actions that occurred within a selected amount of time.
4. Click any entry to view its details.

**Purging the Audit Log**

Use this task to purge the Audit Log. You can only purge Audit Log records by age. When you purge the Audit Log, the records are deleted permanently.

**Task**

For option definitions, click ? in the interface.

1. Click Menu | User Management | Audit Log.
2. Click Actions | Purge.
3. In the Purge dialog box, next to Purge records older than, type a number and select a time unit.
4. Click OK.

All records older than the specified timeframe are purged.

**Purging the Audit Log on a schedule**

Use this task to purge the Audit Log with a scheduled server task.

**Task**

For option definitions, click ? in the interface.

1. Click Menu | Automation | Server Tasks, then click Actions | New Task. The Server Task Builder wizard opens to the Description page.
2. Name, describe the task, and click Enabled after Schedule Status.
3. Click Next. The Actions page appears.
4. Select Purge Audit Log from the drop-down list.
5. After Purge records older than, type a number and select the time unit to use before purging the Audit Log entries.
6. Click Next. The Schedule page appears.
7. Schedule the task as needed, then click Next. The Summary page appears.
8. Review the task's details, then click Save.
The Server Task log
The Server Task log reports on events that occur on your ePolicy Orchestrator server.
From the server task log you can view the detailed results of scheduled server tasks that are running or have been run on your server. Entries in the log provides details about:

• The success or failure of the task
• Any subtasks run when performing the scheduled task

You can also terminate a task that is currently in progress.

Working with the Server Task Log
Use these tasks to view and maintain the Server Task Log.

Tasks
• Viewing the Server Task Log on page 114
Use this task to review the status of server tasks and long-running actions.
• Filtering the Server Task Log on page 115
As the Server Task Log grows, you can filter it to show only the most recent activity. You can filter the log to show only entries from the last day, last seven days, last 30 days, or by Failed or In Progress task status.
• Purging the Server Task Log on page 115
As the Server Task Log grows, you can purge items older than a specified (user-configurable) number of days, weeks, months, or years.

Viewing the Server Task Log
Use this task to review the status of server tasks and long-running actions.

The status of each server task appears in the Status column:

• Completed — Task completed successfully.
• Failed — Task was started but did not complete successfully.
• In progress — Task has started but not finished.
• Waiting — Task is waiting for another task to finish.
• Terminated — Task was terminated manually before it finished.

For option definitions, click ? in the interface.

Task
1 Click Menu | Automation | Server Task Log. The Server Task Log display appears.
2 Click any of the column titles to sort the events.
3 Select any of the task logs, click Actions, then select one of the following to manipulate the server task log:
   • Choose Columns — The Select Columns to Display page appears.
   • Export Table — The Export page appears.
   • Purge — The Purge dialog box appears. Type a number and a time unit to determine the number of task log entries to delete, then click OK.
   • Terminate Task — Stop a task that is in progress.
Filtering the Server Task Log
As the Server Task Log grows, you can filter it to show only the most recent activity. You can filter the log to show only entries from the last day, last seven days, last 30 days, or by Failed or In Progress task status.

Task
For option definitions, click ? in the interface.
1. Click Menu | Automation | Server Task Log.
2. Select the desired filter from the Filter drop-down list.

Purging the Server Task Log
As the Server Task Log grows, you can purge items older than a specified (user-configurable) number of days, weeks, months, or years.

Task
For option definitions, click ? in the interface.
1. Click Menu | Automation | Server Task Log, then click Actions | Purge.
2. In the Purge dialog box, type a number of days, weeks, months, or years. Any item of this age and older are deleted.
3. Click OK.

Allowed Cron syntax when scheduling a server task
Cron syntax is made up of six or seven fields, separated by a space. Accepted Cron syntax, by field in descending order, is detailed in the following table. Most Cron syntax is acceptable, but a few cases are not supported. For example, you cannot specify both the Day of Week and Day of Month values.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Allowed Values</th>
<th>Allowed Special Characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seconds</td>
<td>0 - 59</td>
<td>, - * /</td>
</tr>
<tr>
<td>Minutes</td>
<td>0 - 59</td>
<td>, - * /</td>
</tr>
<tr>
<td>Hours</td>
<td>0 - 23</td>
<td>, - * /</td>
</tr>
<tr>
<td>Day of Month</td>
<td>1 - 31</td>
<td>, - * ? / L W C</td>
</tr>
<tr>
<td>Month</td>
<td>1 - 12, or JAN - DEC</td>
<td>, - * /</td>
</tr>
<tr>
<td>Day of Week</td>
<td>1 - 7, or SUN - SAT</td>
<td>, - * ? / L C #</td>
</tr>
<tr>
<td>Year (optional)</td>
<td>Empty, or 1970 - 2099</td>
<td>, - * /</td>
</tr>
</tbody>
</table>

Notes on allowed special characters
- Commas (,) are allowed to specify additional values. For example, "5,10,30" or "MON,WED,FRI".
- Asterisks (*) are used for "every." For example, ":*" in the minutes field is "every minute".
- Question marks (?) are allowed to specify no specific value in the Day of Week or Day of Month fields.
  - The question mark must be used in one of these fields, but cannot be used in both.
- Forward slashes (/) identify increments. For example, "5/15" in the minutes field means the task runs at minutes 5, 20, 35 and 50.
• The letter "L" means "last" in the Day of Week or Day of Month fields. For example, "0 15 10 ? * 6L" means the last Friday of every month at 10:15 am.

• The letter "W" means "weekday". So, if you created a Day of Month as "15W", this means the weekday closest to the 15th of the month. Also, you can specify "LW", which means the last weekday of the month.

• The pound character "#" identifies the "Nth" day of the month. For example, using "6#3" in the Day of Week field is the third Friday of every month, "2#1" is the first Monday, and "4#5" is the fifth Wednesday.

If the month does not have a fifth Wednesday, the task does not run.

The Threat Event Log

Use the Threat Event Log to quickly view and sort through events in the database. The log can be purged only by age.

You can choose which columns are displayed in the sortable table. You can choose from a variety of event data to use as columns.

Depending on which products you are managing, you can also take certain actions on the events. Actions are available in the Actions menu at the bottom of the page.

Common event format

Most managed products now use a common event format. The fields of this format can be used as columns in the Threat Event Log. These include:

• **Action Taken** — Action that was taken by the product in response to the threat.

• **Agent GUID** — Unique identifier of the agent that forwarded the event.

• **DAT Version** — DAT version on the system that sent the event.

• **Detecting Product Host Name** — Name of the system hosting the detecting product.

• **Detecting Product ID** — ID of the detecting product.

• **Detecting Product IPv4 Address** — IPv4 address of the system hosting the detecting product (if applicable).

• **Detecting Product IPv6 Address** — IPv6 address of the system hosting the detecting product (if applicable).

• **Detecting Product MAC Address** — MAC address of the system hosting the detecting product.

• **Detecting Product Name** — Name of the detecting managed product.

• **Detecting Product Version** — Version number of the detecting product.

• **IPv4 Address** — IPv4 address of the system which sent the event.

• **IPv6 Address** — IPv6 address of the system which sent the event.

• **MAC Address** — MAC address of the system which sent the event.

• **Network Protocol** — Threat target protocol for network-homed threat classes.

• **Port Number** — Threat target port for network-homed threat classes.

• **Process Name** — Target process name (if applicable).

• **Server ID** — Server ID which sent the event.

• **Threat Name** — Name of the threat.

• **Threat Source Host Name** — System name from which the threat originated.

• **Threat Source IPv4 Address** — IPv4 address of the system from which the threat originated.
• **Engine Version** — Version number of the detecting product’s engine (if applicable).

• **Event Category** — Category of the event. Possible categories depend on the product.

• **Event Generated Time (UTC)** — Time in Coordinated Universal Time that the event was detected.

• **Event ID** — Unique identifier of the event.

• **Event Received Time (UTC)** — Time in Coordinated Universal Time that the event was received by the McAfee ePO server.

• **File Path** — File path of the system which sent the event.

• **Host Name** — Name of the system which sent the event.

• **Threat Source IPv6 Address** — IPv6 address of the system from which the threat originated.

• **Threat Source MAC Address** — MAC address of the system from which the threat originated.

• **Threat Source URL** — URL from which the threat originated.

• **Threat Source User Name** — User name from which the threat originated.

• **Threat Type** — Class of the threat.

• **User Name** — Threat source user name or email address.

---

**Working with the Threat Event Log**

Use these tasks to view and purge the Threat Event Log.

**Tasks**

- **Viewing the Threat Event Log on page 117**
  Use this task to view the Threat Event Log.

- **Purging Threat Events on page 117**
  Use this task to purge Threat Event records from the database. Purging Threat Event records deletes them permanently.

- **Purging the Threat Event Log on a schedule on page 118**
  Use this task to purge the Threat Event Log with a scheduled server task.

**Viewing the Threat Event Log**

Use this task to view the Threat Event Log.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu | Reporting | Threat Event Log**.

2. Click any of the column titles to sort the events. You can also click **Actions | Choose Columns** and the Select Columns to Display page appears.

3. From the Available Columns list, select different table columns that meet your needs, then click **Save**.

4. Select events in the table, then click **Actions** and select **Show Related Systems** to see the details of the systems that sent the selected events.

**Purging Threat Events**

Use this task to purge Threat Event records from the database. Purging Threat Event records deletes them permanently.
**Task**
For option definitions, click ? in the interface.

1. Click Menu | Reporting | Threat Event Log.
2. Click Actions | Purge.
3. In the Purge dialog box, next to Purge records older than, type a number and select a time unit.
4. Click OK.

Records older than the specified age are deleted permanently.

**Purging the Threat Event Log on a schedule**
Use this task to purge the Threat Event Log with a scheduled server task.

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

1. Click Menu | Automation | Server Tasks, then click Actions | New Task. The Server Task Builder wizard opens to the Description page.
2. Name, describe the task, and click Enabled after Schedule Status.
3. Click Next. The Actions page appears.
4. Select Purge Threat Event Log from the drop-down list.
5. Select whether to purge by age or from a queries results. If you purge by query, you must pick a query that results in a table of events.
6. Click Next. The Schedule page appears.
7. Schedule the task as needed, then click Next. The Summary page appears.
8. Review the task’s details, then click Save.
Managing your network security with your ePolicy Orchestrator server

Your ePolicy Orchestrator server makes deploying products to your systems and keeping them updated with the latest content from McAfee is an essential part of protecting your organization from threats.

Chapter 12 Organizing the System Tree
Chapter 13 Working with the agent from the McAfee ePO server
Chapter 14 Using the Software Manager to check in software
Chapter 15 Using policies to manage products and systems
Chapter 16 Using tasks to manage products and systems
Chapter 17 Managing packages and extensions manually
Chapter 18 Responding to events in your network
Organizing the System Tree

The System Tree is a graphical representation of how your managed network is organized. ePolicy Orchestrator software allows you to automate and customize systems organization. The organizational structure you put in place affects how security policies are inherited and enforced throughout your environment.

You can organize your System Tree using any of these methods:

- Automatic synchronization with your Active Directory or NT domain server.
- Criteria-based sorting, using criteria applied to systems manually or automatically.
- Manual organization from within the console (drag-and-drop).

Contents

- The System Tree structure
- Considerations when planning your System Tree
- Tags and how they work
- Active Directory and NT domain synchronization
- Criteria-based sorting
- How a system is added to the System Tree when sorted
- Working with tags
- Creating and populating groups
- Moving systems manually within the System Tree
- Transferring systems between McAfee ePO servers

The System Tree structure

The System Tree is a hierarchical structure that allows you to organize systems in your network into groups and subgroups.

The default System Tree structure includes two groups:

- My Organization — The root of your System Tree.
- Lost&Found — The catch-all for any systems that have not, or could not be added to other groups in your System Tree.
**The My Organization group**

The My Organization group, the root of your System Tree, contains all systems added to or detected on your network (manually or automatically). Until you create your own structure, all systems are added to the Lost&Found group.

The My Organization group has these characteristics:

- It can't be deleted.
- It can't be renamed.

**The Lost&Found group**

The Lost&Found group is a subgroup of the My Organization group. Depending on the methods you specify creating and maintaining the System Tree, the server uses different characteristics to determine where to place systems. The Lost&Found group stores systems whose locations could not be determined.

The Lost&Found group has these characteristics:

- It can't be deleted.
- It can't be renamed.
- Its sorting criteria can't be changed from being a catch-all group (although you can provide sorting criteria for the subgroups you create within it.)
- It always appears last in the list and is not alphabetized among its peers.
- Users must be granted permissions to the Lost&Found group to see the contents of Lost&Found.
- When a system is sorted into Lost&Found, it is placed in a subgroup named for the system’s domain. If no such group exists, one is created.

If you delete systems from the System Tree, be sure you select the option to remove their agents. If the agent is not removed, deleted systems reappear in the Lost&Found group because the agent continues to communicate to the server.

**System Tree groups**

System Tree groups represent a collection of systems. Deciding which systems to group together depends on the unique needs of your network and business. You can group systems based on machine-type (e.g. laptops, servers, desktops), geography (e.g. North America, Europe), political boundaries (e.g. Finance, Development), or any other criteria that supports your needs.

Groups have these characteristics:

- They are created by global administrators or users with the appropriate permissions.
- They can include both systems and other groups (subgroups).
- They are administered by a global administrator or a user with appropriate permissions.

Grouping systems with similar properties or requirements into these units allows you to manage policies for systems in one place, rather than setting policies for each system individually.

As part of the planning process, consider the best way to organize systems into groups prior to building the System Tree.
Inheritance

Inheritance is an important property that simplifies policy and task administration. Because of inheritance, child groups in the System Tree hierarchy inherit policies set at their parent groups. For example:

• Policies set at the My Organization level of the System Tree are inherited by groups below it.
• Group policies are inherited by subgroups or individual systems within that group.

Inheritance is enabled by default for all groups and individual systems that you add to the System Tree. This allows you to set policies and schedule client tasks in fewer places.

To allow for customization, however, inheritance can be broken by applying a new policy at any location of the System Tree (provided a user has appropriate permissions). You can lock policy assignments to preserve inheritance.

Considerations when planning your System Tree

An efficient and well-organized System Tree can simplify maintenance. Many administrative, network, and political realities of each environment can affect how your System Tree is structured. Plan the organization of the System Tree before you build and populate it. Especially for a large network, you want to build the System Tree only once.

Because every network is different and requires different policies — and possibly different management — McAfee recommends planning your System Tree before implementing the McAfee ePO software.

Regardless of the methods you choose to create and populate the System Tree, consider your environment while planning the System Tree.

Administrator access

When planning your System Tree organization, consider the access requirements of those who must manage the systems.

For example, you might have very decentralized network administration in your organization, where different administrators have responsibilities over different parts of the network. For security reasons, you might not have a global administrator account that can access every part of your network. In this scenario, you might not be able to set policies and deploy agents using a single global administrator account. Instead, you might need to organize the System Tree into groups based on these divisions and create accounts and permission sets.

Consider these questions:

• Who is responsible for managing which systems?
• Who requires access to view information about the systems?
• Who should not have access to the systems and the information about them?

These questions impact both the System Tree organization, and the permission sets you create and apply to user accounts.
Environmental borders and their impact on system organization

How you organize the systems for management depends on the borders that exist in your network. These borders influence the organization of the System Tree differently than the organization of your network topology.

McAfee recommends evaluating these borders in your network and organization, and whether they must be considered when defining the organization of your System Tree.

Topological borders

Your network is already defined by NT domains or Active Directory containers. The better organized your network environment, the easier it is to create and maintain the System Tree with the synchronization features.

Geographic borders

Managing security is a constant balance between protection and performance. Organize your System Tree to make the best use of limited network bandwidth. Consider how the server connects to all parts of your network, especially remote locations that are often connected by slower WAN or VPN connections, instead of faster LAN connections. You may want to configure updating and agent-server communication policies differently for remote sites to minimize network traffic over slower connections.

Grouping systems first by geography provides several advantages for configuring policies:

- You can configure update policies for the group so that all systems update from one or more distributed software repositories located nearby.
- You can schedule client tasks to run at times better suited to the site's location.

Political borders

Many large networks are divided by individuals or groups responsible for managing different portions of the network. Sometimes these borders do not coincide with topological or geographic borders. Who accesses and manages the segments of the System Tree affects how you structure it.

Functional borders

Some networks are divided by the roles of those using the network; for example, Sales and Engineering. Even if the network is not divided by functional borders, you may need to organize segments of the System Tree by functionality if different groups require different policies.

A business group may run specific software that requires special security policies. For example, arranging your email Exchange Servers into a group and setting specific exclusions for VirusScan Enterprise on-access scanning.

Subnets and IP address ranges

In many cases, organizational units of a network use specific subnets or IP ranges, so you can create a group for a geographic location and set IP filters for it. Also, if your network isn’t spread out geographically, you can use network location, such as IP address, as the primary grouping criterion.

If possible, consider using sorting criteria based on IP address information to automate System Tree creation and maintenance. Set IP subnet masks or IP address range criteria for applicable groups within the System Tree. These filters automatically populate locations with the appropriate systems.

Tags and systems with similar characteristics

You can use tags for automated sorting into groups. Tags identify systems with similar characteristics. If you can organize your groups by characteristics, you can create and assign tags based on that
criteria, then use these tags as group sorting criteria to ensure systems are automatically placed within the appropriate groups.

If possible, consider using tag-based sorting criteria to automatically populate groups with the appropriate systems.

**Operating systems and software**

Consider grouping systems with similar operating systems to manage operating system-specific products and policies more easily. If you have legacy systems, you can create a group for them and deploy and manage security products on these systems separately. Additionally, by giving these systems a corresponding tag, you can automatically sort them into a group.

---

**Tags and how they work**

Tags are like labels that you can apply to one or more systems, automatically (based on criteria) or manually. Once tags are applied, you can use them to organize systems in the System Tree or run queries that result in an actionable list of systems. Therefore, with tags as organizational criteria, you can apply policies, assign tasks, and take a number of actions on systems with the same tags.

**Traits of tags**

With tags, you can:

- Apply one or more tags to one or more systems.
- Apply tags manually.
- Apply tags automatically, based on user-defined criteria, when the agent communicates with the server.
- Exclude systems from tag application.
- Run queries to group systems with certain tags, then take direct action on the resulting list of systems.
- Base System Tree sorting criteria on tags to group systems into desired System Tree groups automatically.

**Who can use tags**

Users with appropriate permissions can:

- Create and edit tags and tag criteria.
- Apply and remove existing tags to systems in the groups where they have access.
- Exclude systems from receiving specific tags.
- Use queries to view and take actions on systems with certain tags.
- Use scheduled queries with chained tag actions to maintain tags on specific systems within the parts of the System Tree where they have access.
- Configure sorting criteria based on tags to ensure that systems stay in the appropriate groups of the System Tree.
Types of tags

ePolicy Orchestrator uses two types of tags:

- **Tags without criteria.** These tags can be applied only to selected systems in the System Tree (manually) and systems listed in the results of a query.

- **Criteria-based tags.** These tags are applied to all non-excluded systems at each agent-server communication. Such tags use criteria based on any properties sent by the agent. They can also be applied to non-excluded systems on demand.

---

Active Directory and NT domain synchronization

ePolicy Orchestrator can integrate with Active Directory and NT domains as a source for systems, and even (in the case of Active Directory) as a source for the structure of the System Tree.

Active Directory synchronization

If your network runs Active Directory, you can use Active Directory synchronization to create, populate, and maintain part or all of the System Tree with Active Directory synchronization settings. Once defined, the System Tree is updated with any new systems (and subcontainers) in your Active Directory.

Active Directory integration allows you to:

- Synchronize with your Active Directory structure, by importing systems and the Active Directory subcontainers (as System Tree groups) and keeping them up-to-date with Active Directory. At each synchronization, both systems and the structure are updated in the System Tree to reflect the systems and structure of Active Directory.

- Import systems as a flat list from the Active Directory container (and its subcontainers) into the synchronized group.

- Control what to do with potential duplicate systems.

- Use the system description, which is imported from Active Directory with the systems.

In previous versions of ePolicy Orchestrator, there were the two tasks: Active Directory Import and Active Directory Discovery. Now, use this process to integrate the System Tree with your Active Directory systems structure:

1. Configure the synchronization settings on each group that is a mapping point in the System Tree. At the same location, you can configure whether to:
   - Deploy agents to discovered systems.
   - Delete systems from the System Tree when they are deleted from Active Directory.
   - Allow or disallow duplicate entries of systems that already exist elsewhere in the System Tree.

2. Use the Synchronize Now action to import Active Directory systems (and possibly structure) into the System Tree according to the synchronization settings.

3. Use an NT Domain/Active Directory Synchronization server task to regularly synchronize the systems (and possibly the Active Directory structure) with the System Tree according to the synchronization settings.
Types of Active Directory synchronization

There are two types of Active Directory synchronization (systems only and systems and structure). Which one you use depends on the level of integration you want with Active Directory.

With each type, you control the synchronization by selecting whether to:

- Deploy agents automatically to systems new to ePolicy Orchestrator. You may not want to set this on the initial synchronization if you are importing a large number of systems and have limited bandwidth. The agent MSI is about 6 MB in size. However, you might want to deploy agents automatically to any new systems that are discovered in Active Directory during subsequent synchronization.

- Delete systems from ePolicy Orchestrator (and remove their agents) when they are deleted from Active Directory.

- Prevent adding systems to the group if they exist elsewhere in the System Tree. This ensures that you don't have duplicate systems if you manually move or sort the system to another location.

- Exclude certain Active Directory containers from the synchronization. These containers and their systems are ignored during synchronization.

Systems and structure

When using this synchronization type, changes in the Active Directory structure are carried over into your System Tree structure at the next synchronization. When systems or containers are added, moved, or removed in Active Directory, they are added, moved, or removed in the corresponding locations of the System Tree.

When to use this synchronization type

Use this to ensure that the System Tree (or parts of it) look exactly like your Active Directory structure.

If the organization of Active Directory meets your security management needs and you want the System Tree to continue to look like the mapped Active Directory structure, use this synchronization type with subsequent synchronization.

Systems only

Use this synchronization type to import systems from an Active Directory container, including those in non-excluded subcontainers, as a flat list to a mapped System Tree group. You can then move these to appropriate locations in the System Tree by assigning sorting criteria to groups.

If you choose this synchronization type, be sure to select not to add systems again if they exist elsewhere in the System Tree. This prevents duplicate entries for systems in the System Tree.

When to use this synchronization type

Use this synchronization type when you use Active Directory as a regular source of systems for ePolicy Orchestrator, but the organizational needs for security management do not coincide with the organization of containers and systems in Active Directory.

NT domain synchronization

Use your NT domains as a source for populating your System Tree. When you synchronize a group to an NT domain, all systems from the domain are put in the group as a flat list. You can manage these systems in the single group, or you can create subgroups for more granular organizational needs. Use a method, like automatic sorting, to populate these subgroups automatically.

If you move systems to other groups or subgroups of the System Tree, be sure to select to not add the systems when they already exist elsewhere in the System Tree. This prevents duplicate entries for systems in the System Tree.
Unlike Active Directory synchronization, only the system names are synchronized with NT domain synchronization; the system description is not synchronized.

Criteria-based sorting

As in past releases of ePolicy Orchestrator, you can use IP address information to automatically sort managed systems into specific groups. You can also create sorting criteria based on tags, which are like labels assigned to systems. You can use either type of criteria or both to ensure systems are where you want them in the System Tree.

Systems only need to match one criterion of a group’s sorting criteria to be placed in the group.

After creating groups and setting your sorting criteria, perform a Test Sort action to confirm that the criteria and sorting order achieve the desired results.

Once you have added sorting criteria to your groups, you can run the Sort Now action. The action moves selected systems to the appropriate group automatically. Systems that do not match the sorting criteria of any group are moved to Lost&Found.

New systems that call in to the server for the first time are added automatically to the correct group. However, if you define sorting criteria after the initial agent-server communication, you must run the Sort Now action on those systems to move them immediately to the appropriate group, or wait until the next agent-server communication.
Sorting status of systems

On any system or collection of systems, you can enable or disable System Tree sorting. If you disable System Tree sorting on a system, it is excluded from sorting actions, except when the Test Sort action is performed. When a test sort is performed, the sorting status of the system or collection is considered and can be moved or sorted from the Test Sort page.

System Tree sorting settings on the McAfee ePO server

For sorting to take place, sorting must be enabled on the server and on the systems. By default, sorting systems once enabled. As a result, systems are sorted at the first agent-server communication (or next, if applying changes to existing systems) and are not sorted again.

Test sorting systems

Use this feature to view where systems would be placed during a sort action. The Test Sort page displays the systems and the paths to the location where they would be sorted. Although this page does not display the sorting status of systems, if you select systems on the page (even ones with sorting disabled), clicking Move Systems places those systems in the location identified.

How settings affect sorting

You can choose three server settings that determine whether and when systems are sorted. Also, you can choose whether any system can be sorted by enabling or disabling System Tree sorting on selected systems in the System Tree.

Server settings

The server has three settings:

- **Disable System Tree sorting** — If criteria-based sorting does not meet your security management needs and you want to use other System Tree features (like Active Directory synchronization) to organize your systems, select this setting to prevent other McAfee ePO users from mistakenly configuring sorting criteria on groups and moving systems to undesirable locations.

- **Sort systems on each agent-server communication** — Systems are sorted again at each agent-server communication. When you change sorting criteria on groups, systems move to the new group at their next agent-server communication.

- **Sort systems once** — Systems are sorted at the next agent-server communication and marked to never be sorted again at agent-server communication, as long as this setting is selected. You can still sort such a system, however, by selecting it and clicking Sort Now.

System settings

You can disable or enable System Tree sorting on any system. If disabled on a system, that system will not be sorted, regardless of how the sorting action is taken. However, performing the Test Sort action will sort this system. If enabled on a system, that system is sorted always for the manual Sort Now action, and can be sorted at agent-server communication, depending on the server settings for System Tree sorting.

IP address sorting criteria

In many networks, subnets and IP address information reflect organizational distinctions, such as geographical location or job function. If IP address organization coincides with your needs, consider
using this information to create and maintain parts or all of your System Tree structure by setting IP address sorting criteria for such groups.

In this version of ePolicy Orchestrator, this functionality has changed, and now allows for the setting of IP sorting criteria randomly throughout the tree. You no longer need to ensure that the sorting criteria of the child group’s IP address is a subset of the parent’s, as long as the parent has no assigned criteria. Once configured, you can sort systems at agent-server communication, or only when a sort action is manually initiated.

IP address sorting criteria should not overlap between different groups. Each IP range or subnet mask in a group’s sorting criteria should cover a unique set of IP addresses. If criteria does overlap, the group where those systems end up depends on the order of the subgroups on the System Tree | Groups Details tab. You can check for IP overlap using the Check IP Integrity action in the Group Details tab.

### Tag-based sorting criteria

In addition to using IP address information to sort systems into the appropriate group, you can define sorting criteria based on the tags assigned to systems. Tag-based criteria can be used with IP address-based criteria for sorting.

### Group order and sorting

To provide additional flexibility with System Tree management, you can configure the order of a group’s subgroups, and therefore the order by which they are considered for a system’s placement during sorting. When multiple subgroups have matching criteria, changing this order can change where a system ends up in the System Tree.

Additionally, if you are using catch-all groups, they must be the last subgroup in the list.

### Catch-all groups

Catch-all groups are groups whose sorting criteria is set to All others on the Sorting Criteria page of the group. Only subgroups at the last position of the sort order can be catch-all groups. These groups receive all systems that were sorted into the parent group, but were not sorted into any of the catch-all’s peers.

### How a system is added to the System Tree when sorted

When the agent communicates with the server for the first time, the server uses an algorithm to place the system in the System Tree. When it cannot find an appropriate location for a system, it puts the system in the Lost&Found group.

On each agent-server communication, the server attempts to locate the system in the System Tree by agent GUID (only systems whose agents have already called into the server for the first time have an agent GUID in the database). If a matching system is found, it is left in it’s existing location.

If a matching system is not found, the server uses an algorithm to sort the systems into the appropriate groups. Systems can be sorted into any criteria-based group in the System Tree, no matter how deep it is in the structure, as long as each parent group in the path does not have non-matching criteria. Parent groups of a criteria-based subgroup must have either no criteria or matching criteria.
The sorting order assigned to each subgroup (defined in the Group Details tab) determines the order that subgroups are considered by the server when it searches for a group with matching criteria.

1. The server searches for a system without an agent GUID (its agent has never called in before) with a matching name in a group with the same name as the domain. If found, the system is placed in that group. This can happen after the first Active Directory or NT domain synchronization, or when you have manually added systems to the System Tree.

2. If a matching system is still not found, the server searches for a group of the same name as the domain where the system originates. If such a group is not found, one is created under the Lost&Found group, and the system is placed there.

3. Properties are updated for the system.

4. The server applies all criteria-based tags to the system if the server is configured to run sorting criteria at each agent-server communication.

5. What happens next depends on whether System Tree sorting is enabled on both the server and the system.
   - If System Tree sorting is disabled on either the server or the system, the system is left where it is.
   - If System Tree sorting is enabled on the server and system, the system is moved based on the sorting criteria in the System Tree groups.

6. The server considers the sorting criteria of all top-level groups according to the sorting order on the My Organization group’s Group Details tab. The system is placed in the first group with matching criteria or a catch-all group it considers.
   - Once sorted into a group, each of its subgroups are considered for matching criteria according to their sorting order on the Group Details tab.
   - This continues until there is no subgroup with matching criteria for the system, and is placed in the last group found with matching criteria.

7. If such a top-level group is not found, the subgroups of top-level groups (without sorting criteria) are considered according to their sorting.

8. If such a second-level criteria-based group is not found, the criteria-based third-level groups of the second-level unrestricted groups are considered.

9. This process continues down through the System Tree until a system is sorted into a group.

10. If the server cannot sort the system into any group, it is placed in the Lost&Found group within a subgroup that is named after its domain.
Working with tags

Use these tasks to create and apply tags to systems.

Tasks

- Creating tags with the Tag Builder on page 132
  Use this task to create a tag with the New Tag Builder wizard. Tags can use criteria that's evaluated against every system:

- Excluding systems from automatic tagging on page 133
  Use this task to exclude systems from having specific tags applied. Alternatively, you can use a query to collect systems, then exclude the desired tags from those systems from the query results.

- Applying tags to selected systems on page 133
  Use this task to apply a tag manually to selected systems in the System Tree.

- Applying criteria-based tags automatically to all matching systems on page 133
  Use these tasks to apply criteria-based tags automatically to all systems that match its criteria.

Creating tags with the Tag Builder

Use this task to create a tag with the New Tag Builder wizard. Tags can use criteria that's evaluated against every system:

- Automatically at agent-server communication.

- When the Run Tag Criteria action is taken.

- Manually on selected systems, regardless of criteria, with the Apply Tag action.

Tags without criteria can only be applied manually to selected systems.

Task

For option definitions, click ? in the interface.

1. Click Menu | Systems | Tag Catalog, then click Tag Actions | New Tag. The Tag Builder wizard opens.

2. On the Description page, type a name and meaningful description, then click Next. The Criteria page appears.

3. Select and configure the desired criteria, then click Next. The Evaluation page appears.

   To apply the tag automatically, you must configure criteria for the tag.

4. Select whether systems are evaluated against the tag's criteria only when the Run Tag Criteria action is taken, or also at each agent-server communication, then click Next. The Preview page appears.

   These options are unavailable if criteria was not configured. When systems are evaluated against a tag's criteria, the tag is applied to systems that match the criteria and have not been excluded from the tag.

5. Verify the information on this page, then click Save.

   If the tag has criteria, this page displays the number of systems that will receive this tag when evaluated against its criteria.

The tag is added to the list of tags on the Tag Catalog page.
Excluding systems from automatic tagging
Use this task to exclude systems from having specific tags applied. Alternatively, you can use a query
to collect systems, then exclude the desired tags from those systems from the query results.

Task
For option definitions, click ? in the interface.

1. Click Menu | Systems | System Tree | Systems, then select the group that contains the systems in the System Tree.
2. Select one or more systems in the Systems table, then click Actions | Tag | Exclude Tag.
3. In the Exclude Tag dialog box, select the desired tag to exclude from the selected systems from the drop-down list, then click OK.
4. Verify the systems have been excluded from the tag:
   a. Click Menu | Systems | Tag Catalog, then select the desired tag in the list of tags.
   b. Next to Systems with tag in the details pane, click the link for the number of systems excluded from criteria-based tag application. The Systems Excluded from the Tag page appears.
   c. Verify the desired systems are in the list.

Applying tags to selected systems
Use this task to apply a tag manually to selected systems in the System Tree.

Task
For option definitions, click ? in the interface.

1. Click Menu | Systems | System Tree | Systems, then select the group that contains the desired system.
2. Select the desired systems, then click Actions | Tag | Apply Tag.
3. In the Apply Tag dialogue box, select the desired tag from the drop-down list to apply to the selected systems, then click OK.
4. Verify the tags have been applied:
   a. Click Menu | Systems | Tag Catalog select, then select the desired tag in the list of tags.
   b. Next to Systems with tag in the details pane, click the link for the number of systems tagged manually. The Systems with Tag Applied Manually page appears.
   c. Verify the desired systems are in the list.

Applying criteria-based tags automatically to all matching systems
Use these tasks to apply criteria-based tags automatically to all systems that match its criteria.
Tasks

- **Applying criteria-based tags to all matching systems on page 134**
  Use this task to apply a criteria-based tag to all systems that match the criteria, except for those that have been excluded from the tag.

- **Applying criteria-based tags on a schedule on page 134**
  Use this task to schedule a regular task that applies a tag to all systems that match its criteria.

Applying criteria-based tags to all matching systems

Use this task to apply a criteria-based tag to all systems that match the criteria, except for those that have been excluded from the tag.

**Task**

For option definitions, click ? in the interface.

1. Click Menu | Systems | Tag Catalog, then select the desired tag from the Tags list.
2. Click Actions | Run Tag Criteria.
3. On the Action panel, select whether to reset manually tagged and excluded systems.
   - This removes the tag from systems that don’t match the criteria and applies the tag to systems which match criteria but were excluded from receiving the tag.
4. Click OK.
5. Verify the systems have the tag applied:
   a. Click Menu | Systems | Tag Catalog, then select the desired tag in the list of tags.
   b. Next to Systems with tag in the details pane, click the link for the number of systems with tag applied by criteria. The Systems with Tag Applied by Criteria page appears.
   c. Verify the desired systems are in the list.

The tag is applied to all systems that match its criteria.

Applying criteria-based tags on a schedule

Use this task to schedule a regular task that applies a tag to all systems that match its criteria.

For option definitions, click ? in the interface.

**Task**

1. Click Menu | Automation | Server Tasks, then click Actions | New Task. The Server Task Builder page appears.
2. On the Description page, name and describe the task and select whether the task is enabled once it is created, then click Next. The Actions page appears.
3 Select **Run Tag Criteria** from the drop-down list, then select the desired tag from the Tag drop-down list.

![Figure 12-1 Run Tag Criteria server task action](image)

4 Select whether to reset manually tagged and excluded systems.

   - **This removes the tag on systems that don’t match the criteria and applies the tag to systems that match criteria but were excluded from receiving the tag.**

5 Click **Next**. The Schedule page appears.

6 Schedule the task as desired, then click **Next**. The Summary page appears.

7 Review the task settings, then click **Save**.

   The server task is added to the list on the Server Tasks page. If you selected to enable the task in the Server Task Builder wizard, it runs at the next scheduled time.

---

### Creating and populating groups

Use these tasks to create and populate groups. You can populate groups with systems, either by typing NetBIOS names for individual systems or by importing systems directly from your network. You can also populate groups using drag-and-drop by dragging the selected systems and dragging them into any group in the System Tree. Drag-and-drop also allows you to move groups and subgroups within the System Tree.

There is no single way to organize a System Tree, and because every network is different, your System Tree organization can be as unique as your network layout. Although you won’t use each method offered, you can use more than one.

For example, if you use Active Directory in your network, consider importing your Active Directory containers rather than your NT domains. If your Active Directory or NT domain organization does not make sense for security management, you can create your System Tree in a text file and import it into your System Tree. If you have a smaller network, you can create your System Tree by hand and add each system manually.
Tasks

• **Creating groups manually on page 136**
  Use this task to create groups manually. You can populate these groups with systems by typing NetBIOS names for individual systems or by importing systems directly from your network.

• **Adding systems manually to an existing group on page 137**
  Use this task to import systems from your Network Neighborhood to groups. You can also import a network domain or Active Directory container.

• **Exporting systems from the System Tree on page 138**
  You can export a list of systems from the System Tree to a .txt file for later use. Export at the group or subgroup level while retaining the System Tree organization.

• **Importing systems from a text file on page 138**
  Use these tasks to create a text file of systems and groups to import into the System Tree.

• **Sorting systems into criteria-based groups on page 140**
  Use these tasks to configure and implement sorting to group systems. For systems to sort into groups, sorting must be enabled on the server and the desired systems, and sorting criteria and the sorting order of groups must be configured.

• **Importing Active Directory containers on page 142**
  Use this task to import systems from your network’s Active Directory containers directly into your System Tree by mapping Active Directory source containers to the groups of the System Tree. Unlike previous versions, you can now:

• **Importing NT domains to an existing group on page 144**
  Use this task to import systems from an NT domain to a group you created manually.

• **Synchronizing the System Tree on a schedule on page 146**
  Use this task to schedule a server task that updates the System Tree with changes in the mapped domain or Active Directory container.

• **Updating the synchronized group with an NT domain manually on page 147**
  Use this task to update a synchronized group with its mapped NT domain, including:

### Creating groups manually

Use this task to create groups manually. You can populate these groups with systems by typing NetBIOS names for individual systems or by importing systems directly from your network.

**Task**

For option definitions, click ? in the interface.

1. Select the desired group in the System Tree under which to create a subgroup. Then:
   - From the Group Details page (Menu | Systems | System Tree | Group Details) click Actions | New Subgroup.
   - From the System Tree page (Menu | Systems | System Tree) click System Tree Actions | New Subgroup.

2. The New Subgroup dialog box appears.

   ![You can create more than one subgroup at a time.](image)
3 Type the desired name then click **OK**. The new group appears in the System Tree.

4 Repeat as necessary until you are ready to populate the groups with the desired systems. Add systems to the System Tree and ensure they get to the desired groups by:
   - Typing system names manually.
   - Importing them from NT domains or Active Directory containers. You can regularly synchronize a domain or a container to a group for ease of maintenance.
   - Setting up IP address-based or tag-based sorting criteria on the groups. When agents check in from systems with matching IP address information or matching tags, they are automatically placed in the appropriate group.

### Adding systems manually to an existing group

Use this task to import systems from your Network Neighborhood to groups. You can also import a network domain or Active Directory container.

**Task**

For option definitions, click ? in the interface.

1 Click **Menu | Systems | System Tree**, then in the **System Tree Actions** menu click **New Systems**. The New Systems page appears.

![New Systems page](image)

**Figure 12-2 New Systems page**

2 Select whether to deploy the agent to the new systems, and whether the systems are added to the selected group or to a group according to sorting criteria.

3 Next to **Target systems**, type the NetBIOS name for each system in the text box, separated by commas, spaces, or line breaks. Alternatively, click **Browse** to select the systems.
If you selected **Push agents and add systems to the current group**, you can enable automatic System Tree sorting. Do this to apply the sorting criteria to these systems. Specify the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent version</td>
<td>Select the agent version to deploy.</td>
</tr>
<tr>
<td>Installation path</td>
<td>Configure the agent installation path or accept the default.</td>
</tr>
<tr>
<td>Credentials for agent installation</td>
<td>Type valid credentials to install the agent.</td>
</tr>
<tr>
<td>Number of attempts</td>
<td>Type an integer, using zero for continuous attempts.</td>
</tr>
<tr>
<td>Retry interval</td>
<td>Type the number seconds between retries.</td>
</tr>
<tr>
<td>Abort After</td>
<td>Type the number of minutes before aborting the connection.</td>
</tr>
<tr>
<td>Push Agent using</td>
<td>Select either a specific Agent Handler or all Agent Handlers.</td>
</tr>
</tbody>
</table>

5 Click **OK**.

**Exporting systems from the System Tree**

You can export a list of systems from the System Tree to a .txt file for later use. Export at the group or subgroup level while retaining the System Tree organization.

It can be useful to have a list of the systems in your System Tree. You can import this list into your McAfee ePO Server to quickly restore your previous structure and organization.

![This task does not remove systems from you System Tree. It creates a .txt file that contains the names and structure of systems in your System Tree.](image)

**Task**

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

1 Click **Menu | Systems | System Tree.** The **System Tree** page opens.

2 Select the group or subgroup containing the systems you want to export, then click **System Tree Actions | Export Systems.** The **Export Systems** page opens.

3 Select whether to export:
   - **All systems in this group** — Exports the systems in the specified **Source group**, but does not export systems listed in nested subgroups under this level.
   - **All systems in this group and subgroups** — Exports all systems at and below this level.

4 Click **OK**.

The **Export** page opens. You can click the **systems** link to view the system list, or right-click the link to save a copy of the **ExportSystems.txt** file.

**Importing systems from a text file**

Use these tasks to create a text file of systems and groups to import into the System Tree.
Tasks

- Creating a text file of groups and systems on page 139
  Use this task to create a text file of the NetBIOS names for your network systems that you want to import into a group. You can import a flat list of systems, or organize the systems into groups, then add the specified systems to them. You can create the text file by hand. In large networks, use other network administration tools to generate a text file list of systems on your network.

- Importing systems and groups from a text file on page 139
  Use this task to import systems or groups of systems into the System Tree from a text file you have created and saved.

Creating a text file of groups and systems

Use this task to create a text file of the NetBIOS names for your network systems that you want to import into a group. You can import a flat list of systems, or organize the systems into groups, then add the specified systems to them. You can create the text file by hand. In large networks, use other network administration tools to generate a text file list of systems on your network.

Define the groups and their systems by typing the group and system names in a text file. Then import that information into ePolicy Orchestrator. You must have network utilities, such as the NETDOM.EXE utility available with the Microsoft Windows Resource Kit, to generate complete text files containing complete lists of the systems on your network. Once you have the text file, edit it manually to create groups of systems, and import the entire structure into the System Tree.

Regardless of how you generate the text file, you must use the correct syntax before importing it.

For option definitions, click ? in the interface.

Task

1. List each system separately on its own line. To organize systems into groups, type the group name followed by a backslash (\), then list the systems belonging to that group beneath it, each on a separate line.
   
   GroupA\system1
   GroupA\system2
   GroupA\GroupB\system3
   GroupC\GroupD

2. Verify the names of groups and systems, and the syntax of the text file, then save the text file to a temporary folder on your server.

Importing systems and groups from a text file

Use this task to import systems or groups of systems into the System Tree from a text file you have created and saved.

For option definitions, click ? in the interface.

Task

1. Click Menu | Systems | System Tree, then click System Tree Actions and select New Systems. The New Systems page appears.

2. Select Import systems from a text file into the selected group, but do not push agents.
3 Select whether the import file contains:
   • Systems and System Tree Structure
   • Systems only (as a flat list)
4 Click Browse, then select the text file.
5 Select what to do with systems that already exist elsewhere in the System tree.
6 Click OK.

The systems are imported to the selected group in the System Tree. If your text file organized the systems into groups, the server creates the groups and imports the systems.

**Sorting systems into criteria-based groups**

Use these tasks to configure and implement sorting to group systems. For systems to sort into groups, sorting must be enabled on the server and the desired systems, and sorting criteria and the sorting order of groups must be configured.

**Tasks**

- *Adding sorting criteria to groups on page 140*
  Use this task to configure sorting criteria for a group. Sorting criteria can be based on IP address information or tags.

- *Enabling System Tree sorting on the server on page 39*
  Use this task to enable System Tree sorting on the server. System Tree sorting must be enabled on the server and the desired systems for systems to be sorted.

- *Enabling and disabling System Tree Sorting on Systems on page 141*
  The sorting status of a system determines whether it can be sorted into a criteria-based group.

- *Sorting systems manually on page 141*
  Use this task to sort selected systems into groups with criteria-based sorting enabled.

**Adding sorting criteria to groups**

Use this task to configure sorting criteria for a group. Sorting criteria can be based on IP address information or tags.

**Task**

For option definitions, click ? in the interface.

1 Click Menu | Systems | System Tree | Group Details and select the group in the System Tree.
2 Next to Sorting criteria click Edit. The Sorting Criteria page for the selected group appears.
3 Select Systems that match any of the criteria below, then the criteria selections appear.

> Although you can configure multiple sorting criteria for the group, a system only has to match a single criterion to be placed in this group.
4 Configure the criterion. Options include:
   - **IP addresses** — Use this text box to define an IP address range or subnet mask as sorting criteria. Any system whose address falls within it is sorted into this group.
   - **Tags** — Add specific tags to ensure systems with such tags that come into the parent group are sorted into this group.

5 Repeat as necessary until sorting criteria reconfigured for the group, then click **Save**.

**Enabling System Tree sorting on the server**
Use this task to enable System Tree sorting on the server. System Tree sorting must be enabled on the server and the desired systems for systems to be sorted.

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

1 Click **Menu** | **Configuration** | **Server Settings**, then select **System Tree Sorting** in the Setting Categories list and click **Edit**.

2 Select whether to sort systems only on the first agent-server communication or on each agent-server communication.

   If you selected to sort only on the first agent-server communication, all enabled systems are sorted on their next agent-server communication and are never sorted again for as long as this option is selected. However, these systems can be sorted again manually by taking the Sort Now action, or by changing this setting to sort on each agent-server communication.

   If you selected to sort on each agent-server communication, all enabled systems are sorted at each agent-server communication as long as this option is selected.

**Enabling and disabling System Tree Sorting on Systems**
The sorting status of a system determines whether it can be sorted into a criteria-based group.

You can change the sorting status on systems in any table of systems (such as query results), and also automatically on the results of a scheduled query.

For option definitions, click ? in the interface.

**Task**

1 Click **Menu** | **Systems** | **System Tree** | **Systems**, then select the desired systems.

2 Click **Actions** | **Directory Management** | **Change Sorting Status**, then select whether to enable or disable System Tree sorting on selected systems.

3 In the Change Sorting Status dialog box select whether to disable or enable system tree sorting on the selected system.

   Depending on the server setting for System Tree sorting, these systems are sorted on the next agent-server communication. Otherwise, they can only be sorted with the Sort Now action.

**Sorting systems manually**
Use this task to sort selected systems into groups with criteria-based sorting enabled.
**Task**
For option definitions, click ? in the interface.

1. Click **Menu** | **Systems** | **System Tree** | **Systems** and select the group that contains the desired systems.

2. Select the systems then click **Actions** | **Directory Management** | **Sort Now**. The Sort Now dialog box appears.

   If you want to preview the results of the sort before sorting, click **Test Sort** instead. (However, if you move systems from within the Test Sort page, all selected systems are sorted, even if they have System Tree sorting disabled.)

3. Click **OK** to sort the systems.

**Importing Active Directory containers**
Use this task to import systems from your network’s Active Directory containers directly into your System Tree by mapping Active Directory source containers to the groups of the System Tree. Unlike previous versions, you can now:

- Synchronize the System Tree structure to the Active Directory structure so that when containers are added or removed in Active Directory, the corresponding group in the System Tree is added or removed also.
- Delete systems from the System Tree when they are deleted from Active Directory.
- Prevent duplicate entries of systems in the System Tree when they already exist in other groups.

For option definitions, click ? in the interface.

**Task**

1. Click **Menu** | **Systems** | **System Tree** | **Group Details**, then select the desired group in the System Tree. This should be the group to which you want to map an Active Directory container.

   You cannot synchronize the Lost&Found group of the System Tree.

2. Next to **Synchronization type**, click **Edit**. The Synchronization Settings page for the selected group appears.
3 Next to Synchronization type, select Active Directory. The Active Directory synchronization options appear.

4 Select the type of Active Directory synchronization you want to occur between this group and the desired Active Directory container (and its subcontainers):
   - **Systems and container structure** — Select this option if you want this group to truly reflect the Active Directory structure. When synchronized, the System Tree structure under this group is modified to reflect that of the Active Directory container it's mapped to. When containers are added or removed in Active Directory, they are added or removed in the System Tree. When systems are added, moved, or removed from Active Directory, they are added, moved, or removed from the System Tree.
   - **Systems only** — Select this option if you only want the systems from the Active Directory container (and non-excluded subcontainers) to populate this group, and this group only. No subgroups are created when mirroring Active Directory.

5 Select whether a duplicate entry for the system will be created for a system that already exists in another group of the System Tree.

   McAfee does not recommend selecting this option, especially if you are only using the Active Directory synchronization as a starting point for security management and use other System Tree management functionality (for example, tag sorting) for further organizational granularity below the mapping point.

6 In Active Directory domain you can:
   - Type the fully-qualified domain name of your Active Directory domain.
   - Select from a list of already registered LDAP servers.

7 Next to Container, click Add and select a source container in the Select Active Directory Container dialog box, then click OK.

8 To exclude specific subcontainers, click Add next to Exceptions and select a subcontainer to exclude, then click OK.

9 Select whether to deploy agents automatically to new systems. If you do, be sure to configure the deployment settings.

   McAfee recommends that you do not deploy the agent during the initial import if the container is large. Deploying the 3.62 MB agent package to many systems at once may cause network traffic issues. Instead, import the container, then deploy the agent to groups of systems at a time, rather than all at once. Consider revisiting this page and selecting this option after the initial agent deployment, so that the agent is installed automatically on new systems added to Active Directory.

10 Select whether to delete systems from the System Tree when they are deleted from the Active Directory domain. Optionally choose whether to remove agents from the deleted systems.
11 To synchronize the group with Active Directory immediately, click **Synchronize Now**.
   Clicking **Synchronize Now** saves any changes to the synchronization settings before synchronizing the group. If you have an Active Directory synchronization notification rule enabled, an event is generated for each system added or removed (these events appear in the Audit Log, and are queryable). If you deployed agents to added systems, the deployment is initiated to each added system. When the synchronization completes, the **Last Synchronization** time is updated, displaying the time and date when the synchronization finished, not when any agent deployments completed.

   Alternatively, you can schedule an NT Domain/Active Directory Synchronization server task for the first synchronization. This is useful if you are deploying agents to new systems on the first synchronization, when bandwidth is a larger concern.

12 When the synchronization completes, view the results with the System Tree.
   Once the systems are imported, distribute agents to them if you did not select to do so automatically. Also, consider setting up a recurring NT Domain/Active Directory Synchronization server task to keep your System Tree up to date with any new systems or organizational changes in your Active Directory containers.

### Importing NT domains to an existing group

Use this task to import systems from an NT domain to a group you created manually.

You can populate groups automatically by synchronizing entire NT domains with specified groups. This is an easy way to add all the systems in your network to the System Tree at once as a flat list with no system description.

If the domain is very large, you can create subgroups to assist with policy management or System Tree organization. To do this, first import the domain into a group of your System Tree, then manually create logical subgroups.

To manage the same policies across several domains, import each of the domains into a subgroup under the same group, on which you can set policies that inherit into each of the subgroups.

When using this method:

- Set up IP address or tag sorting criteria on subgroups to automatically sort the imported systems.
- Schedule a recurring NT Domain/Active Directory Synchronization server task for easy maintenance.

For option definitions, click ? in the interface.
Task

1. Click Menu | Systems | System Tree | Group Details and select or create a group in the System Tree.

2. Next to Synchronization type, click Edit. The Synchronization Settings page for the selected group appears.

3. Next to Synchronization type, select NT Domain. The domain synchronization settings appear.

4. Next to Systems that exist elsewhere in the System Tree, select what to do with systems that would be added during synchronization already exist in another group of the System Tree.

   McAfee does not recommend selecting Add systems to the synchronized group and leave them in their current System Tree location, especially if you are only using the NT domain synchronization as a starting point for security management and use other System Tree management functionalities (for example, tag sorting) for further organizational granularity below the mapping point.

5. Next to Domain, click Browse and select the NT domain to map to this group, then click OK. Alternatively, you can type the name of the domain directly in the text box.

   When typing the domain name, do not use the fully-qualified domain name.

6. Select whether to deploy agents automatically to new systems. If you do so, be sure to configure the deployment settings.

   McAfee recommends that you do not deploy the agent during the initial import if the domain is large. Deploying the 3.62 MB agent package to many systems at once may cause network traffic issues. Instead, import the domain, then deploy the agent to smaller groups of systems at a time, rather than all at once. However, once you've finished deploying agents, consider revisiting this page and selecting this option after the initial agent deployment, so that the agent is installed automatically on any new systems that are added to the group (or its subgroups) by domain synchronization.

7. Select whether to delete systems from the System Tree when they are deleted from the NT domain. You can optionally choose to remove agents from deleted systems.
8 To synchronize the group with the domain immediately, click Synchronize Now, then wait while the systems in the domain are added to the group.

Clicking Synchronize Now saves changes to the synchronization settings before synchronizing the group. If you have an NT domain synchronization notification rule enabled, an event is generated for each system added or removed. (These events appear in the Audit Log, and are queryable). If you selected to deploy agents to added systems, the deployment is initiated to each added system. When the synchronization completes, the Last Synchronization time is updated. The time and date are when the synchronization finished, not when any agent deployments completed.

9 If you want to synchronize the group with the domain manually, click Compare and Update. The Manually Compare and Update page appears.

Clicking Compare and Update saves any changes to the synchronization settings.

a If you are going to remove any systems from the group with this page, select whether to remove their agents when the system is removed.

b Select the systems to add to and remove from the group as necessary, then click Update Group to add the selected systems. The Synchronize Setting page appears.

10 Click Save, then view the results in the System Tree if you clicked Synchronize Now or Update Group.

Once the systems are added to the System Tree, distribute agents to them if you did not select to deploy agents as part of the synchronization. Also, consider setting up a recurring NT Domain/Active Directory Synchronization server task to keep this group up-to-date with new systems in the NT domain.

**Synchronizing the System Tree on a schedule**

Use this task to schedule a server task that updates the System Tree with changes in the mapped domain or Active Directory container.

Depending on a group's synchronization settings, this task:

- Adds new systems on the network to the specified group.
- Adds new corresponding groups when new Active Directory containers are created.
- Deletes corresponding groups when Active Directory containers are removed.
- Deploys agents to new systems.
- Removes systems that are no longer in the domain or container.
- Applies policies and tasks of the site or group to new systems.
- Prevents or allows duplicate entries of systems that still exist in the System Tree that you've moved to other locations.

The agent cannot be deployed to all operating systems in this manner. You might need to distribute the agent manually to some systems.
**Task**
For option definitions, click ? in the interface.

1 Click Menu | Automation | Server Tasks, then click Actions | New Task. The Server Task Builder opens.

2 On the Description page, name the task and choose whether it is enabled once it is created, then click Next. The Actions page appears.

3 From the drop-down list, select Active Directory Synchronization/NT Domain.

4 Select whether to synchronize all groups or selected groups. If you are synchronizing only some synchronized groups, click Select Synchronized Groups and select specific ones.

5 Click Next. The Schedule page appears.

6 Schedule the task, then click Next. The Summary page appears.

7 Review the task details, then click Save.

In addition to the task running at the scheduled time, you can run this task immediately by clicking Run next to the task on the Server Tasks page.

---

**Updating the synchronized group with an NT domain manually**
Use this task to update a synchronized group with its mapped NT domain, including:

- Add systems currently in the domain.
- Remove systems from your System Tree that are no longer in the domain.
- Remove agents from all systems that no longer belong to the specified domain.

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

1 Click Menu | Systems | System Tree | Group Details, then select the group that is mapped to the NT domain.

2 Next to Synchronization type, click Edit. The Synchronization Settings page appears.

3 Select NT Domain, then click Compare and Update near the bottom of the page. The Manually Compare and Update page appears.

4 If you are removing systems from the group, select whether to remove the agents from systems that are removed.

5 Click Add All or Add to import systems from the network domain to the selected group.
   
   Click Remove All or Remove to delete systems from the selected group.

6 Click Update Group when finished.

---

**Moving systems manually within the System Tree**
Use this task to move systems from one group to another in the System Tree. You can move systems from any page that displays a table of systems, including the results of a query.

In addition to the steps below, you can also drag-and-drop systems from the Systems table to any group in the System Tree.
Even if you have a perfectly organized System Tree that mirrors your network hierarchy, and use automated tasks and tools to regularly synchronize your System Tree, you may need to move systems manually between groups. For example, you may need to periodically move systems from the Lost&Found group.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu | Systems | System Tree | Systems** and then browse to and select the systems.
3. Select whether to enable or disable System Tree sorting on the selected systems when they are moved.
4. Select the group in which to place the systems, then click OK.

---

**Transferring systems between McAfee ePO servers**

Use this task to transfer systems between McAfee ePO servers.

For option definitions, click ? in the interface.

**Task**

1. Click **Menu | Systems | System Tree**, then select the systems you want to transfer.
2. Click **Actions | Agent | Transfer Systems**. The Transfer Systems dialog box appears.
3. Select the desired server from the drop-down menu and click OK.

> Once a managed system has been 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.
Working with the agent from the McAfee ePO server

The McAfee ePO interface includes pages where agent tasks and policies can be configured, and where agent properties can be viewed.

Contents
- Agent-server communication
- Viewing agent and product properties
- Responding to policy events
- Running client tasks immediately
- Sending manual wake-up calls to systems
- Sending manual wake-up calls to a group
- Locate inactive agents
- Queries provided by McAfee Agent
- Windows system and product properties reported by the agent

Agent-server communication

The agent has to talk to an ePolicy Orchestration server periodically to ensure all settings are current. These communications are referred to as agent-server communication. During each agent-server communication, the agent collects its current system properties, as well as events that have not yet been sent, and sends them to the server. The server sends new or changed policies and tasks to the agent, and the repository list if it has changed since the last agent-server communication. The agent enforces the new policies locally on the managed system and applies any task or repository changes.

ePolicy Orchestrator 4.0 uses a proprietary network protocol. Versions 4.5 and later use an industry-standard Transport Layer Security (TLS) network protocol for secure network transmissions.

After the agent is installed, it calls in to the server at a random time within ten minutes. Thereafter, the agent calls in whenever one of the following situations occurs:

- The agent-server communication interval (ASCI) lapses.
- At agent startup.
- Agent wake-up calls are sent from McAfee ePO or Agent Handlers.
- Communication is initiated manually from the managed system (Windows only).
Agent-server communication interval

The agent-server communication interval determines how often the agent calls in to the server.

The agent-server communication interval (ASCI) is set on the **General** tab of the McAfee Agent policy page. The default setting of 60 minutes means that the agent contacts the server once every hour. When deciding whether to modify the interval, consider what the agent does at each ASCI:

- The agent collects and sends its properties to the server or Agent Handler.
- The agent sends the events that have occurred since the last agent-server communication.
- The server or Agent Handler sends new policies and tasks to the client. This action might dictate other resource-consuming actions, such as an immediate DAT download.
- The agent enforces policies.

Although these activities do not burden any one computer, a number of factors can cause the cumulative demand on the network, McAfee ePO servers, or on Agent Handlers to be significant.
- A large number of systems being managed by ePolicy Orchestrator.
- Your organization has stringent threat response requirements.
- The network or physical location of clients in relation to servers or Agent Handlers is highly distributed.
- Inadequate available bandwidth.

In general, if your environment includes these variables, you want to perform an agent-server communication less frequently. For clients with critical functions, you might want to set a more frequent interval.

Agent-server communication interruption handling

Agent-server communication follows a specific algorithm designed to work around issues that might cause a problem connecting with an ePolicy Orchestrator server. Communication interruptions can happen for many of reasons, and the agent-server connection algorithm is designed to re-attempt communication if its first attempt fails.

The agent cycles through the following connection methods up to 6 times or until one of a set of responses is returned.

1. IP Address
2. Fully qualified domain name
3. NetBIOS

The agent iterates through those three connection methods in that order up to six times for a total of 18 connection attempts. There is no delay between connection attempts. The agent stops this cycle if a connection attempt results in any of the following:
- No error
- Download failed
- Upload failed
- Agent is shutting down
- Transfer aborted
- Server busy (status code from McAfee ePO)
• Upload success (status code from McAfee ePO)
• No package to receive (status code from McAfee ePO)
• Agent needs to regenerate GUID (status code from McAfee ePO)

Other results such as connection refused, failed to connect, connection timeout, or other errors causes the agent to retry immediately using the next connection method in the list.

**Wake-up calls and tasks**

The purpose of an agent wake-up call is to trigger an immediate agent-server communication rather than wait for the current agent-server communication interval to expire.

There are two ways to issue a wake-up call:

- Manually from the server — This is the most common approach and requires the agent wake-up communication port be open.
- On a schedule set by the administrator — This approach is useful when agent-server communication is disabled. The administrator can create and deploy a wake-up task, which triggers a wake-up call on a schedule.

Some reasons for issuing an agent wake-up call are:

- You make a policy change that you want the agent to adopt immediately, without waiting for the ASCI to expire.
- You created a new task that you want the agent to run immediately.
- A query generated a report indicating that a client is out of compliance, and you want to test its status as part of a troubleshooting procedure.

If you are have converted a particular Windows system to use as a SuperAgent, it can issue wake-up calls to designated network broadcast segments. SuperAgents distribute the bandwidth impact of the agent wake-up call, and help distribute network traffic.

**SuperAgents and broadcast wake-up calls**

If you operate in a Windows environment and plan to use agent wake-up calls to initiate agent-server communication, consider converting an agent on each network broadcast segment into a SuperAgent. SuperAgents distribute the bandwidth load of concurrent wake-up calls. Instead of sending agent wake-up calls from the server to every agent, the server sends the SuperAgent wake-up call to SuperAgents in the selected System Tree segment.

The process is:

1. Server sends a wake-up call to all SuperAgents.
2. SuperAgents broadcast a wake-up call to all agents in the same broadcast segment.
3. All notified agents (regular agents notified by a SuperAgent and all SuperAgents) exchange data with the server.

When you send a SuperAgent wake-up call, agents without an operating SuperAgent on their broadcast segment are not prompted to communicate with the server.
SuperAgent deployment tips

To deploy enough SuperAgents to the appropriate locations, first determine the broadcast segments in your environment and select a system (preferably a server) in each segment to host a SuperAgent. Be aware that agents in broadcast segments without SuperAgents do not receive the broadcast wake-up call, so they do not call in to the server in response to a wake-up call. If you use SuperAgents, make sure all agents are assigned a SuperAgent.

Agent and SuperAgent wake-up calls use the same secure channels. Make sure the following ports are not blocked by a firewall on the client:

- The agent wake-up communication port (8081 by default).
- The agent broadcast communication port (8082 by default).

SuperAgent caching and communication interruptions

The SuperAgent caches the contents of its repository in a specific manner designed to minimize wide-area network (WAN) usage.

If an agent has been converted to a SuperAgent, it can cache content from its McAfee ePO server to distribute locally to other agents, reducing WAN bandwidth. To activate this, turn on LazyCaching in the McAfee Agent | General policy options page which you access from Menu | Policy | Policy Catalog.

How the cache works

When a client system first requests content, the SuperAgent assigned to that system caches that content. From that point on, the cache is updated whenever a newer version of the package requested is available in the Master Repository.

The SuperAgent is guaranteed only to store content required by the agents assigned to it because it does not pull any content from the McAfee ePO server until requested from a client. This minimizes traffic between the SuperAgent and the McAfee ePO server. While the SuperAgent is retrieving content from the Master Repository, client system requests for that content are paused.

The SuperAgent must have access to the Master Repository. Without this access, agents receiving updates from the SuperAgent never receive new content. Make sure your SuperAgent policy includes access to the Master Repository.

Agents configured to use the SuperAgent as their repository receive the content cached in the SuperAgent repository instead of directly from the McAfee ePO server. This improves agent system performance by keeping the majority of network traffic local to the SuperAgent and its clients.

If the SuperAgent is reconfigured to use a new repository, the cache is updated to reflect the new repository.

When the cache is flushed

SuperAgents flush content from their cache in two situations.

- If the Checking new repository content interval has expired since the last time updates were requested, the SuperAgent downloads updates from the Master Repository, processes them, and completely flushes the cache if any new content is available.

- When a global update occurs, SuperAgents receive a wakeup call that flushes all content in the cache.

When the SuperAgent flushes its cache, it deletes every file in its repository not listed in Replica.log. This includes any personal files you might have put in that folder.
How communication interruptions are handled

When a SuperAgent receives a request for content that might be outdated, the SuperAgent attempts to contact the McAfee ePO server and other sites listed in Sitelist.xml to see if new content is available. If the connection attempts time out, the SuperAgent distributes content from its own repository instead. This is done to ensure the requester receives content even if that content might be outdated.

Viewing agent and product properties

A common troubleshooting task is to verify that the policy changes you made match the properties retrieved from a system.

The properties you see depend on whether you configured the agent to send full or minimal properties on the McAfee Agent policy pages.

Task
For option definitions, click ? in the interface.

1. Click Menu | Systems | System Tree.
2. On the Systems tab, click the row corresponding to the system you want to examine.

Information about the system's properties, installed products, and agent appear. New in ePolicy Orchestrator 4.6 is a ribbon at the top of the System Information page containing Summary, Properties, and Threat Events windows.

Responding to policy events

You can set up an automatic response in ePolicy Orchestrator filtered to see only policy events.

Task
For option definitions, click ? in the interface.

1. Click Menu | Automation | Automatic Responses to open the Automatic Responses page.
2. Click Actions | New Response.
3. Enter a Name for the response, and an optional Description.
4. Select ePO Notification Events for the Event group, and Client or Server for the Event type.
5. Click Enabled to enable the response and click Next.
6. From the Available Properties, select Event Description.
7 Click ... in the Event Description row and choose one of the following options from the list:

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent failed to collect properties for any point products</td>
<td>This event is broadcast when a property collection failure first occurs. A subsequent success event is not broadcast. Each failing point product generates a separate event.</td>
</tr>
<tr>
<td>Agent failed to enforce policy for any point products</td>
<td>This event is broadcast when a policy enforcement failure first occurs. A subsequent success event is not broadcast. Each failing point product generates a separate event.</td>
</tr>
</tbody>
</table>

8 Enter remaining information into the filter as needed, then click Next.

9 Select Aggregation, Grouping, and Throttling options as needed.

10 Choose an action type and enter the desired behavior depending on action type, then click Next.

11 Review the summarized response behavior. If correct, click Save.

An automatic response has now been created that will perform the described action when a policy event occurs.

---

**Running client tasks immediately**

When ePolicy Orchestrator 4.6 is communicating with McAfee Agent 4.6, you can run client tasks immediately using the run tasks now feature.

ePolicy Orchestrator puts tasks into a queue when they are scheduled to run instead of immediately executing them. While a task can be queued up immediately, it only starts executing at the same time if no other tasks are ahead of it in the queue. Tasks created during the Run Client Task Now procedure are run and the task is deleted after it finishes.

**Task**

For option definitions, click ? in the interface.

1 Click Menu | Systems | System Tree.

2 Select one or more systems on which to run a task.

3 Click Actions | Agent | Run Client Task Now.

4 Select the Product supplying the task and the Task Type.

5 To run an existing task, click the Task Name then click Run Task Now.

6 To define a new task, click Create New Task.

   a Enter the information appropriate to the task you are creating.

   If you create a McAfee Agent Product Deployment or Product Update task during this procedure, one of the available options is Run at every policy enforcement. This option has no effect as the task is deleted after it finishes.

The Running Client Task Status page appears, and displays the state of all running tasks. When the tasks are complete, the results can be viewed in the Audit Log and Server Log.
Sending manual wake-up calls to systems

Manually sending an agent or SuperAgent wake-up call to systems in the System Tree is useful when you make policy changes and you want agents to call in for an update before the next agent-server communication.

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

1. Click **Menu** | **Systems** | **System Tree**, then select the group that contains the target systems.
2. Select the systems from the list, then click **Actions** | **Agent** | **Wake Up Agents**.
3. Make sure the systems you selected appear in the **Target** section.
4. Next to **Wake-up call type**, select whether to send an **Agent Wake-Up Call** or **SuperAgent Wake-Up Call**.
5. Accept the default **Randomization** (0 - 60 minutes) or type a different value. Consider the number of systems that are receiving the wake-up call, and how much bandwidth is available. If you type 0, agents respond immediately.
6. To send minimal product properties as a result of this wake-up call, deselect **Get full product properties**.... The default is to send full product properties.
7. To update all policies and tasks during this wake-up call, select **Force complete policy and task update**.
8. Enter a **Number of attempts**, **Retry interval**, and **Abort after** settings for this wake-up call if you do not want the default values.
9. Click **OK** to send the agent or SuperAgent wake-up call.

Sending manual wake-up calls to a group

An agent or SuperAgent wake-up call can be sent to an entire System Tree group in a single task. This is useful when you have made policy changes and want agents to call in for an update before the next agent-server communication.

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

1. Click **Menu** | **Systems** | **System Tree**.
2. Select the target group from the **System Tree** and click the **Group Details** tab.
3. Click **Actions** | **Wake Up Agents**.
4. Make sure the selected group appears next to **Target group**.
5. Select whether to send the 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. Accept the default **Randomization** (0 - 60 minutes), or type a different value. If you type 0, agents awaken immediately.
To send minimal product properties as a result of this wake-up call, deselect *Get full product properties...*.
The default is to send full product properties.

To update all policies and tasks during this wake-up call, select *Force complete policy and task update*.

Click **OK** to send the agent or SuperAgent wake-up call.

---

### Locate inactive agents

An inactive agent is one that has not communicated with the McAfee ePO server within a user-specified time period.

Some agents might become disabled or be uninstalled by users. In other cases, the system hosting the agent might have been removed from the network. McAfee recommends performing regular weekly searches for systems with these inactive agents.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu** | **Reporting** | **Queries & Reports**.
2. In the **Groups** list, select the **McAfee Agent** shared group.
3. Click **Run** in the **Inactive Agents** row to run the query.

The default configuration for this query finds systems that have not communicated with the McAfee ePO server in the last month. You can specify hours, days, weeks, quarters or years.

When you find inactive agents, review their activity logs for problems that might interfere with agent-server communication. The query results allow you to take a variety of actions with respect to the systems identified, including ping, delete, wake up, and re-deploy an agent.

---

### Queries provided by McAfee Agent

McAfee Agent adds a number of standard queries to your ePolicy Orchestrator environment.

The following queries are installed into the McAfee Agent shared group.

**Table 13-1  Queries provided by McAfee Agent**

<table>
<thead>
<tr>
<th>Query</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Communication Summary</td>
<td>A pie chart of managed systems indicating whether the agents have communicated with the McAfee ePO server within the past day.</td>
</tr>
<tr>
<td>Agent Handler Status</td>
<td>A pie chart displaying Agent Handler communication status within the last hour.</td>
</tr>
<tr>
<td>Agent Versions Summary</td>
<td>A pie chart of installed agents by version number on managed systems.</td>
</tr>
<tr>
<td>Inactive Agents</td>
<td>A table listing all managed systems whose agents have not communicated within the last month.</td>
</tr>
<tr>
<td>Managed nodes having point product policy enforcement failures</td>
<td>A single group bar chart showing all nodes having at least one policy enforcement failure in the last 24 hours.</td>
</tr>
<tr>
<td>Managed nodes having point product property collection failures</td>
<td>A single group bar chart showing all nodes having at least one property collection failure in the last 24 hours.</td>
</tr>
</tbody>
</table>
Table 13-1  Queries provided by McAfee Agent  (continued)

<table>
<thead>
<tr>
<th>Query</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repositories and Percentage Utilization</td>
<td>A pie chart displaying individual repository utilization as a percentage of all repositories.</td>
</tr>
<tr>
<td>Repository Usage Based on DAT and Engine Pulling</td>
<td>A stacked bar chart displaying DAT and Engine pulling per repository.</td>
</tr>
<tr>
<td>Systems per Agent Handler</td>
<td>A pie chart displaying the number of managed systems per Agent Handler.</td>
</tr>
</tbody>
</table>

Windows system and product properties reported by the agent

The lists below show the data reported to ePolicy Orchestrator from its managed systems. The properties reported vary by operating system. Those listed here are properties reported by Windows.

System properties

This list shows the system data reported to ePolicy Orchestrator by your nodes' operating systems. Review the details on your system before concluding that system properties are incorrectly reported.

- **Agent Version**
- **CPU Serial Number**
- **CPU Speed (MHz)**
- **CPU Type**
- **Custom Props 1-4**
- **Default Language**
- **Description**
- **DNS Name**
- **Domain Name**
- **Free Disk Space**
- **Free Memory**
- **Installed Products**
- **IP Address**
- **IPX Address**
- **Is 64 Bit OS**
- **Is Laptop**
- **Last Communication**
- **Management Type**
- **Number Of CPUs**
- **Operating System**
- **OS Build Number**
- **OS OEM Identifier**
- **OS Platform**
- **OS Service Pack Version**
- **OS Type**
- **OS Version**
- **Subnet Address**
- **Subnet Mask**
- **System Description**
- **System Location**
- **System Name**
- **System Tree Sorting**
- **Tags**
- **Time Zone**
- **Total Disk Space**
- **Total Physical Memory**
- **Used Disk Space**
- **User Name**

Product properties

Each McAfee product designates the properties it reports to ePolicy Orchestrator and, of those, which are included in a set of minimal properties. This list shows the kinds of product data that are reported to ePolicy Orchestrator by the McAfee software installed on your system. If you find errors in the reported values, review the details of your products before concluding that they are incorrectly reported.

- **Agent Wake-Up Communication Port**
- **Agent-to-Server Communication Interval**
- **DAT Version**
- **Engine Version**
- **HotFix/Patch Version**
- **Language**
- **License Status**
- **Policy Enforcement Interval**
- **Product Version**
- **Service Pack**
Using the Software Manager to check in software

The Software Manager provides a single location within the ePolicy Orchestrator console to review and acquire McAfee software and software components.

Contents

- What's in the Software Manager
- Checking in, updating, and removing software using the Software Manager

What's in the Software Manager

The Software Manager eliminates the need to access the McAfee Product Download website to obtain new McAfee software and software updates.

You can use the Software Manager to download:

- Licensed software
- Evaluation software
- Software updates
- Product documentation

DATs and Engines are not available from the Software Manager.
Licensed software
Licensed software is any software your organization has purchased form McAfee. When viewing the Software Manager in the ePolicy Orchestrator console, any software licensed to your company not already installed on your server is listed in the Software Not Checked In product category. The number displayed next to each subcategory in the Product Categories list indicates how many products are available.

Evaluation software
Evaluation software is software for which your organization does not currently possess a license. You can install evaluation software on your server, but functionality might be restricted until you acquire a product license.

Software updates
When a new update for the software you're using is released, you can use the Software Manager to check in new packages and extensions. Available software updates are listed in the Updates Available category.

Product documentation
New and updated product documentation can be obtained from the Software Manager. Help extensions can be installed automatically. PDF and HTML documentation such as Product Guides and Release Notes can also be downloaded from the Software Manager.

About software component dependencies
Many of the software products you can install for use with your McAfee ePO server have predefined dependencies on other components. Dependencies for product extensions are installed automatically. For all other product components, you must review the dependencies list in the component details page, and install them first.

Checking in, updating, and removing software using the Software Manager
From the Software Manager, you can check in, update, and remove McAfee managed product components from your server.

Both licensed and evaluation software can be accessed in the Software Manager.

Software availability, and whether it is in the Licensed or Evaluation category, depends on your License key. For more information, contact your Administrator.
Task
For option definitions, click ? in the interface.

1. Click Menu | Software | Software Manager.

2. In the Software Manager page Product Categories list, select one of the following categories, or use the search box to find your software:
   - Updates Available — Lists any available updates to licensed software components already installed or checked into this ePolicy Orchestrator server.
   - Checked in Software — Displays all software (both Licensed and Evaluation) installed or checked into this server.
   - Software Not Checked in — Displays any software that is available, but not installed on this server.
   - Software (by Label) — Displays software by function as described by McAfee product suites.

3. When you’ve located the correct software, click:
   - Download to download product documentation to a location on your network.
   - Check in to check in a product extension or package on this server.
   - Update to update a package or extension that is currently installed or checked into this server.
   - Remove to uninstall a package or extension that is currently installed or checked into this server.

4. In the Check In Software Summary page, review and accept the product details and End User License Agreement (EULA), then click OK to complete the operation.
Using policies to manage products and systems

Policies ensure that a product's features are configured correctly on your managed systems.
Managing products from a single location is a central feature of ePolicy Orchestrator. One of the ways this is accomplished is through application and enforcement of product policies. Policies ensure a product’s features are configured correctly, while client tasks are the scheduled actions that run on the managed systems hosting any client-side software.

Are you configuring policies for the first time?

When configuring policies for the first time:

1. Plan product policies for the segments of your System Tree.
2. Create and assign policies to groups and systems.

Contents
- Policy management
- Policy application
- How policy assignment rules work
- Creating Policy Management queries
- Working with the Policy Catalog
- Working with policies
- Viewing policy information
- Sharing policies among McAfee ePO servers
- Frequently asked questions

Policy management

A policy is a collection of settings that you create, configure, then enforce. Policies ensure that the managed security software products are configured and perform accordingly.
Some policy settings are the same as the settings you configure in the interface of the product installed on the managed system. Other policy settings are the primary interface for configuring the product or component. The ePolicy Orchestrator console allows you to configure policy settings for all products and systems from a central location.
**Policy categories**

Policy settings for most products are grouped by category. Each policy category refers to a specific subset of policy settings. Policies are created by category. In the Policy Catalog page, policies are displayed by product and category. When you open an existing policy or create a new policy, the policy settings are organized across tabs.

**Where policies are displayed**

To see all of the policies that have been created per policy category, click Menu | Policy | Policy Catalog, then select a Product and Category from the drop-down lists. On the Policy Catalog page, users can see only policies of the products to which they have permissions.

To see which policies, per product, are applied to a specific group of the System Tree, click Menu | Systems | System Tree | Assigned Policies page, select a group, then select a Product from the drop-down list.

> A McAfee Default policy exists for each category. You cannot delete, edit, export, or rename these policies, but you can copy them and edit the copy.

**How policy enforcement is set**

For each managed product or component, choose whether the agent enforces all or none of its policy selections for that product or component.

From the Assigned Policies page, choose whether to enforce policies for products or components on the selected group.

In the Policy Catalog page, you can view policy assignments, where they are applied, and if they are enforced. You can also lock policy enforcement to prevent changes to enforcement below the locked node.

> If policy enforcement is turned off, systems in the specified group do not receive updated sitelists during an agent-server communication. As a result, managed systems in the group might not function as expected. For example, you might configure managed systems to communicate with Agent Handler A, but with policy enforcement turned off, the managed systems won't receive the new sitelist with this information, so they report to a different Agent Handler listed in an expired sitelist.

**When policies are enforced**

When you reconfigure policy settings, the new settings are delivered to, and enforced on, the managed systems at the next agent-server communication. The frequency of this communication is determined by the Agent-to-server-communication interval (ASCI) settings on the General tab of the McAfee Agent policy pages, or the McAfee Agent Wakeup client task schedule (depending on how you implement agent-server communication). This interval is set to occur once every 60 minutes by default.

Once the policy settings are in effect on the managed system, the agent continues to enforce policy settings locally at a regular interval. This enforcement interval is determined by the Policy enforcement interval setting on the General tab of the McAfee Agent policy pages. This interval is set to occur every five minutes by default.

Policy settings for McAfee products are enforced immediately at the policy enforcement interval, and at each agent-server communication if policy settings have changed.
Exporting and importing policies

If you have multiple servers, you can export and import policies between them via XML files. In such an environment, you only need to create a policy once.

You can export and import individual policies, or all policies for a given product.

This feature can also be used to back up policies if you need to reinstall the server.

Policy sharing

Policy sharing is another way to transfer policies between servers. Sharing policies allows you to manage policies on one server, and use them on many additional servers all through the McAfee ePO console. For more information, see Sharing policies among McAfee ePO servers.

Policy application

Policies are applied to any system by one of two methods, inheritance or assignment.

Inheritance

Inheritance determines whether the policy settings and client tasks for a group or system are taken from its parent. By default, inheritance is enabled throughout the System Tree.

When you break this inheritance by assigning a new policy anywhere in the System Tree, all child groups and systems that are set to inherit the policy from this assignment point do so.

Assignment

You can assign any policy in the Policy Catalog to any group or system, provided you have the appropriate permissions. Assignment allows you to define policy settings once for a specific need, then apply the policy to multiple locations.

When you assign a new policy to a particular group of the System Tree, all child groups and systems that are set to inherit the policy from this assignment point do so.

Assignment locking

You can lock the assignment of a policy on any group or system, provided you have the appropriate permissions. Assignment locking prevents other users:

- With appropriate permissions at the same level of the System Tree from inadvertently replacing a policy.
- With lesser permissions (or the same permissions but at a lower level of the System Tree) from replacing the policy.

Assignment locking is inherited with the policy settings.

Assignment locking is valuable when you want to assign a certain policy at the top of the System Tree and ensure that no other users replace it anywhere in the System Tree.

Assignment locking only locks the assignment of the policy, but does not prevent the policy owner from making changes to its settings. Therefore, if you intend to lock a policy assignment, make sure that you are the owner of the policy.
Policy ownership

All policies for products and features to which you have permissions are available from the Policy Catalog page. To prevent any user from editing other users’ policies, each policy is assigned an owner — the user who created it.

Ownership provides that no one can modify or delete a policy except its creator or a global administrator. Any user with appropriate permissions can assign any policy in the Policy Catalog page, but only the owner or a global administrator can edit it.

If you assign a policy that you do not own to managed systems, be aware that if the owner of the named policy modifies it, all systems where this policy is assigned receive these modifications. Therefore, if you wish to use a policy owned by a different user, McAfee recommends that you first duplicate the policy, then assign the duplicate to the desired locations. This provides you ownership of the assigned policy.

You can specify multiple non-global administrator users as owners of a single policy.

How policy assignment rules work

Policy assignments rules reduce the overhead of managing numerous policies for individual users or systems that meet specific criteria, while maintaining more generic policies across your System Tree.

This level of granularity in policy assignment limits the instances of broken inheritance in the System Tree needed to accommodate the policy settings that particular users or systems require. Policy assignments can be based on either user specific or system specific criteria:

- **User-based policies** — Policies that include at least one user specific criteria. For example, you can create a policy assignment rule that is enforced for all users in your engineering group. You can then create another policy assignment rule for members of your IT department so they can log on to any computer in the engineering network with the access rights they need to troubleshoot problems on a specific system in that network. User based policies can also include system based criteria.

- **System-based policies** — Policies that include only system based criteria. For example, you can create a policy assignment rule that is enforced for all servers on your network based on the tags you’ve applied, or all systems in a specific location in your System Tree. System based policies cannot include user based criteria.

Policy assignment rule priority

Policy assignment rules can be prioritized to simplify maintenance of policy assignment management. When you set priority to a rule, it is enforced before other assignments with a lower priority.

In some cases, the outcome can be that some rule settings are overridden. For example, consider a user or system that is included in two policy assignment rules, rules A and B. Rule A has priority level 1, and allows included users unrestricted access to internet content. Rule B has priority level 2, and heavily restricts the same user’s access to internet content. In this scenario, rule A is enforced because it has higher priority. As a result, the user has unrestricted access to internet content.
How multi-slot policies work with policy assignment rule priority

Priority of rules is not considered for multi-slot policies. When a single rule containing multi-slot policies of the same product category is applied, all settings of the multi-slot policies are combined. Similarly, if multiple rules containing multi-slot policy settings are applied, all settings from each multi-slot policy are combined. As a result, the applied policy is a combination of the settings of each individual rule.

When multi-slot policies are aggregated, they are aggregated only with multi-slot policies of the same type; user-based or system-based. However, multi-slot policies assigned using policy assignment rules are not aggregated with multi-slot policies assigned in the System Tree. Multi-slot policies assigned using policy assignment rules override policies assigned in the System Tree. Furthermore, user-based policies take priority over system-based policies. Consider the following scenario where:

<table>
<thead>
<tr>
<th>Policy type</th>
<th>Assignment type</th>
<th>Policy name</th>
<th>Policy settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generic policy</td>
<td>Policy assigned in the</td>
<td>A</td>
<td>Prevents internet access from all systems to which the</td>
</tr>
<tr>
<td></td>
<td>System Tree</td>
<td></td>
<td>policy is assigned.</td>
</tr>
<tr>
<td>System-based</td>
<td>Policy assignment rule</td>
<td>B</td>
<td>Allows internet access from systems with the tag &quot;IsLaptop.&quot;</td>
</tr>
<tr>
<td>User-based</td>
<td>Policy assignment rule</td>
<td>C</td>
<td>Allows unrestricted internet access to all users in the Admin user group from all systems.</td>
</tr>
</tbody>
</table>

Scenario: Using multi-slot policies to control Internet access

In your System Tree, there is a group named "Engineering" which consists of systems tagged with either "IsServer" or "IsLaptop." In the System Tree, policy A is assigned to all systems in this group. Assigning policy B to any location in the System Tree above the Engineering group using a policy assignment rule overrides the settings of policy A, and allows systems tagged with "IsLaptop" to access the internet. Assigning policy C to any group in the System Tree above the Engineering group allows users in the Admin user group to access the internet from all systems, including those in the Engineering group tagged with "IsServer."

Excluding Active Directory objects from aggregated policies.

Because rules that consist of multi-slot policies are applied to assigned systems without regard to priority, you might need to prevent policy setting aggregation in some instances. You can prevent aggregation of user-based multi-slot policy settings across multiple policy assignment rules by excluding a user (or other Active Directory objects such as a group or organizational unit) when creating the rule. For more information on the multi-slot policies that can be used in policy assignment rules, refer to the product documentation for the managed product you are using.

About user-based policy assignments

User-based policy assignment rules give you the ability to create user specific policy assignments. These assignments are enforced at the target system when a user logs on.
On a managed system, the agent keeps a record of the users who log on to the network. The policy assignments you create for each user are pushed down to the system they log on to, and are cached during each agent-server communication. The agent applies the policies that you have assigned to each user.

When a user logs on to a managed system for the first time, there can be a slight delay while the agent contacts its assigned server for the policy assignments specific to this user. During this time, the user has access only to that functionality allowed by the default machine policy, which typically is your most secure policy.

To use user-based policy assignments, you must first register and configure a registered LDAP server for use with your ePolicy Orchestrator server.

**About migrating legacy policy assignment rules**

Policy assignment rules created using a version 4.5 ePolicy Orchestrator server were user-based by default. For migrated legacy policy assignment rules with no user-based criteria specified, the rules will continue to be evaluated as user-based. However, when creating a new user-based policy assignment rule, you must specify at least one user-based criteria.

Applying your migrated legacy user-based policy assignment rules causes your ePolicy Orchestrator server to perform a look up on the LDAP server for every managed system in your network at each agent-server communication interval.

**About system-based policy assignments**

System-based policies allow you to assign policies to systems using system based criteria.

You can assign a system-based policy using two types of system-based criteria:

- **System Tree location** — All policy assignment rules require that System Tree location is specified.
- **Tags** — User defined tags can be used to assign policies to system based on the tags you have applied.

Once you have defined and applied a tag to your systems, you can create a policy assignment rule to assign policies to any system with that tag. This functionality is useful in cases when you want all systems of a particular type to have the same security policy, regardless of their location in the System Tree.

**Using tags to assign system-based policies**

Using tags to assign system-based policies makes automating policy assignment easier than ever.

System-based policies which specify tags as criteria work in a similar fashion to user-based policies. They are assigned based on selection criteria you define using the Policy Assignment Builder. Any system you can tag, you can apply a specific policy to, based on that tag.
Scenario: Creating new SuperAgents using tags

You've decided to create a new set of SuperAgents in your environment, but you don't have time to manually identify the systems in your System Tree that will host these SuperAgents. Instead, you can use the Tag Builder to tag all systems that meet a specific set of criteria with a new tag: "isSuperAgent." Once you've built the tag, you can create a Policy Assignment Rule that applies your SuperAgent policy settings to every system tagged with "isSuperAgent."

Once the tag is created, you can use the Run Tag Criteria action from the Tag Catalog page, and as each system with the new tag calls in at its regular interval, it is assigned a new policy based on your isSuperAgent Policy Assignment Rule.

Working with policy assignment rules

Use these tasks to configure and manage policy assignment rules. With these tasks you can set up, create, and manage policy assignment rules in your network.

Tasks

- Creating policy assignment rules on page 169
  Use this task to create policy assignment rules. Policy assignment rules allow you to enforce policies for users or systems based on configured rule criteria.

- Managing policy assignment rules on page 170
  Use this table to perform common management tasks when working with policy assignment rules.

Creating policy assignment rules

Use this task to create policy assignment rules. Policy assignment rules allow you to enforce policies for users or systems based on configured rule criteria.

Task

For option definitions, click ? in the interface.

1 Click Menu | Policy | Policy Assignment Rules, then click Actions | New Assignment Rule. The Policy Assignment Builder opens to the Details page.

2 Specify the details for this policy assignment rule, including:
   - A unique Name and Description.
   - The Rule Type. The rule type you specify determines which criteria is available in the Selection Criteria step.

   By default, the priority for new policy assignment rules is assigned sequentially based on the number of existing rules. After you've create the rule, you can edit the priority by clicking Edit Priority on the Policy Assignment Rules page.

3 Click Next. The Assigned Policies page opens.

4 Click Add Policy to select the policies that you want to be enforced by this policy assignment rule.

5 Click Next. The Selection Criteria page opens.

6 Specify the criteria you want to use in this rule. Your criteria selection determines which systems or users are assigned this policy.

7 Review the summary and click Save.
Managing policy assignment rules
Use this table to perform common management tasks when working with policy assignment rules.

To perform these actions, click Menu | Policy | Policy Assignment Rules. Select the action to perform from the Actions menu or the Actions column.

<table>
<thead>
<tr>
<th>To do this...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete a policy assignment rule</td>
<td>Click Delete in the selected assignment row.</td>
</tr>
<tr>
<td>Edit a policy assignment rule</td>
<td>Click on the selected assignment. The Policy Assignment Builder wizard opens. Work through each page of this wizard to modify this policy assignment rule.</td>
</tr>
<tr>
<td>Export policy assignment rules</td>
<td>Click Export. The Download Policy Assignment Rules page opens, where you can view or download the PolicyAssignmentRules.xml file.</td>
</tr>
<tr>
<td>Import policy assignment rules</td>
<td>Click Import. The Import Policy Assignment Rules dialog box opens, from which you can browse to a previously downloaded PolicyAssignmentRules.xml file. You are prompted to choose which rules included in the file to import. You can select which rules to import and, if any rules in the file have the same name as those already in your Policy Assignment Rules list, you can select which to retain.</td>
</tr>
<tr>
<td>Edit the priority of a policy assignment rule</td>
<td>Click Edit Priority. The Policy Assignment Rule</td>
</tr>
<tr>
<td>View the summary of a policy assignment rule</td>
<td>Click &gt; in the selected assignment row.</td>
</tr>
</tbody>
</table>

Creating Policy Management queries
Use this task to create either of the following Policy Management queries:

- **Applied Policies** query — Retrieves policies assigned to a specified managed systems.
- **Broken Inheritance** query — Retrieves information on policies that are broken in the system hierarchy.

**Task**

For option definitions, click ? in the interface.

1. Click Menu | Reporting | Queries & Reports, then click Actions | New. The Query Builder wizard opens.
2. On the Result Type page, select Policy Management from the Feature Group list.
3. Select one of these Result Types, then click Next to display the Chart page:
   - **Applied Client Tasks**
   - **Applied Policies**
   - **Client Tasks Assignment Broken Inheritance**
   - **Policies Assignment Broken Inheritance**
4. Select the type of chart or table to display the primary results of the query, then click Next. The Columns page appears.

   If you select **Boolean Pie Chart**, you must configure the criteria you want to include in the query.
5 Select the columns to be included in the query, then click **Next**. The Filter page appears.

6 Select properties to narrow the search results, then click **Run**. The Unsaved Query page displays the results of the query, which is actionable.

   [Information] Selected properties appear in the content pane with operators that can specify criteria, which narrows the data that is returned for that property.

7 In the Unsaved Query page, take any available actions on items in any tables or drill-down tables.
   - If the query didn't return the expected results, click **Edit Query** to go back to the Query Builder and edit the details of this query.
   - If you don't need to save the query, click **Close**.
   - If you want to use again this query again, click **Save** and continue to the next step.

8 In the Save Query page, type a name for the query, add any notes, and select one of the following:
   - **New Group** — Type the new group name and select either:
     - **Private group (My Groups)**
     - **Public group (Shared Groups)**
   - **Existing Group** — Select the group from the list of **Shared Groups**.

9 Click **Save**.

---

**Working with the Policy Catalog**

Use these tasks to create and maintain policies from the Policy Catalog page.

**Tasks**

- **Creating a policy from the Policy Catalog page** on page 172
  Use this task to create a new policy from the Policy Catalog. By default, policies created here are not assigned to any groups or systems. When you create a policy here, you are adding a custom policy to the Policy Catalog.

- **Duplicating a policy on the Policy Catalog page** on page 172
  Use this task to create a new policy based on an existing one. For example, if you already have a policy that is similar to one you want to create, you can duplicate the existing one, then make the desired changes.

- **Editing a policy’s settings from the Policy Catalog** on page 173
  Use this task to modify the settings of a policy. Your user account must have appropriate permissions to edit policy settings for the desired product.

- **Renaming a policy from the Policy Catalog** on page 173
  Use this task to rename a policy. Your user account must have appropriate permissions to edit policy settings for the desired product.

- **Deleting a policy from the Policy Catalog** on page 173
  Use this task to delete a policy from the Policy Catalog. When you delete a policy, all groups and systems where it is currently applied inherit the policy of their parent group. Before deleting a policy, review the groups and systems where it is assigned. If you don’t want the group or system to inherit the policy from the parent group, assign a different policy.
Creating a policy from the Policy Catalog page

Use this task to create a new policy from the Policy Catalog. By default, policies created here are not assigned to any groups or systems. When you create a policy here, you are adding a custom policy to the Policy Catalog.

You can create policies before or after a product is deployed.

For option definitions, click ? in the interface.

**Task**

1. Click **Menu | Policy | Policy Catalog**, then select the **Product** and **Category** from the drop-down lists. All created policies for the selected category appear in the details pane.

2. Click **Actions | New Policy**. The New Policy dialog box appears.

3. Select the policy you want to duplicate from the **Create a policy based on this existing policy** drop-down list.

4. Type a name for the new policy and click **OK**. The Policy Settings wizard opens.

5. Edit the policy settings on each tab as needed.

6. Click **Save**.

Duplicating a policy on the Policy Catalog page

Use this task to create a new policy based on an existing one. For example, if you already have a policy that is similar to one you want to create, you can duplicate the existing one, then make the desired changes.

For option definitions, click ? in the interface.

**Task**

1. Click **Menu | Policy | Policy Catalog**, then select the **Product** and **Category** from the drop-down lists. All created policies for the selected category appear in the details pane.

2. Locate the policy to duplicate, then click **Duplicate** in that policy’s row. The Duplicate Existing Policy dialog box appears.

3. Type the name of the new policy in the field, then click **OK**. The new policy appears on the Policy Catalog page.

4. Click on the new policy in the list.

5. Edit the settings as needed, then click **Save**.
Editing a policy’s settings from the Policy Catalog
Use this task to modify the settings of a policy. Your user account must have appropriate permissions
to edit policy settings for the desired product.

For option definitions, click ? in the interface.

**Task**

1. Click *Menu | Policy | Policy Catalog*, then select the *Product* and *Category* from the drop-down lists.
   All created policies for the selected category appear in the details pane.

2. Locate the desired policy, then click on the policy name.

3. Edit the settings as needed, then click *Save*.

Renaming a policy from the Policy Catalog
Use this task to rename a policy. Your user account must have appropriate permissions to edit policy
settings for the desired product.

**Task**

For option definitions, click ? in the interface.

1. Click *Menu | Policy | Policy Catalog*, then select the *Product* and *Category* from the drop-down lists.
   All created policies for the selected category appear in the details pane.

2. Locate the desired policy, then click *Rename* in the desired policy’s row.
   The Rename Policy dialog box appears.

3. Type a new name for the existing policy, then click *OK*.

Deleting a policy from the Policy Catalog
Use this task to delete a policy from the Policy Catalog. When you delete a policy, all groups and
systems where it is currently applied inherit the policy of their parent group. Before deleting a policy,
review the groups and systems where it is assigned. If you don’t want the group or system to inherit
the policy from the parent group, assign a different policy.

If you delete a policy that is applied to the My Organization group, the McAfee Default policy of this
category is assigned.

For option definitions, click ? in the page interface.

**Task**

1. Click *Menu | Policy | Policy Catalog*, then select the *Product* and *Category* from the drop-down lists.
   All created policies for the selected category appear in the details pane.

2. Locate the desired policy, then click *Delete* in the policy’s row.

3. Click *OK* when prompted.

**Working with policies**
Use these tasks to assign and manage the policies in your environment.
Tasks

- **Configuring agent policies to use a distributed repository on page 174**
  Use this task to customize how agents select distributed repositories.

- **Changing the owners of a policy on page 175**
  Use this task to change the owners of a policy. By default, ownership is assigned to the user that created the policy. This task can only be performed by global administrators.

- **Moving policies between McAfee ePO servers on page 175**
  Use these tasks to move policies between servers. To do this, you must export the policy to an XML file from the Policy Catalog page of the source server, then import it to the Policy Catalog page on the target server.

- **Assigning a policy to a group of the System Tree on page 176**
  Use this task to assign a policy to a specific group of the System Tree. You can assign policies before or after a product is deployed.

- **Assigning a policy to a managed system on page 177**
  Use this task to assign a policy to a specific managed system. You can assign policies before or after a product is deployed.

- **Assigning a policy to multiple managed systems within a group on page 177**
  Use this task to assign a policy to multiple managed systems within a group. You can assign policies before or after a product is deployed.

- **Enforcing policies for a product on a group on page 178**
  Use this task to enable or disable policy enforcement for a product on a System Tree group. Policy enforcement is enabled by default, and is inherited in the System Tree.

- **Enforcing policies for a product on a system on page 178**
  Use this task to enable or disable policy enforcement for a product on a system. Policy enforcement is enabled by default, and is inherited in the System Tree.

- **Copying and pasting assignments on page 179**
  Use these tasks to copy and paste policy assignments from one group or system to another. This is an easy way to share multiple assignments between groups and systems from different portions of the System Tree.

**Configuring agent policies to use a distributed repository**

Use this task to customize how agents select distributed repositories.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu | Policy | Policy Catalog**, then select the **Product** as **McAfee Agent** and **Category** as **Repository**.

2. Click on the required existing agent policy.

3. Select the **Repositories** tab.

4. From **Repository list selection**, select either **Use this repository list** or **Use other repository list**.
5 Under **Select repository by**, specify the method to sort repositories:
- **Ping time** — Sends an ICMP ping to the closest five repositories (based on subnet value) and sorts them by response time.
- **Subnet distance** — Compares the IP addresses of client systems and all repositories and sorts repositories based on how closely the bits match. The more closely the IP addresses resemble each other, the higher in the list the repository is placed.
  - If needed you can set the **Maximum number of hops**.
- **User order in repository list** — Selects repositories based on their order in the list.

6 From the **Repository list** you can disable repositories by clicking **Disable** in the **Actions** field associated with the repository to be disabled.

7 In the **Repository list**, click **Move to Top** or **Move to Bottom** to specify the order in which you want client systems to select distributed repositories.

8 Click **Save** when finished.

**Changing the owners of a policy**

Use this task to change the owners of a policy. By default, ownership is assigned to the user that created the policy. This task can only be performed by global administrators.

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

1 Click **Menu | Policy | Policy Catalog**, then select the **Product and Category**. All created policies for the selected category appear in the details pane.

2 Locate the desired policy, then click on the **Owner of the policy**. The Policy Ownership page appears.

3 Select the desired owners of the policy from the list, then click **OK**.

**Moving policies between McAfee ePO servers**

Use these tasks to move policies between servers. To do this, you must export the policy to an XML file from the Policy Catalog page of the source server, then import it to the Policy Catalog page on the target server.

**Tasks**
- **Exporting a single policy on page 175**
  Use this task to export a policy to an XML file. Use this file to import the policy to another McAfee ePO server, or to keep as a backup of the policy.
- **Exporting all policies of a product on page 176**
  Use this task to export all policies of a product to an XML file. Use this file to import the policy to another McAfee ePO server, or to keep as a backup of the policies.
- **Importing policies on page 176**
  Use this task to import a policy XML file. Regardless of whether you exported a single policy or all named policies, the import procedure is the same.

**Exporting a single policy**

Use this task to export a policy to an XML file. Use this file to import the policy to another McAfee ePO server, or to keep as a backup of the policy.
Task
For option definitions, click ? in the interface.

1. Click Menu | Policy | Policy Catalog, then select the Product and Category from the drop-down lists.
   All created policies for the selected category appear in the details pane.

2. Locate the desired policy, then click Export next to the policy.
   The Export page appears.

3. Right-click the link to download and save the file.

4. Name the policy XML file and save it.

   If you plan to import this file into a different McAfee ePO server, ensure that this location is accessible to the target ePolicy Orchestrator server.

Exporting all policies of a product
Use this task to export all policies of a product to an XML file. Use this file to import the policy to another McAfee ePO server, or to keep as a backup of the policies.

Task
For option definitions, click ? in the interface.

1. Click Menu | Policy | Policy Catalog, then select the Product and Category.
   All created policies for the selected category appear in the details pane.

2. Click Export next to Product policies. The Export page appears.

3. Right-click the link to download and save the file.

   If you plan to import this file into a different McAfee ePO server, ensure that this location is accessible to the target ePolicy Orchestrator server.

Importing policies
Use this task to import a policy XML file. Regardless of whether you exported a single policy or all named policies, the import procedure is the same.

Task
For option definitions, click ? in the interface.

1. Click Menu | Policy | Policy Catalog, then click Import next to Product policies.

2. Browse to and select the desired policy XML file, then click OK.

3. Select the policies you want to import and click OK.
   The policies are added to the policy catalog.

Assigning a policy to a group of the System Tree
Use this task to assign a policy to a specific group of the System Tree. You can assign policies before or after a product is deployed.
Task
For option definitions, click ? in the interface.

1 Click Menu | Systems | System Tree | Assigned Policies, then select the desired Product.
Each assigned policy per category appears in the details pane.

2 Locate the desired policy category, then click Edit Assignment.
The Policy Assignment page appears.

3 If the policy is inherited, select Break inheritance and assign the policy and settings below next to Inherited from.

4 Select the desired policy from the Assigned policy drop-down list.

From this location, you can also edit the selected policy's settings, or create a new policy.

5 Choose whether to lock policy inheritance.
Locking policy inheritance prevents any systems that inherit this policy from having another one assigned in its place.

6 Click Save.

Assigning a policy to a managed system
Use this task to assign a policy to a specific managed system. You can assign policies before or after a product is deployed.

Task
For option definitions, click ? in the interface.

1 Click Menu | Systems | System Tree | Systems, then select the desired group under System Tree.
All the systems within this group (but not its subgroups) appear in the details pane.

2 Select the desired system, then click Actions | Agent | Modify Policies on a Single System.
The Policy Assignment page for that system appears.

3 Select the desired Product.
The categories of selected product are listed with the system's assigned policy.

4 Locate the desired policy category, then click Edit Assignments.

5 If the policy is inherited, select Break inheritance and assign the policy and settings below next to Inherited from.

6 Select the desired policy from the Assigned policy drop-down list.

From this location, you can also edit settings of the selected policy, or create a new policy.

7 Choose whether to lock policy inheritance.
Locking policy inheritance prevents any systems that inherit this policy from having another one assigned in its place.

8 Click Save.

Assigning a policy to multiple managed systems within a group
Use this task to assign a policy to multiple managed systems within a group. You can assign policies before or after a product is deployed.
Task
For option definitions, click ? in the interface.

1 Click Menu | Systems | System Tree | Systems, then select the desired group in the System Tree. All the systems within this group (but not its subgroups) appear in the details pane.

2 Select the desired systems, then click Actions | Agent | Set Policy & Inheritance. The Assign Policy page appears.

3 Select the Product, Category, and Policy from the drop-down lists.

4 Select whether to Reset inheritance or Break inheritance, then click Save.

Enforcing policies for a product on a group
Use this task to enable or disable policy enforcement for a product on a System Tree group. Policy enforcement is enabled by default, and is inherited in the System Tree.

Task
For option definitions, click ? in the interface.

1 Click Menu | Systems | System Tree | Assigned Policies, then select the desired group in the System Tree.

2 Select the desired Product, then click the link next to Enforcement Status. The Enforcement page appears.

3 To change the enforcement status you must first select Break inheritance and assign the policy and settings below.

4 Next to Enforcement status, select Enforcing or Not enforcing accordingly.

5 Choose whether to lock policy inheritance. Locking inheritance for policy enforcement prevents breaking enforcement for groups and systems that inherit this policy.

6 Click Save.

Enforcing policies for a product on a system
Use this task to enable or disable policy enforcement for a product on a system. Policy enforcement is enabled by default, and is inherited in the System Tree.

Task
For option definitions, click ? in the interface.

1 Click Menu | Systems | System Tree | Systems, then select the group under System Tree where the system belongs. The list of systems belonging to this group appears in the details pane.

2 Select the desired system, then click Actions | Modify Policies on a Single System. The Policy Assignment page appears.

3 Select the desired Product, then click Enforcing next to Enforcement status. The Enforcement page appears.

4 If you want to change the enforcement status you must first select Break inheritance and assign the policy and settings below.
Next to Enforcement status, select Enforcing or Not enforcing accordingly.

Click Save.

Copying and pasting assignments
Use these tasks to copy and paste policy assignments from one group or system to another. This is an easy way to share multiple assignments between groups and systems from different portions of the System Tree.

Tasks
- **Copying policy assignments from a group on page 179**
  Use this task to copy policy assignments from a group in the System Tree.

- **Copying policy assignments from a system on page 179**
  Use this task to copy policy assignments from a specific system.

- **Pasting policy assignments to a group on page 179**
  Use this task to paste policy assignments to a group. You must have already copied policy assignments from a group or system.

- **Pasting policy assignments to a specific system on page 180**
  Use this task to paste policy assignments to a specific system. You must have already copied policy assignments from a group or system.

Copying policy assignments from a group
Use this task to copy policy assignments from a group in the System Tree.

Task
For option definitions, click ? in the interface.

1. Click Menu | Systems | System Tree | Assigned Policies, then select the desired group in the System Tree.
2. Click Actions | Copy Assignments.
3. Select the products or features for which you want to copy policy assignments, then click OK.

Copying policy assignments from a system
Use this task to copy policy assignments from a specific system.

Task
For option definitions, click ? in the interface.

1. Click Menu | Systems | System Tree | Systems, then select the desired group in the System Tree. The systems belonging to the selected group appear in the details pane.
2. Select the desired system, then click Actions | Agent | Modify Policies on a Single System.
3. Click Actions | Copy Assignments, select the desired products or features for which you want to copy policy assignments, then click OK.

Pasting policy assignments to a group
Use this task to paste policy assignments to a group. You must have already copied policy assignments from a group or system.
**Task**
For option definitions, click ? in the interface.

1. Click **Menu | Systems | System Tree | Assigned Policies**, then select the desired group in the System Tree.

2. In the details pane, click **Actions** and select **Paste Assignments**.
   If the group already has policies assigned for some categories, the Override Policy Assignments page appears.

   When pasting policy assignments, an extra policy appears in the list (Enforce Policies and Tasks). This policy controls the enforcement status of other policies.

3. Select the policy categories you want to replace with the copied policies, then click **OK**.

**Pasting policy assignments to a specific system**
Use this task to paste policy assignments to a specific system. You must have already copied policy assignments from a group or system.

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

1. Click **Menu | Systems | System Tree | Systems**, then select the desired group in the System Tree.
   All of the systems belonging to the selected group appear in the details pane.

2. Select the system where you want to paste policy assignments, then click **Actions | Agent | Modify Policies on a Single System**.

3. In the details pane, click **Actions | Paste Assignment**.
   If the system already has policies assigned for some categories, the Override Policy Assignments page appears.

   When pasting policy assignments, an extra policy appears in the list (Enforce Policies and Tasks). This policy controls the enforcement status of other policies.

4. Confirm the replacement of assignments.

**Viewing policy information**
Use these tasks to view detailed information about the policies, their assignments, inheritance, and their owners.
Tasks

- **Viewing groups and systems where a policy is assigned on page 181**
  Use this task to view the groups and systems where a policy is assigned. This list shows the assignment points only, not each group or system that inherits the policy.

- **Viewing the settings of a policy on page 181**
  Use this task to view the specific settings of a policy.

- **Viewing policy ownership on page 182**
  Use this task to view the owners of a policy.

- **Viewing assignments where policy enforcement is disabled on page 182**
  Use this task to view assignments where policy enforcement, per policy category, is disabled.

- **Viewing policies assigned to a group on page 182**
  Use this task to view the policies assigned to a group.

- **Viewing policies assigned to a specific system on page 183**
  Use this task to view the policies assigned to a specific system.

- **Viewing a group’s policy inheritance on page 183**
  Use this task to view the policy inheritance of a specific group.

- **Viewing and resetting broken inheritance on page 183**
  Use this task to view where policy inheritance is broken.

**Viewing groups and systems where a policy is assigned**
Use this task to view the groups and systems where a policy is assigned. This list shows the assignment points only, not each group or system that inherits the policy.

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

1. Click **Menu | Policy | Policy Catalog**, then select the desired **Product** and **Category**. All created policies for the selected category appear in the details pane.

![Figure 15-1 Policy Catalog page](image)

2. Under **Assignments** on the row of the desired policy, click the link that indicates the number of groups or systems the policy is assigned to (for example, 6 assignments). On the Assignments page, each group or system where the policy is assigned appears with its **Node Name** and **Node Type**.

**Viewing the settings of a policy**
Use this task to view the specific settings of a policy.
**Task**

For option definitions, click ? in the interface.

1. Click Menu | Policy | Policy Catalog, then select the desired Product and Category.
   All created policies for the selected category appear in the details pane.

2. Click next to the desired policy.
   The policy pages and their settings appear.

You can also view this information when accessing the assigned policies of a specific group. To access this information click Menu | Systems | System Tree | Assigned Policies, then click the link for the selected policy in the Policy column.

**Viewing policy ownership**

Use this task to view the owners of a policy.

**Task**

For option definitions, click ? in the interface.

1. Click Menu | Policy | Policy Catalog, then select the desired Product and Category.
   All created policies for the selected category appear in the details pane.

2. The owners of the policy are displayed under Owner.

**Viewing assignments where policy enforcement is disabled**

Use this task to view assignments where policy enforcement, per policy category, is disabled.

**Task**

For option definitions, click ? in the interface.

1. Click Menu | Policy | Policy Catalog, then select the desired Product and Category.
   All created policies for the selected category appear in the details pane.

2. Click the link next to Product enforcement status, which indicates the number of assignments where enforcement is disabled, if any.
   The Enforcement for <policy name> page appears.

3. Click any item in the list to go to its Assigned Policies page.

**Viewing policies assigned to a group**

Use this task to view the policies assigned to a group.

**Task**

For option definitions, click ? in the interface.

1. Click Menu | Systems | System Tree | Assigned Policies, then select a group in the System Tree.
   All assigned policies, organized by product, appear in the details pane.

2. Click any policy to view its settings.
Viewing policies assigned to a specific system
Use this task to view the policies assigned to a specific system.

Task
For option definitions, click ? in the interface.

1 Click Menu | Systems | System Tree | Systems, then select the desired group in the System Tree. All systems belonging to the group appear in the details pane.
2 Select the system, then click Actions | Agent | Modify Policies on a Single System.
3 Select the product. The product’s policies assigned to this system appear.
4 Click any policy to view its settings.

Viewing a group’s policy inheritance
Use this task to view the policy inheritance of a specific group.

For option definitions, click ? in the interface.

Task
1 Click Menu | Systems | System Tree | Assigned Policies. All assigned policies, organized by product, appear in the details pane.
2 The desired policy row, under Inherit from, displays the name of the group from which the policy is inherited.

Viewing and resetting broken inheritance
Use this task to view where policy inheritance is broken.

Task
For option definitions, click ? in the interface.

1 Click Menu | Systems | System Tree | Assigned Policies. All assigned policies, organized by product, appear in the details pane. The desired policy row, under Broken Inheritance, displays the number of groups and systems where this policy’s inheritance is broken.

This is the number of groups or systems where the policy inheritance is broken, not the number of systems that do not inherit the policy. For example, if only one group does not inherit the policy, this is represented by 1 doesn’t inherit, regardless of the number of systems within the group.

2 Click the link indicating the number of child groups or systems that have broken inheritance. The View broken inheritance page displays a list of the names of these groups and systems.
3 To reset the inheritance of any of these, select the checkbox next to the name, then click Actions and select Reset Inheritance.

Sharing policies among McAfee ePO servers
Policy sharing allows the administrator to designate policies that are developed on one server to be transmitted to other servers for implementation. In earlier versions of ePolicy Orchestrator, sharing
was possible only by exporting a policy from the source server and importing it to the target servers one at a time.

The process has been simplified and automated. Now the administrator needs only to:

1. Designate the policy for sharing.
2. Register the servers that will share the policy.
3. Schedule a server task to distribute the shared policy.

**Setting up policy sharing for multiple McAfee ePO servers**

Use these tasks to configure policy sharing for use with multiple McAfee ePO servers. McAfee recommends completing these tasks in the sequence listed here.

If the policy needs to be modified after it has been shared, edit the policy and run the shared policies task again. It might be prudent to inform local administrators of the change.

### Tasks

- **Registering servers for policy sharing on page 184**
  Use this task to register the servers that will share a policy.

- **Designating policies for sharing on page 184**
  Use this task to designate a policy to be shared among multiple McAfee ePO servers.

- **Scheduling server tasks to share policies on page 185**
  Use this task to schedule a server task so that policies are shared among multiple McAfee ePO servers.

### Registering servers for policy sharing

Use this task to register the servers that will share a policy.

For option definitions, click ? in the interface.

**Task**

1. Click **Menu | Configuration | Registered Servers**, then click **New Server**. The Registered Server Builder wizard opens to the Description page.

2. From the **Server type** menu, select **ePO**, specify a name and any notes, then click **Next**. The Details page appears.

3. Specify any details for your server and click **Enable** in the **Policy sharing** field, then click **Save**.

### Designating policies for sharing

Use this task to designate a policy to be shared among multiple McAfee ePO servers.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu | Policy | Policy Catalog**, then click **Product** menu and select the product whose policy you want to share.

2. In the **Actions** column for the policy to be shared, click **Share**.

Beginning with ePolicy Orchestrator 4.6, shared policies are automatically pushed to ePolicy Orchestrator servers with policy sharing enabled. When you click **Share** in step 2, the policy is immediately pushed to all registered ePolicy Orchestrator servers that have policy sharing enabled. Changes to shared policies are similarly pushed.
Scheduling server tasks to share policies
Use this task to schedule a server task so that policies are shared among multiple McAfee ePO servers.

Task
For option definitions, click ? in the interface.

1. Click Menu | Automation | Server Tasks, then click Actions | New Task. The Server Task Builder wizard opens.
2. On the Description page, specify the name of the task and any notes, then click Next. The Actions page appears.
   
   New server tasks are enabled by default. If you do not want this task to be enabled, select Disabled in the Schedule status field.

3. From the Actions drop-down menu, select Share Policies, then click Next. The Schedule page appears.
4. Specify the schedule for this task, then click Next. The Summary page opens.
5. Review the summary details, then click Save.

Frequently asked questions

What is a policy?
A policy is a customized subset of product settings that correspond to a policy category. You can create, modify, or delete as many named policies as needed for each policy category.

What are the McAfee Default and My Default policies?
Upon installation, each policy category contains at least two policies. These are named McAfee Default and My Default. These are the only policies present for first-time installations. The configurations for both, initially, are the same.

The McAfee Default named policies cannot be edited, renamed, or deleted. The My Default policies can be edited, renamed, and deleted.
What happens to the child groups and systems of the group where I assigned a new policy?

All child groups and systems that are set to inherit the specific policy category, inherit the policy applied to a parent group.

How are the groups and systems where a policy is applied affected when the policy is modified in the Policy Catalog?

All groups and systems where a policy is applied receive any modification made to the policy at the next agent-server communication. The policy is then enforced at each policy enforcement interval.

I assigned a new policy, but it’s not being enforced on the managed systems. Why?

New policy assignments are not enforced until the next agent-server communication.

I pasted policy assignments from one group or system (source) to another (target), but the policies assigned to the target location are not the same as the source location. Why not?

When you copy and paste policy assignments, only true assignments are pasted. If the source location was inheriting a policy that you selected to copy, it is the inheritance characteristic that was pasted to the target, so the target then inherits the policy (for that particular policy category) from its parent, which might be a different policy than the one that was inherited onto the source.
Using tasks to manage products and systems

Client and server tasks help automate the process of managing the security software deployed to the systems on your network.

Managing products from a single location is a central feature of your ePolicy Orchestrator software. One of the ways this is accomplished is through creation and scheduling of client and server tasks. Both are scheduled actions that run on your server or managed systems to ensure the most current security content is deployed to your network.

Are you configuring tasks for the first time?
When configuring tasks for the first time:

1. Plan client tasks for the segments of your System Tree.
2. Create and assign client tasks to groups and systems.
3. Create server tasks to keep your repositories up-to-date and automate server maintenance tasks.
4. Schedule tasks to run automatically.

Contents
- Deployment packages for products and updates
- Product and update deployment
- First time product and update deployment overview
- Server tasks and what they do
- Client tasks and what they do
- Confirming that clients are using the latest DAT files
- Evaluating new DATs and engines before distribution

Deployment packages for products and updates

The ePolicy Orchestrator software deployment infrastructure supports deploying products and components, as well as updating both.

Each McAfee product that ePolicy Orchestrator can deploy provides a product deployment package zip file. The zip file contains product installation files, which are compressed in a secure format. ePolicy Orchestrator can deploy these packages to any of your managed systems, once they are checked in to the master repository.

These zip files are used for both detection definition (DAT) and engine update packages.

You can configure product policy settings before or after deployment. McAfee recommends configuring policy settings before deploying the product to network systems. This saves time and ensures that your systems are protected as soon as possible.
These package types can be checked in to the master repository with pull tasks, or manually.

### Supported package types

<table>
<thead>
<tr>
<th>Package type</th>
<th>Description</th>
<th>Origination</th>
</tr>
</thead>
<tbody>
<tr>
<td>SuperDAT (SDAT.exe) files</td>
<td>The SuperDAT files contain both DAT and engine files in one update package. If bandwidth is a concern, McAfee recommends updating DAT and engine files separately.</td>
<td>McAfee website. Download and check SuperDAT files in to the master repository manually.</td>
</tr>
<tr>
<td>Supplemental detection definition (ExtraDAT) files</td>
<td>The ExtraDAT files address one or more specific threats that have appeared since the last DAT file was posted. If the threat has a high severity, distribute the ExtraDAT immediately, rather than wait until that signature is added to the next DAT file. ExtraDAT files are from the McAfee website. You can distribute them through ePolicy Orchestrator. Pull tasks do not retrieve ExtraDAT files.</td>
<td>McAfee website. Download and check supplemental DAT files in to the master repository manually.</td>
</tr>
<tr>
<td>Product deployment and update packages</td>
<td>A product deployment package contains the installation software of a McAfee product.</td>
<td>Product CD or downloaded product zip file. Check product deployment packages in to the master repository manually. For specific locations, see the documentation for that product.</td>
</tr>
<tr>
<td>Agent language packages</td>
<td>An agent language package contains files necessary to display agent information in a local language.</td>
<td>Master repository — Checked in at installation. For future versions of the agent, you must check agent language packages into the master repository manually.</td>
</tr>
</tbody>
</table>

### Package signing and security

All packages created and distributed by McAfee are signed with a key pair using the DSA (Digital Signature Algorithm) signature verification system, and are encrypted using 168-bit 3DES encryption. A key is used to encrypt or decrypt sensitive data.

You are notified when you check in packages that are not signed by McAfee. If you are confident of the content and validity of the package, continue with the check-in process. These packages are secured in the same manner described above, but are signed by ePolicy Orchestrator when they are checked in.

Digital signatures guarantee that packages originated from McAfee or were checked in by you, and that they have not been tampered with or corrupted. The agent only trusts package files signed by ePolicy Orchestrator or McAfee. This protects your network from receiving packages from unsigned or untrusted sources.
Package ordering and dependencies

If one product update is dependent on another, you must check in the update packages to the master repository in the required order. For example, if Patch 2 requires Patch 1, you must check in Patch 1 before Patch 2. Packages cannot be reordered once they are checked in. You must remove them and check them in again, in the proper order. If you check in a package that supersedes an existing package, the existing package is removed automatically.

Product and update deployment

The McAfee ePO repository infrastructure allows you to deploy product and update packages to your managed systems from a central location. Although the same repositories are used, there are differences.

Comparison of product deployment and update packages

<table>
<thead>
<tr>
<th>Product deployment packages</th>
<th>Update packages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Must be manually checked in to the master repository.</td>
<td>DAT and engine update packages can be copied from the source site automatically with a pull task. All other update packages must be checked in to the master repository manually.</td>
</tr>
<tr>
<td>Can be replicated to the distributed repositories and installed automatically on managed systems using a deployment task.</td>
<td>Can be replicated to the distributed repositories and installed automatically on managed systems with global updating.</td>
</tr>
<tr>
<td>If not implementing global updating for product deployment, a deployment task must be configured and scheduled for managed systems to retrieve the package.</td>
<td>If not implementing global updating for product updating, an update client task must be configured and scheduled for managed systems to retrieve the package.</td>
</tr>
</tbody>
</table>

Product deployment and updating process

Follow this high-level process for distributing DAT and engine update packages.

1. Check in the update package to the master repository with a pull task, or manually.

2. Do one of the following:
   - Using global updating — Nothing else is required for systems on the network. You should, however, create and schedule an update task for laptop systems that leave the network.
   - Not using global updating — Use a replication task to copy the contents of the master repository to the distributed repositories, then create and schedule an update task for agents to retrieve and install the update on managed systems.

First time product and update deployment overview

Follow this process to ensure your product and update deployments are completed successfully.

When deploying products for the first time:

1. Configure server tasks for repository pull and repository replication.

2. Check in product and update packages to the master repository using the Software Manager.

Server tasks and what they do

Server tasks are configurable actions that run on your ePolicy Orchestrator server on a schedule. You can leverage server tasks to help automate repetitive server tasks that need to be performed on your server.

McAfee ePO software includes preconfigured server tasks and actions by default. Most of the additional software products you manage with your ePolicy Orchestrator server also add preconfigured server tasks.

Global updating

McAfee recommends using global updating as part of your updating strategy. Global updating automates replication to your distributed repositories and keeping your managed systems up-to-date. Replication and update tasks are not required. Checking contents in to your master repository initiates a global update. The entire process should finish within an hour in most environments.

Additionally, you can specify which packages and updates initiate a global update. However, when you only specify that certain content initiates a global update, ensure that you create a replication task to distribute content that was not selected to initiate a global update.

When using global updating, McAfee recommends scheduling a regular pull task (to update the master repository) at a time when network traffic is minimal. Although global updating is much faster than other methods, it increases network traffic during the update.

Global updating process

Most environments can be updated within an hour using this Global updating process:

1. Contents are checked in to the master repository.
2. The server performs an incremental replication to all distributed repositories.
3. The 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 for updating.
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.

If the agent does not receive the broadcast for any reason, such as when the client computer is turned off, or there are no SuperAgents, at the next ASCI, the minimum catalog version is supplied, which starts the process.

If the agent receives notification from a SuperAgent, the agent is supplied with the list of updated packages. If the agent finds the new catalog version at the next ASCI, it is not supplied with the list of packages to update, and therefore updates all packages available.
**Requirements**

These requirements must be met to implement global updating:

- A SuperAgent must use the same agent-server secure communication (ASSC) key as the agents that receive its wake-up call.

- A SuperAgent is installed on each broadcast segment. Managed systems cannot receive a SuperAgent wake-up call if there is no SuperAgent on the same broadcast segment. Global updating uses the SuperAgent wake-up call to alert agents that new updates are available.

- Distributed repositories are set up and configured throughout your environment. McAfee recommends SuperAgent repositories, but they are not required. Global updating functions with all types of distributed repositories.

- If using SuperAgent repositories, managed systems must be able to “see” the repository from which it updates. Although a SuperAgent is required on each broadcast segment for systems to receive the wake-up call, SuperAgent repositories are not required on each broadcast segment. The managed systems, however, must “see” the SuperAgent repository from which to update.

**Deploying update packages automatically with global updating**

Use this task to enable global updating on the server. Global updating automatically deploys user-specified update packages to managed systems.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu | Configuration | Server Settings**, select **Global Updating**, then click **Edit** at the bottom of the page.

   ![Edit Global Updating page](image)

   **Figure 16-1  Edit Global Updating page**

2. On the Edit Global Updating page next to **Status**, select **Enabled**.

3. Edit the **Randomization interval**, if desired.

   Each client update occurs at a randomly selected time within the randomization interval, which helps distribute network load. The default is 20 minutes.

   For example, if you update 1000 clients using the default randomization interval of 20 minutes, roughly 50 clients update each minute during the interval, lowering the load on your network and on your server. Without the randomization, all 1000 clients would try to update simultaneously.
4 Next to **Package types**, select which packages initiate an update. Global updating initiates an update only if new packages for the components specified here are checked in to the master repository or moved to another branch. Select these components carefully.

- **Signatures and engines** — Select **Host Intrusion Prevention Content**, if needed.

Selecting a package type determines what initiates a global update (not what is updated during the global update process). Agents receive a list of updated packages during the global update process. The agents use this list to install only updates that are needed. For example, agents only update packages that have changed since the last update and not all packages if they have not changed.

5 When finished, click **Save**. Once enabled, global updating initiates an update the next time you check in any of the selected packages or move them to another branch.

Be sure to run a Pull Now task and schedule a recurring Repository Pull server task, when you are ready for the automatic updating to begin.

### Pull tasks

Use pull tasks to update your master repository with DAT and engine update packages from the source site. DAT and engine files must be updated often. McAfee releases new DAT files daily, and engine files less frequently. Deploy these packages to managed systems as soon as possible to protect them against the latest threats.

With this release, you can specify which packages are copied from the source site to the master repository.

ExtraDAT files must be checked in to the master repository manually. They are available from the McAfee website.

A scheduled Repository Pull server task runs automatically and regularly at the times and days you specify. For example, you can schedule a weekly repository pull task at 5:00 a.m. every Thursday.

You can also use the Pull Now task to check updates into the master repository immediately. For example, when McAfee alerts you to a fast-spreading virus and releases a new DAT file to protect against it.

If a pull task fails, you must check the packages in to the master repository manually.

Once you have updated your master repository, you can distribute these updates to your systems automatically with global updating or with replication tasks.

### Considerations when scheduling a pull task

Consider these when scheduling pull tasks:

- **Bandwidth and network usage** — If you are using global updating, as recommended, schedule a pull task to run when bandwidth usage by other resources is low. With global updating, the update files are distributed automatically after the pull task finishes.

- **Frequency of the task** — DAT files are released daily, but you might not want to use your resources daily for updating.

- **Replication and update tasks** — Schedule replication tasks and client update tasks to ensure that the update files are distributed throughout your environment.
Replication tasks

Use replication tasks to copy the contents of the master repository to distributed repositories. Unless you have replicated master repository contents to all your distributed repositories, some systems do not receive them. Ensure that all your distributed repositories are up-to-date.

If you are using global updating for all of your updates, replication tasks might not be necessary for your environment, although they are recommended for redundancy. However, if you are not using global updating for any of your updates, you must schedule a Repository Replication server task or run a Replicate Now task.

Scheduling regular Repository Replication server tasks is the best way to ensure that your distributed repositories are up-to-date. Scheduling daily replication tasks ensures that managed systems stay up-to-date. Using Repository Replication tasks automates replication to your distributed repositories.

Occasionally, you might check in files to your master repository that you want to replicate to distributed repositories immediately, rather than wait for the next scheduled replication. Run a Replicate Now task to update your distributed repositories manually.

Full vs. incremental replication

When creating a replication task, select Incremental replication or Full replication. Incremental replication uses less bandwidth and copies only the new updates in the master repository that are not yet in the distributed repository. Full replication copies the entire contents of the master repository.

McAfee recommends scheduling a daily incremental replication task. Schedule a weekly full replication task if it is possible for files to be deleted from the distributed repository outside of the replication functionality of the ePolicy Orchestrator software.

Repository selection

New distributed repositories are added to the repository list file containing all available distributed repositories. The agent of a managed system updates this file each time it communicates with the McAfee ePO server. The agent performs repository selection each time the agent (McAfee Framework Service) service starts, and when the repository list changes.

Selective replication provides more control over the updating of individual repositories. When scheduling replication tasks, you can choose:

- Specific distributed repositories to which the task applies. Replicating to different distributed repositories at different times lessens the impact on bandwidth resources. These repositories can be specified when you create or edit the replication task.
- Specific files and signatures that are replicated to the distributed repositories. Selecting only those types of files that are necessary to each system that checks in to the distributed repository lessens the impact on bandwidth resources. When you define or edit your distributed repositories, you can choose which packages you want to replicate to the distributed repository.

This functionality is intended for updating only products that are installed on several systems in your environment, like Virus Scan Enterprise. The functionality allows you to distribute these updates only to the distributed repositories these systems use.
How agents select repositories

By default, agents can attempt to update from any repository in the repository list file. The agent can use a network ICMP ping or subnet address compare algorithm to find the distributed repository with the quickest response time. Usually, this is the distributed repository closest to the system on the network.

You can also tightly control which distributed repositories agents use for updating by enabling or disabling distributed repositories in the agent policy settings. McAfee does not recommend disabling repositories in the policy settings. Allowing agents to update from any distributed repository ensures that they receive the updates.

Deploying update packages with pull and replication tasks

Use these tasks to implement a task-based updating strategy once you have created your repository infrastructure. You must rely on these tasks if you are not using global updating in your environment.

Tasks

- Using pull tasks to update the master repository on page 194
  Use either of these tasks to update the contents of the master repository from the McAfee update site or from a user-configured source site.

- Replicating packages from the master repository to distributed repositories on page 196
  Use one of these tasks to replicate contents of the master repository to distributed repositories. You can schedule a Repository Replication server task that occurs regularly, or run a Replicate Now task for immediate replication.

Using pull tasks to update the master repository

Use either of these tasks to update the contents of the master repository from the McAfee update site or from a user-configured source site.

You can schedule pull tasks or run them immediately.

Tasks

- Running a pull task on a schedule on page 194
  Use this task to schedule a recurring pull task that updates the master repository from the source site. Pull tasks now provide the ability to select which packages are copied from the source site.

- Running a Pull Now task on page 195
  Use this task to initiate a pull task that updates the master repository from the source site immediately. With this release, you can select which packages in the source site are copied to the master repository.

Running a pull task on a schedule

Use this task to schedule a recurring pull task that updates the master repository from the source site. Pull tasks now provide the ability to select which packages are copied from the source site.

Task

For option definitions, click ? in the interface.

1. Click Menu | Software | Master Repository, then click Actions | Schedule Pull. The Server Task Builder wizard opens.

2. On the Description page, name and describe the task.
3 Choose whether to enable or disable the task, then click Next.
   The Actions page appears. Disabled tasks can be run manually, but do not run at scheduled times.

4 From the Actions menu, select Repository Pull.

5 Select the source site from which to pull contents into the master repository.

6 Select one of the following branches to receive the packages:
   - Current — Use the packages without testing them first.
   - Evaluation — Used to test the packages in a lab environment first.
   - Previous — Use the previous version to receive the package.

7 Select Move existing packages of the same type to the Previous branch to move the current package versions
   saved in the Current branch to the Previous branch.

8 Select whether to pull:
   - All packages.
   - Selected packages — If you select this option, you must click Select Packages and choose the packages
     to pull from the source site when this task runs.

   ![Available Source Site Packages dialog box](image)

9 Click Next.
   The Schedule page of the wizard appears.

10 Schedule the task as needed, then click Next.
   The Summary page appears.

   The Schedule page provides more flexibility than the scheduling functionality of previous versions. In addition to more granular
   scheduling in all of the schedule types, you can use cron syntax by selecting the Advanced schedule type.

11 Review the summary information, then click Save.

   The scheduled Repository Pull task is added to the task list on the Server Tasks page.

**Running a Pull Now task**

Use this task to initiate a pull task that updates the master repository from the source site immediately. With this release, you can select which packages in the source site are copied to the master repository.
Task
For option definitions, click ? in the interface.

1. Click Menu | Software | Master Repository, then click Actions | Pull Now.
   The Pull Now wizard opens.

2. Select the source site from the list of available repositories.

3. Select one of the following branches to receive the packages:
   - Current — Use the packages without testing them first.
   - Evaluation — Used to test the packages in a lab environment first.
   - Previous — Use the previous version to receive the package.

4. Select Move existing packages of the same type to the Previous branch to move the current package versions saved in the Current branch to the Previous branch.

5. Click Next.
   The Package Selection page appears.

6. Select which packages to copy from the source site, then click Next.
   The Summary page appears.

7. Verify the task details, then click Start Pull to begin the pull task.
   The Server Task Log page appears, where you can monitor the status of the task until it finishes.

Replicating packages from the master repository to distributed repositories
Use one of these tasks to replicate contents of the master repository to distributed repositories. You can schedule a Repository Replication server task that occurs regularly, or run a Replicate Now task for immediate replication.

Tasks
- Running a Repository Replication server task on a schedule on page 196
  Use this task to create a scheduled Repository Replication server task.
- Running a Replicate Now task on page 197
  Use this task to replicate contents from the master repository to distributed repositories immediately.
- Avoiding replication of selected packages on page 89
  If distributed repositories are set up to replicate only selected packages, your newly checked-in package is replicated by default. Depending on your requirements for testing and validating, you might want to avoid replicating some packages to your distributed repositories.

Running a Repository Replication server task on a schedule
Use this task to create a scheduled Repository Replication server task.

For option definitions, click ? in the interface.

Task
1. Click Menu | Software | Distributed Repositories, then click Actions | Schedule Replication.
   The Server Task Builder wizard opens.

2. On the Description page, name and describe the task.
Choose whether to enable or disable the task, then click Next. The Actions page appears. Disabled tasks can be run manually, but do not run at scheduled times.

Select Repository Replication from the drop-down menu.

From the Replication type drop-down menu, select one:

- Incremental — Replicates only the differences between the master and distributed repositories.
- Full — Replicates all contents of the master repository to the distributed repositories.

Next to Replicate to, select All repositories or Selected repositories.

If you select Selected repositories, you must click Select Repositories to choose which distributed repositories receive packages when this task is initiated.

Click Next. The Schedule page of the wizard appears.

Schedule the task as desired, then click Next. The Summary page appears.

The Schedule page provides more flexibility than the scheduling functionality of previous versions. In addition to more granular scheduling in all of the schedule types, you can use cron syntax by selecting the Advanced schedule type.

Review the summary information, then click Save. The scheduled Repository Pull task is added to the task list on the Server Tasks page.

**Running a Replicate Now task**

Use this task to replicate contents from the master repository to distributed repositories immediately.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu | Software | Distributed Repositories**, then click **Actions | Replicate Now**. The Replicate Now wizard opens.

2. On the Repositories page, select which distributed repositories participate in the replication, then click **Next**. If you are not sure which distributed repositories need to be updated, replicate to them all.
3. On the Replication Type, select **Incremental replication** or **Full replication**, then click **Next**.

   If this is the first time you are replicating to a distributed repository, it is a full replication even if you select incremental replication.

4. On the Summary page, review the details then click **Start Replication**.
   The Server Task Log page displays the status of the task until it is complete. Replication time depends on the changes to the master repository and the number of distributed repositories to which you are replicating.

   After the task is complete, you can initiate an immediate client update task so that managed systems in other locations can get updates from the distributed repositories.

### Avoiding replication of selected packages

If distributed repositories are set up to replicate only selected packages, your newly checked-in package is replicated by default. Depending on your requirements for testing and validating, you might want to avoid replicating some packages to your distributed repositories.

Use this task to avoid replicating a newly checked-in package.

For option definitions, click ? in the interface.

#### Task

1. Click **Menu | Software | Distributed Repositories**, then click on the desired repository. The **Distributed Repository Builder** wizard opens.
2. On the **Package Types** page, deselect the package that you want to avoid being replicated.
3. Click **Save**.

### Allowed Cron syntax when scheduling a server task

Cron syntax is made up of six or seven fields, separated by a space. Accepted Cron syntax, by field in descending order, is detailed in the following table. Most Cron syntax is acceptable, but a few cases are not supported. For example, you cannot specify both the Day of Week and Day of Month values.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Allowed Values</th>
<th>Allowed Special Characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seconds</td>
<td>0 - 59</td>
<td>, - * /</td>
</tr>
<tr>
<td>Minutes</td>
<td>0 - 59</td>
<td>, - * /</td>
</tr>
<tr>
<td>Hours</td>
<td>0 - 23</td>
<td>, - * /</td>
</tr>
<tr>
<td>Day of Month</td>
<td>1 - 31</td>
<td>, - * ? / L W C</td>
</tr>
<tr>
<td>Month</td>
<td>1 - 12, or JAN - DEC</td>
<td>, - * /</td>
</tr>
<tr>
<td>Day of Week</td>
<td>1 - 7, or SUN - SAT</td>
<td>, - * ? / L C #</td>
</tr>
<tr>
<td>Year (optional)</td>
<td>Empty, or 1970 - 2099</td>
<td>, - * /</td>
</tr>
</tbody>
</table>

#### Notes on allowed special characters

- Commas (,) are allowed to specify additional values. For example, "5,10,30" or "MON, WED, FRI".
- Asterisks (*) are used for "every." For example, "*" in the minutes field is "every minute".
- Question marks (?) are allowed to specify no specific value in the Day of Week or Day of Month fields.

   The question mark must be used in one of these fields, but cannot be used in both.
• Forward slashes (/) identify increments. For example, "5/15" in the minutes field means the task runs at minutes 5, 20, 35 and 50.

• The letter "L" means "last" in the Day of Week or Day of Month fields. For example, "0 15 10 ? * 6L" means the last Friday of every month at 10:15 am.

• The letter "W" means "weekday". So, if you created a Day of Month as "15W", this means the weekday closest to the 15th of the month. Also, you can specify "LW", which means the last weekday of the month.

• The pound character "#" identifies the "Nth" day of the month. For example, using "6#3" in the Day of Week field is the third Friday of every month, "2#1" is the first Monday, and "4#5" is the fifth Wednesday.

  If the month does not have a fifth Wednesday, the task does not run.

About the pull and replication task information in the Server Task log
The server task log provides information about your pull and replication tasks, in addition to all server tasks. This provides the status of the task and any errors that might have occurred.

Replication task information in the server task log
Click Menu | Automation | Server Task Log to access the following information for replication tasks:

• Start date and task duration
• Status of task at each site (when expanded)
• Any errors or warnings, their codes, and the site to which they apply

Pull task information in the server task log
Click Menu | Automation | Server Task Log to access the following information for pull tasks:

• Start date and task duration
• Any errors or warnings and their codes
• Status of each package that is checked in to the master repository
• Information regarding any new packages that are being checked in to the master repository

Client tasks and what they do

EPolicy Orchestrator allows you to create and schedule client tasks to help automate management of systems in your managed network.

Which extension files are installed on your McAfee ePO server determines which client tasks are available.

Client tasks are commonly used for:

• Product deployment
• Product functionality (for example, the VirusScan Enterprise On-Demand Scan task)
• Upgrades and updates
For information about what client tasks are available, and for details about their functionality, see the product documentation for your managed products.

**How the Client Task Catalog works**

The Client Task Catalog allows you to create client task objects you can use to help manage systems in your network.

Client Tasks Catalog applies the concept of logical objects to ePolicy Orchestrator client tasks. You can create client task objects for a variety of purposes without the need to assign them immediately. As a result, you can treat these objects as reusable components when assigning and scheduling client tasks.

Client tasks can be assigned at any level in the System Tree, and are inherited by groups and systems lower in the tree. As with Policies and policy assignments, you can break the inheritance for an assigned client task.

Client task objects can be shared across multiple registered ePolicy Orchestrator servers in your environment. When client task objects are set to be shared, each registered server receives a copy after your Share Client Task server task runs. Any changes made to the task are updated each time it runs. When a client task object is shared, only the owner of the object can modify its settings.

Share Client Task

Global Administrators on the target server that receives a shared task is not an owner for that shared task. None of the users on the target server is owner for any shared task objects the target receives.

**Deployment tasks**

Once you have checked in the product deployment package, use the Product Deployment client task to install the product on managed systems. The task installs any product that is deployable through the ePolicy Orchestrator software and has been checked in to the master repository.

**Best practices**

You can run the Product Deployment task for any group or individual system. When deciding how to stage your product deployment, McAfee recommends considering the size of the package and the available bandwidth between the master or distributed repositories and the managed systems. In addition to potentially overwhelming the McAfee ePO server or your network, deploying products to many systems can make troubleshooting problems more complicated.

Consider a phased rollout to install products to groups of systems at a time. If your network links are fast, try deploying to several hundred clients at a time. If you have slower or less reliable network connections, try smaller groups. As you deploy to each group, monitor the deployment, run reports to confirm successful installations, and troubleshoot any problems with individual systems.

If you are deploying McAfee products or components that are installed on a subset of your managed systems:

1. Use a tag to identify these systems.
2. Move the tagged systems to a group.
3. Configure a Product Deployment client task for the group.

**Using the Product Deployment task to deploy products to managed systems**

Use these tasks to deploy products to managed systems with the Product Deployment client task.

ePolicy Orchestrator allows you to create this task for a single system, or for groups of the System Tree.
**Tasks**

- **Configuring the Deployment task for groups of managed systems on page 201**
  
  Use this task to configure the Product Deployment task to deploy products to groups of managed systems in the System Tree.

- **Configuring the Deployment task to install products on a managed system on page 202**
  
  Use this task to deploy products to a single system using the Product Deployment task. Create a Product Deployment client task for a single system when that system requires:

**Configuring the Deployment task for groups of managed systems**

Use this task to configure the Product Deployment task to deploy products to groups of managed systems in the System Tree.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu | Policy | Client Task Catalog**, select **McAfee Agent | Product Deployment** as Client Task Types, then click **Actions | New Task**. The New Task dialog box appears.

2. Ensure that **Product Deployment** is selected, then click **OK**.

3. Type a name for the task you are creating and add any notes.

4. Next to **Target platforms**, select the type(s) of platform to use the deployment.

5. Next to **Products and components** set the following:
   - Select the desired product from the first drop-down list. The products listed are those for which you have already checked in a package to the master repository. If you do not see the product you want to deploy listed here, you must first check in that product’s package.
   - Set the **Action** to **Install**, then select the **Language** of the package, and the **Branch**.
   - To specify command-line installation options, type the desired command-line options in the **Command line** text field. See the product documentation for information on command-line options of the product you are installing.

   ![Information](You can click + or – to add or remove products and components from the list displayed.)

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

7. Click **Menu | Systems | System Tree | Assigned Client Tasks**, then select the required group in the System Tree.

8. Select the **Preset** filter as **Product Deployment (McAfee Agent)**.

   Each assigned client task per selected category appears in the details pane.

9. Click **Actions | New Client Task Assignment**. The Client Task Assignment Builder wizard appears.

10. On the Select Task page, select **Product** as **McAfee Agent** and **Task Type** as **Product Deployment**, then select the task you created for deploying product.

11. Next to **Tags**, select the desired platforms to which you are deploying the packages, then click **Next**:
   - **Send this task to all computers**
   - **Send this task to only computers that have the following criteria** — Use one of the edit links to configure the criteria.
12 On the Schedule page, select whether the schedule is enabled, and specify the schedule details, then click Next.

13 Review the summary, then click Save.

Configuring the Deployment task to install products on a managed system

Use this task to deploy products to a single system using the Product Deployment task. Create a Product Deployment client task for a single system when that system requires:

- A product installed that other systems within the same group do not require.
- A different schedule than other systems in the group. For example, if a system is located in a different time zone than its peers.

For option definitions, click ? in the interface.

Task

1 Click Menu | Policy | Client Task Catalog, select McAfee Agent | Product Deployment as Client Task Types, then click Actions | New Task. The New Task dialog box appears.

2 Ensure that Product Deployment is selected, then click OK.

3 Type a name for the task you are creating and add any notes.

4 Next to Target platforms, select the type(s) of platform to use the deployment.

5 Next to Products and components set the following:

   • Select the desired product from the first drop-down list. The products listed are those for which you have already checked in a package to the master repository. If you do not see the product you want to deploy listed here, you must first check in that product’s package.

   • Set the Action to Install, then select the Language of the package, and the Branch.

   • To specify command-line installation options, type the desired command-line options in the Command line text field. See the product documentation for information on command-line options of the product you are installing.

       You can click + or – to add or remove products and components from the list displayed.

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

7 Click Menu | Systems | System Tree | Systems, then select the system on which you want to deploy product and click Actions | Agent | Modify Tasks on a single system.

8 Click Actions | New Client Task Assignment. The Client Task Assignment Builder wizard appears.

9 On the Select Task page, select Product as McAfee Agent and Task Type as Product Deployment, then select the task you created for deploying product.

10 Next to Tags, select the desired platforms to which you are deploying the packages, then click Next:

   • Send this task to all computers

   • Send this task to only computers that have the following criteria — Use one of the edit links to configure the criteria.
11 On the Schedule page, select whether the schedule is enabled, and specify the schedule details, then click Next.

12 Review the summary, then click Save.

**Update tasks**

Once an update package has been checked in to the master repository and replicated to the distributed repositories, the agents on the managed systems still need to know when to go to the distributed repositories for updates. If you are using global updating, this is not necessary.

You can create and configure update client tasks to control when and how managed systems receive update packages. If you are not using global updating, creating these tasks are the only way you can control client updating with the ePolicy Orchestrator software.

If you are using global updating, this task is not necessary, although you can create a daily task for redundancy.

**Considerations when creating update client tasks**

Consider the following when scheduling client update tasks:

- Create a daily Update client task that the highest level of the System Tree that is inherited by all systems. If your organization is large, you can use randomization intervals to mitigate the bandwidth impact. Also, for large networks with offices in different time zones, help balance network load by running the task at the local system time on the managed system, rather than at the same time for all systems.

- Schedule the task at least an hour after the scheduled replication task, if you are using scheduled replication tasks.

- Run update tasks for DAT and engine files at least once a day. Managed systems might be logged off from the network and miss the scheduled task. Running the task frequently ensures these systems receive the update.

- Maximize bandwidth efficiency and create several scheduled client update tasks that update separate components and run at different times. For example, you can create one task to update only DAT files, then create another to update both DAT and engine files weekly or monthly (engine packages are released less frequently).

- Create and schedule additional tasks to update products that do not use the agent for Windows.

- Create a task to update your main workstation applications, such as VirusScan Enterprise, to ensure they all receive the update files. Schedule it to run daily or several times a day.

**Updating managed systems regularly with a scheduled update task**

Use this task to create and configure update tasks. If you are not using global updating, McAfee recommends using a daily Update client task to ensure systems are up-to-date with the latest DAT and engine files.

**Task**

For option definitions, click ? in the interface.

1 Click **Menu | Policy | Client Task Catalog**, select **McAfee Agent | Product Update** as Client Task Types, then click **Actions | New Task**. The New Task dialog box appears.

2 Ensure that **Product Update** is selected, then click **OK**.

3 Type a name for the task you are creating and add any notes.
4. Next to the Update in Progress dialog Box select if you want the users to be aware an update is in process and if you want to allow them to postpone the process.

5. Next to Package types select one of these, then click Save:
   - All packages
   - Selected packages — If selected, you must configure which of the following to include:
     - Signatures and engines
       
       When configuring individual signatures and engines, if you select Engine and deselect DAT when the new engine is updated a new DAT is automatically updated to ensure complete protection.
     - Patches and service packs

6. Click Menu | Systems | System Tree | Systems, then select the system on which you want to deploy product update and click Actions | Agent | Modify Tasks on a single system.

   To deploy product update on a group of systems, refer to Configuring the Deployment task for groups of managed systems.

7. Click Actions | New Client Task Assignment. The Client Task Assignment Builder wizard appears.

8. On the Select Task page, select Product as McAfee Agent and Task Type as Product Deployment, then select the task you created for deploying product update.

9. Next to Tags, select the desired platforms to which you are deploying the packages, then click Next:
   - Send this task to all computers
   - Send this task to only computers that have the following criteria — Use one of the edit links to configure the criteria.

10. On the Schedule page, select whether the schedule is enabled, and specify the schedule details, then click Next.

11. Review the summary, then click Save.

   The task is added to the list of client tasks for the groups and systems to which it is applied. Agents receive the new update task information the next time they communicate with the server. If the task is enabled, the update task runs at the next occurrence of the scheduled day and time. Each system updates from the appropriate repository, depending on how the policies for that client’s agent are configured.

**Working with client tasks**

Use these tasks to create and maintain client tasks.

**Tasks**

- Creating and scheduling client tasks on page 204
  Use this task to create and schedule a client task. The process is similar for all client tasks.
- Editing client tasks on page 205
  Use this task to edit a client task’s settings or to schedule information for any existing task.
- Deleting client tasks on page 205
  Use this task to delete unneeded client tasks. You can delete any client task you have created.

**Creating and scheduling client tasks**

Use this task to create and schedule a client task. The process is similar for all client tasks.
Task
For option definitions, click ? in the interface.

1 Click Menu | Systems | System Tree | Client Tasks, select the desired group in the System Tree, then click Actions | New Task.
   The Client Task Builder wizard opens.

2 Type a name for the task you are creating, add any notes, then select the product task type from the drop-down lists.
   For example, select Product Update.

3 Specify any tags to use with this task and click Next.

4 Configure the settings, then click Next.
   The Schedule page appears.

5 Configure the schedule details as needed, then click Next.

6 Review the task settings, then click Save.
   The task is added to the list of client tasks for the selected group and any group that inherits the task.

Editing client tasks
Use this task to edit a client task's settings or to schedule information for any existing task.

Task
For option definitions, click ? in the interface.

1 Click Menu | Systems | System Tree | Client Tasks, then select the group where the desired client task was created in the System Tree.

2 Click Edit Settings next to the task.
   The Client Task Builder wizard opens.

3 Edit the task settings as needed, then click Save.
   The managed systems receive these changes the next time the agents communicate with the server.

Deleting client tasks
Use this task to delete unneeded client tasks. You can delete any client task you have created.

Task
For option definitions, click ? in the interface.

1 Click Menu | Systems | System Tree | Client Tasks, then select the group where the desired client task was created in the System Tree.

2 Click Delete next to the desired client task.

3 Click OK.

Confirming that clients are using the latest DAT files
Use this task to check the version of DAT files on managed systems.
Evaluating new DATs and engines before distribution

Use this task to test update packages using the Evaluation branch. You might want to test DAT and engine files on a few systems before deploying them to your entire organization.

The ePolicy Orchestrator software provides three repository branches for this purpose.

For option definitions, click ? in the interface.

Task

1. Create a scheduled Repository Pull task that copies update packages in the Evaluation branch of your master repository. Schedule it to run after McAfee releases updated DAT files.
   For additional information, see Deploying update packages with pull and replication tasks.

2. Create or select a group in the System Tree to serve as an evaluation group, and create a McAfee Agent policy for the systems to use only the Evaluation branch (in the Repository Branch Update Selection section of the Updates tab).
   The policies take affect the next time the agent calls in to the server. The next time the agent updates, it retrieves them from the Evaluation branch. For additional information, see Configuring the Deployment task for groups of managed systems.

3. Create a scheduled Update client task for the evaluation systems that updates DAT and engine files from the Evaluation branch of your repository. Schedule it to run one or two hours after your Repository Pull task is scheduled to begin.
   The evaluation update task created at the evaluation group level causes it to run only for that group. For additional information, see Updating managed systems regularly with a scheduled update task.

4. Monitor the systems in your evaluation group until satisfied.

5. Move the packages from the Evaluation branch to the Current branch of your master repository. Click Menu | Software | Master Repository to open the Master Repository page.
   Adding them to the Current branch makes them available to your production environment. The next time any Update client tasks run that retrieves packages from the Current branch, the new DAT and engine files are distributed to systems that use the task. For additional information, see Checking in packages manually.
Managing packages and extensions manually

In addition to using the Software Manager, policies, and task to manage product packages and extensions, you can manage them manually.

Contents
- Bringing products under management
- Checking in packages manually
- Deleting DAT or engine packages from the master repository
- Manually moving DAT and engine packages between branches
- Checking in engine, DAT and ExtraDAT update packages manually

Bringing products under management
Use this task to install an extension (zip) file. A product’s extension must be installed before ePolicy Orchestrator can manage the product.

Task
For option definitions, click ? in the interface.

1. Ensure that the extension file is in an accessible location on the network.

2. Click Menu | Software | Extensions | Install Extension.
   The Install Extension dialog box appears.

3. Browse to and select the desired extension (zip) file, then click OK.

4. Verify that the product name appears in the Extensions list.

Checking in packages manually
Use this task to manually check in the deployment packages to the master repository so that the ePolicy Orchestrator software can deploy them.

For option definitions, click ? in the page interface.

Task
1. Click Menu | Software | Master Repository, then click Actions | Check In Package.
   The Check In Package wizard opens.

2. Select the package type, then browse to and select the desired package file.
3 Click Next.
   The Package Options page appears.

4 Confirm or configure the following:
   - **Package info** — Confirm this is the correct package.
   - **Branch** — Select the desired branch. If there are requirements in your environment to test new packages before deploying them throughout the production environment, McAfee recommends using the Evaluation branch whenever checking in packages. Once you finish testing the packages, you can move them to the Current branch by clicking **Menu | Software | Master Repository**.
   - **Options** — Select whether to:
     - **Move the existing package to the Previous branch** — When selected, moves packages in the master repository from the Current branch to the Previous branch when a newer package of the same type is checked in. Available only when you select Current in Branch.
     - **Package signing** — Specifies if the package is signed by McAfee or is third-party package.

5 Click **Save** to begin checking in the package, then wait while the package is checked in.
   The new package appears in the Packages in Master Repository list on the Master Repository tab.

---

**Deleting DAT or engine packages from the master repository**

Use this task to delete packages from the master repository. As you check in new update packages regularly, they replace the older versions or move them to the Previous branch, if you are using the Previous branch. However, you might want to manually delete DAT or engine packages from the master repository.

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

1 Click **Menu | Software | Master Repository**.
   The Packages in Master Repository table appears.

2 In the row of the desired package, click **Delete**.
   The Delete Package dialog box appears.

3 Click **OK**.

---

**Manually moving DAT and engine packages between branches**

Use this task to move packages manually between the Evaluation, Current, and Previous branches after they are checked in to the master repository.

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

1 Click **Menu | Software | Master Repository**.
   The Packages in Master Repository table appears.

2 In the row of the desired package, click **Change Branch**.
   The Change Branch page appears.
3 Select whether to move or copy the package to another branch.

4 Select which branch receives the package.

   If you have NetShield for NetWare in your network, select Support NetShield for NetWare.

5 Click OK.

---

**Checking in engine, DAT and ExtraDAT update packages manually**

Use this task to manually check in the update packages to the master repository, to deploy them using the ePolicy Orchestrator software. Some packages can only be checked in manually.

For option definitions, click ? in the interface.

**Task**

1 Click **Menu | Software | Master Repository**, then click **Actions | Check In Package**.
   The Check In Package wizard opens.

2 Select the package type, then browse to and select the desired package file.

3 Click **Next**.
   The Package Options page appears.

4 Select a branch:
   - **Current** — Use the packages without testing them first.
   - **Evaluation** — Used to test the packages in a lab environment first.

   Once you finish testing the packages, you can move them to the Current branch by clicking **Menu | Software | Master Repository**.

   - **Previous** — Use the previous version to receive the package.

5 Next to **Options**, select whether to:
   - **Move the existing package to the Previous branch** — Select this option to move the existing package (of the same type that you are checking in) to the Previous branch.

6 Click **Save** to begin checking in the package. Wait while the package is checked in.

The new package appears in the Packages in Master Repository list on the Master Repository page.
Responding to events in your network

Using the ePolicy Orchestrator Automatic response feature, you can configure your server to automatically trigger an action in response to various types of events; including threat, client, and server events.

Are you creating an Automatic Response rule for the first time?

When creating a new automatic response rule for the first time:

1. Understand Automatic Responses and how it works with the System Tree and your network.
2. Plan your implementation. Which users need to know about which events?
3. Prepare the components and permissions used with Automatic Responses, including:
   - Automatic Responses permissions — Create or edit permission sets and ensure that they are assigned to the appropriate McAfee ePO users.
   - Email server — Configure the email (SMTP) server at Server Settings.
   - Email contacts list — Specify the list from which you select recipients of notification messages at Contacts.
   - Registered executables — Specify a list of registered executables to run when the conditions of a rule are met.
   - Rogue System Detection permission — Create or edit permission sets and ensure that they are assigned to the appropriate McAfee ePO users.
   - Server tasks — Create server tasks for use as actions to be carried out as a result of a response rule.
   - SNMP servers — Specify a list of SNMP servers to use while creating rules. You can configure rules to send SNMP traps to SNMP servers when the conditions are met to initiate a notification message.

Contents

- About using Automatic Responses
- Automatic Responses and how it works
- Planning
- Determining how events are forwarded
- Configuring Automatic Responses
- Creating and editing Automatic Response rules
- Frequently asked questions
About using Automatic Responses

The complete set of event types for which you can configure an automatic response depends on the software products you are managing with your ePolicy Orchestrator server.

By default, your response can include these actions:

- Create issues
- Execute server tasks
- Run external commands
- Run system commands
- Send email messages
- Send SNMP traps

The ability to specify the event categories that generate a notification message and the frequencies with which such messages are sent are highly configurable.

This feature is designed to create user-configured notifications and actions when the conditions of a rule are met. These include, but are not limited to:

- Detection of threats by your anti-virus software product. Although many anti-virus software products are supported, events from VirusScan Enterprise include the IP address of the source attacker so that you can isolate the system infecting the rest of your environment.
- Outbreak situations. For example, 1000 virus-detected events are received within five minutes.
- High-level compliance of ePolicy Orchestrator server events. For example, a repository update or a replication task failed.
- Detection of new rogue systems.

Automatic Responses and how it works

Before you plan the implementation of Automatic Responses, you should understand how this feature works with ePolicy Orchestrator and the System Tree.

This feature does not follow the inheritance model used when enforcing policies.

Automatic Responses use events that occur on systems in your environment that are delivered to the server and configured response rules associated with the group that contains the affected systems and each parent above it. If the conditions of any such rule are met, designated actions are taken, per the rule’s configurations.
This design allows you to configure independent rules at different levels of the System Tree. These rules can have different:

- **Thresholds for sending a notification message.** For example, an administrator of a particular group wants to be notified if viruses are detected on 100 systems within 10 minutes on the group, but a global administrator does not want to be notified unless viruses are detected on 1,000 systems within the entire environment in the same amount of time.

- **Recipients for the notification message.** For example, an administrator for a particular group wants to be notified only if a specified number of virus detection events occur within the group. Or, a global administrator wants each group administrator to be notified if a specified number of virus detection events occur within the entire System Tree.

Server events are not filtered by System Tree location.

**Throttling, aggregation, and grouping**

You can configure when notification messages are sent by setting thresholds based on Aggregation, Throttling, or Grouping.

**Aggregation**

Use aggregation to determine the thresholds of events when the rule sends a notification message. For example, configure the same rule to send a notification message when the server receives 1,000 virus detection events from different systems within an hour or whenever it has received 100 virus detection events from any system.

**Throttling**

Once you have configured the rule to notify you of a possible outbreak, use throttling to ensure that you do not receive too many notification messages. If you are administering a large network, you might be receiving tens of thousands of events during an hour, creating thousands of notification messages based on such a rule. Responses allows you to throttle the number of notification messages you receive based on a single rule. For example, you can specify in this same rule that you don’t want to receive more than one notification message in an hour.

**Grouping**

Use grouping to combine multiple aggregated events. For example, events with the same severity can be combined into a single group. Grouping allows an administrator to take actions on all the events with the same and higher severity at once. It also allows you to prioritize the events generated at managed systems or at servers.

**Default rules**

ePolicy Orchestrator provides four default rules that you can enable for immediate use while you learn more about the feature.

Before enabling any of the default rules:

- Specify the email server (click **Menu | Configuration | Server Settings**) from which the notification messages are sent.

- Ensure the recipient email address is the one you want to receive email messages. This address is configured on the Actions page of the wizard.
Default notification rules

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Associated Events</th>
<th>Configurations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed repository update or replication failed</td>
<td>Distributed repository update or replication failed</td>
<td>Sends a notification message when any update or replication fails.</td>
</tr>
<tr>
<td>Malware detected</td>
<td>Any events from any unknown products</td>
<td>Sends a notification message:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When the number of events is at least 1,000 within an hour.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• At most, once every two hours.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• With the source system IP address, actual threat names, and actual product information, if available, and many other parameters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When the number of selected distinct value is 500.</td>
</tr>
<tr>
<td>Master repository update or replication failed</td>
<td>Master repository update or replication failed</td>
<td>Sends a notification message when any update or replication fails.</td>
</tr>
<tr>
<td>Non-compliant computer detected</td>
<td>Non-Compliant Computer Detected events</td>
<td>Sends a notification message when any events are received from the Generate Compliance Event server task.</td>
</tr>
<tr>
<td>RSD: Query New Rogue Detection</td>
<td>New rogue system detected</td>
<td>Queries the newly detected system for a McAfee Agent.</td>
</tr>
</tbody>
</table>

Planning

Before creating rules that send notifications, save time by planning:

- The event type and group (product and server) that trigger notification messages in your environment.

- Who should receive which notification messages. For example, it might not be necessary to notify the administrator of group B about a failed replication in group A, but you might want all administrators to know that an infected file was discovered in group A.

- Which types and levels of thresholds you want to set for each rule. For example, you might not want to receive an email message every time an infected file is detected during an outbreak. Instead, you can choose to have such a message sent at most once every five minutes, regardless of how often that server is receiving the event.

- Which commands or registered executables you want to run when the conditions of a rule are met.

- Which server task you want to run when the conditions of a rule are met.

Determining how events are forwarded

Use these tasks to determine when events are forwarded and which events are forwarded immediately.

The server receives event notifications from McAfee Agents. You can configure agent policies to forward events either immediately to the server or only at agent-to-server communication intervals.
If you choose to send events immediately (as set by default), the agent forwards all events as soon as they are received.

The default interval for processing event notifications is one minute. As a result, there might be a delay before events are processed. You can change the default interval in the Event Notifications server settings (Menu | Configuration | Server).

If you choose not to have all events sent immediately, the agent forwards immediately only events that are designated by the issuing product as high priority. Other events are sent only at the agent-server communication.

Tasks

- **Determining which events are forwarded immediately on page 215**
  Use this task to determine whether events are forwarded immediately or only at the agent-to-server communication interval.

- **Determining which events are forwarded on page 215**
  Use this task to determine which events are forwarded to the server.

**Determining which events are forwarded immediately**

Use this task to determine whether events are forwarded immediately or only at the agent-to-server communication interval.

If the currently applied policy is not set for immediate uploading of events, either edit the currently applied policy or create a new McAfee Agent policy. This setting is configured on the Threat Event Log page.

For option definitions click ? in the interface.

**Task**

1. Click Menu | Policy | Policy Catalog, then select Product as McAfee Agent and Category as General.
2. Click on an existing agent policy.
3. On the Events tab, select **Enable priority event forwarding**.
4. Select the event severity.
   Events of the selected severity (and greater) are forwarded immediately to the server.
5. To regulate traffic, type an **Interval between uploads** (in minutes).
6. To regulate traffic size, type the **Maximum number of events per upload**.
7. Click **Save**.

**Determining which events are forwarded**

Use this task to determine which events are forwarded to the server.

For option definitions click ? in the interface.

**Task**

1. Click Menu | Configuration | Server Settings, select Event Filtering, then click **Edit**.
2. Select the desired events, then click **Save**.

These settings take effect once all agents have called in.
Configuring Automatic Responses

Use these tasks to configure the necessary resources to fully leverage Automatic Responses.

Tasks

- **Assigning permission sets to access Automatic Responses on page 216**
  Use these tasks to assign the appropriate permission sets to access the Automatic Responses feature.

- **Working with SNMP servers on page 217**
  Use these tasks to configure Responses to use your SNMP server. You can configure Responses to send SNMP (Simple Network Management Protocol) traps to your SNMP server, which allows you to receive SNMP traps at the same location where you can use your network management application to view detailed information about the systems in your environment.

- **Working with registered executables and external commands on page 220**
  Use these tasks when working with registered executables and external commands. You can configure automatic response rules to run an external command when the rule is initiated.

Assigning permission sets to access Automatic Responses

Use these tasks to assign the appropriate permission sets to access the Automatic Responses feature.

There are two permission sets specific to the Automatic Responses feature:

- Automatic Responses
- Event Notifications

Users accessing this feature require additional permissions, depending on the specific component used. For example, to create an automatic response that triggers a predefined server task, users need full rights to the Server tasks permission sets. Additional permission sets that might be required include:

- Client Events
- Contacts
- Event Notifications
- Issue Management
- Queries
- Registered servers
- Rogue System Detection
- System Tree (view only)
- System Tree access
- Threat Event log

Tasks

- **Assigning permissions to Notifications on page 216**
  Use this task to ensure that all desired administrators and users have the appropriate permissions to Notifications. The permissions to Notification enables McAfee ePO users to add registered executables.

- **Assigning permissions to Automatic Responses on page 217**
  Use this task to ensure that all desired administrators and users have the appropriate permissions to Responses. The permissions to Responses enables McAfee ePO users to create response rules for different event types and groups.

Assigning permissions to Notifications

Use this task to ensure that all desired administrators and users have the appropriate permissions to Notifications. The permissions to Notification enables McAfee ePO users to add registered executables.

For option definitions click ? in the interface.
Responding to events in your network
Configuring Automatic Responses

Task
1 Click Menu | User Management | Permission Sets, then either create a new permission set or select an existing one.
2 Next to Event Notifications, click Edit.
3 Select the desired Notifications permission:
   • No permissions
   • View registered executables
   • Create and edit registered executables
   • View rules and notifications for entire System Tree (overrides System Tree group access permissions)
4 Click Save.
5 If you created a new permission set, click Menu | User Management | Users.
6 Select a user to assign the new permission set to, then click Edit.
7 Next to Permission sets, select the checkbox for the permission set with the desired Notifications permissions, then click Save.

Assigning permissions to Automatic Responses
Use this task to ensure that all desired administrators and users have the appropriate permissions to Responses. The permissions to Responses enables McAfee ePO users to create response rules for different event types and groups.

For option definitions click ? in the interface.

Task
1 Click Menu | User Management | Permission Sets, then either create a new permission set or select an existing one.
2 Next to Automatic Response, click Edit.
3 Select the desired Automatic Response permission:
   • No permissions
   • View Responses; view Response results in the Server Task Log
   • Create, edit, view, and cancel Responses; view Response results in the Server Task Log
4 Click Save.
5 If you created a new permission set, click Menu | User Management | Users.
6 Select a user to assign the new permission set to, then click Edit.
7 Next to Permission sets, select the checkbox for the permission set with the desired Automatic Response permissions, then click Save.

Working with SNMP servers
Use these tasks to configure Responses to use your SNMP server. You can configure Responses to send SNMP (Simple Network Management Protocol) traps to your SNMP server, which allows you to receive
SNMP traps at the same location where you can use your network management application to view detailed information about the systems in your environment.

You do not need to make other configurations or start any services to configure this feature.

Tasks

- **Editing SNMP servers on page 218**
  Use this task to edit existing SNMP server entries.

- **Deleting an SNMP server on page 219**
  Use this task to delete an SNMP server from Notifications.

- **Importing .MIB files on page 220**
  Use this task when setting up rules to send notification messages to an SNMP server via an SNMP trap.

**Editing SNMP servers**

Use this task to edit existing SNMP server entries.

For option definitions click ? in the interface.
### Task
1. Click Menu | Configuration | Registered Servers.
2. From the list of registered server, select the desired SNMP server, then click Actions | Edit.
3. Edit the following server information as needed, then click Save.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>Type the address of the SNMP server. Valid formats include:</td>
</tr>
<tr>
<td>- DNS Name</td>
<td>Specifies the DNS Name of the server. For example, myhost.mycompany.com</td>
</tr>
<tr>
<td>- IPv4</td>
<td>Specifies the IPv4 address of the server xxx.xxx.xxx.xxx/yy</td>
</tr>
<tr>
<td>- IPv6</td>
<td>Specifies the IPv6 address of the server x:xxxx:xxxx:xxxx:xxxx:xxxx/yyy</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>Specifies the security details of the SNMP server.</td>
</tr>
<tr>
<td>- Community</td>
<td>Specifies the community name of the SNMP protocol.</td>
</tr>
<tr>
<td>- SNMPv3 Security</td>
<td>Specifies the SNMPv3 security details. This field is enabled only if the version of the server is v3.</td>
</tr>
<tr>
<td>- Security Name</td>
<td>Specifies the name of the security settings for the SNMP server.</td>
</tr>
<tr>
<td>- Authentication Protocol</td>
<td>Specifies the protocol used by the SNMP server for verification of the source.</td>
</tr>
<tr>
<td>- Authentication Passphrase</td>
<td>Specifies the password for protocol verification.</td>
</tr>
<tr>
<td>- Confirm Authentication Passphrase</td>
<td>Retype the password for protocol verification.</td>
</tr>
<tr>
<td>- Privacy Protocol</td>
<td>Specifies the protocol used by the SNMP server to customize the privacy defined by the user.</td>
</tr>
</tbody>
</table>

If you select AES 192 or AES 245, you must replace the default policy files with the "unlimited strength" version from Sun’s Java SE Downloads site. Find the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6 download. To apply the unlimited strength policies to the McAfee ePO server, replace the policy jar files in directory EPO_DIR/jre/lib/security with those downloaded in the jce_policyle-6.zip, and restart the McAfee ePO server.

| - Privacy Passphrase | Specifies the password for privacy protocol settings. |
| - Confirm Privacy Passphrase | Retype the password for privacy protocol settings. |

| SNMP Version | Specifies the SNMP version your server uses. |
| Send Test Trap | Tests your configuration. |

### Deleting an SNMP server
Use this task to delete an SNMP server from Notifications.

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

1. Click **Menu | Configuration | Registered Servers**.

2. From the list of registered servers, select the desired SNMP server, then click **Actions | Delete**.

3. When prompted, click **Yes**.

The SNMP server is removed from the Registered Servers list.

**Importing .MIB files**

Use this task when setting up rules to send notification messages to an SNMP server via an SNMP trap.

You must import three .mib files from \Program Files\McAfee\ePolicy Orchestrator\MIB. The files must be imported in the following order:

1. NAI-MIB.mib
2. TVD-MIB.mib
3. EPO-MIB.mib

These files allow your network management program to decode the data in the SNMP traps into meaningful text. The EPO-MIB.mib file depends on the other two files to define the following traps:

- **epoThreatEvent** — This trap is sent when an Automatic Response for an McAfee ePO Threat Event is triggered. It contains variables that match properties of the Threat event.

- **epoStatusEvent** — This trap is sent when an Automatic Response for an McAfee ePO Status Event is triggered. It contains variables that match the properties of a (Server) Status event.

- **epoClientStatusEvent** — This trap is sent when an Automatic Response for an McAfee ePO Client Status Event is triggered. It contains variables that match the properties of the Client Status event.

- **rsdAddDetectedSystemEvent** — This trap is sent when an Automatic Response for a Rogue System Detected event is triggered. It contains variables that match the properties of the Rogue System Detected event.

- **epoTestEvent** — This is a test trap that is sent when you click **Send Test Trap** in the New SNMP Server or Edit SNMP Server pages.

For instructions on importing and implementing .mib files, see the product documentation for your network management program.

**Working with registered executables and external commands**

Use these tasks when working with registered executables and external commands. You can configure automatic response rules to run an external command when the rule is initiated.

**Tasks**

- **Adding registered executables on page 221**
  
  Use this task to add registered executables to your available resources. You can run external command action by providing the registered executables and their arguments.

- **Editing registered executables on page 221**

  Use this task to edit an existing registered executable entry.

- **Deleting registered executables on page 221**

  Use this task to delete a registered executable entry.

- **Duplicating registered executables on page 221**

  Use this task to duplicate a registered executables to your available resources.
Adding registered executables
Use this task to add registered executables to your available resources. You can run external command action by providing the registered executables and their arguments.

Task
For option definitions, click ? in the interface.

1. Click Menu | Configuration | Registered Executables, then click Actions | New RegisteredExecutable. The New Registered Executable page appears.
2. Type a name for the registered executable.
3. Type the path or browse to and select the registered executable that you want a rule to execute when triggered, then click Save.

The new registered executable appears in the Registered Executables list.

Editing registered executables
Use this task to edit an existing registered executable entry.

Task
1. Click Menu | Configuration | Registered Executables, then select edit next to the desired executable in the list. The Edit Registered Executable page appears.
2. Edit the name or select a different executable on the system, then click Save.

Deleting registered executables
Use this task to delete a registered executable entry.

Task
For option definitions, click ? in the interface.

1. Click Menu | Configuration | Registered Executables, then select Delete next to the desired executable in the list.
2. When prompted, click OK.

Duplicating registered executables
Use this task to duplicate a registered executable to your available resources.

Task
For option definitions, click ? in the interface.

1. Click Menu | Configuration | Registered Executables, then click Duplicate next to the desired registered executable.
   The Duplicate Registered Executable dialog box appears.
2. Type a name for the registered executable, then click OK.

The duplicated registered executable appears in the Registered Executables list.
Creating and editing Automatic Response rules

Use these tasks to create and edit Automatic Response rules. These tasks allow you to define when and how a response can be taken on the event occurring either at the server or at a managed system.

Automatic Response rules do not have a dependency order.

Tasks

• Describing the rule on page 222
  Set the filters for the response rule on the Filters page of the Response Builder wizard.

• Setting filters for the rule on page 223
  Set the filters for the response rule on the Filters page of the Response Builder wizard.

• Setting thresholds of the rule on page 223
  Use this task to define when the event triggers the rule on the Aggregation page of the Response Builder wizard.

• Configuring the action for Automatic Response rules on page 224
  Use this task to configure the responses that are triggered by the rule on the Responses page of the Response Builder wizard.

Describing the rule

Use this task to begin creating a rule. The Description page of the Response Builder wizard allows you to:

• Name and describe the rule.
• Specify the language used by the response.
• Specify the event type and group that triggers this response.
• Enable or disable the rule.

For option definitions click ? in the interface.
Task

1. Click **Menu | Automation | Automatic Responses**, then click **Actions | New Response**, or **Edit** next to an existing rule.

   The Response Builder wizard opens.

   ![Figure 18-1 Notifications Rules page](image)

2. On the Description page, type a unique name and any notes for the rule.

   - Rule names on each server must be unique. For example, if one user creates a rule named Emergency Alert, no other user (including global administrators) can create a rule with that name.

3. From the Language menu, select the language the rule uses.

4. Select the **Event group** and **Event type** that trigger this response.

5. Select whether the rule is **Enabled** or **Disabled** next to Status.

6. Click **Next**.

**Setting filters for the rule**

Use this task to set the filters for the response rule on the Filters page of the Response Builder wizard.

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

Task

1. From the Available Properties list, select the desired property and specify the value to filter the response result.

   - Available Properties depend on the event type and event group selected on the Description page of the wizard.

2. Click **Next**.

**Setting thresholds of the rule**

Use this task to define when the event triggers the rule on the Aggregation page of the Response Builder wizard.

A rule’s thresholds are a combination of aggregation, throttling, and grouping.
For option definitions click ? in the interface.

**Task**

1. Next to Aggregation, select whether to **Trigger this response for every event**, or to **Trigger this response if multiple events occur within** a defined amount of time. If you select the latter, define the amount of time in minutes, hours, or days.

2. If you selected **Trigger this response if multiple events occur within**, you can choose to trigger a response when the specified conditions are met. These conditions are any combination of:
   - **When the number of distinct values for an event property is at least a certain value**. This condition is used when a distinct value of occurrence of event property is selected.
   - **When the number of events is at least**. Type a defined number of events.

   ![Information icon]
   You can select one or both options. For example, you can set the rule to trigger this response if the distinct value of occurrence of event property selected exceeds 300, or when the number of events exceeds 3,000, whichever threshold is crossed first.

3. Next to Grouping, select whether to group the aggregated events. If you select to group the aggregated events, specify the property of event on which they are grouped.

4. As needed, next to Throttling, select **At most, trigger this response once every** and define an amount of time that must be passed before this rule can send notification messages again. The amount of time can be defined in minutes, hours, or days.

5. Click **Next**.

**Configuring the action for Automatic Response rules**

Use this task to configure the responses that are triggered by the rule on the Responses page of the Response Builder wizard.

You can configure the rule to trigger multiple actions by using the + and - buttons, located next to the drop-down list for the type of notification.

For option definition click ? in the interface.
Task

1. If you want the notification message to be sent as an email or text pager message, select **Send Email** from the drop-down list.
   a. Next to Recipients, click ... and select the recipients for the message. This list of available recipients is taken from Contacts (Menu | User Management | Contacts). Alternatively, you can manually type email addresses, separated by a comma.
   b. Select the importance of the notification email.
   c. Type the **Subject** of the message. Optionally, you can insert any of the available variables directly into the subject.
   d. Type any text that you want to appear in the **Body** of the message. Optionally, you can insert any of the available variables directly into the body.
   e. Click Next if finished, or click + to add another notification.

2. If you want the notification message to be sent as an SNMP trap, select **Send SNMP Trap** from the drop-down list.
   a. Select the desired SNMP server from the drop-down list.
   b. Select the type of value that you want to send in the SNMP trap.
      - Value
      - Number of Distinct Values
      - List of Distinct Values
      - List of All Values
      ![i] Some events do not include this information. If a selection you made is not represented, the information was not available in the event file.
   c. Click Next if finished, or click + to add another notification.

3. If you want the notification to run an external command, select **Run External Command** from the drop-down list.
   a. Select the desired **Registered Executables** and type any **Arguments** for the command.
   b. Click Next if finished, or click + to add another notification.

4. If you want the notification to create an issue, select **Create issue** from the drop-down list.
   a. Select the type of issue that you want to create.
   b. Type a unique name and any notes for the issue. Optionally, you can insert any of the available variables directly into the name and description.
   c. Select the **State**, **Priority**, **Severity**, and **Resolution** for the issue from the respective drop-down list.
   d. Type the name of the assignee in the text box.
   e. Click Next if finished, or click + to add another notification.
5. If you want the notification to run a scheduled task, select *Execute Server Task* from the drop-down list.
   a. Select the task that you want to run from the *Task to execute* drop-down list.
   b. Click *Next* if finished, or click + to add another notification.
6. On the Summary page, verify the information, then click *Save*.

The new response rule appears in the Responses list.

---

**Frequently asked questions**

These are some frequently asked questions.

*If I set up a response rule for virus detections, do I have to receive a notification message for each event received during an outbreak.*

**No.** You can configure rules so that a notification can be sent only once per specified quantity of events within a specified amount of time, or sent at a maximum of once in a specified amount of time.

*Can I create a rule that generates notifications to multiple recipients?*

**Yes.** You can enter multiple email addresses for recipients in the Response Builder wizard.

*Can I create a rule that generates multiple types of notifications?*

**Yes.** Notifications for ePolicy Orchestrator supports any combination of the following notification targets for each rule:

- Email (including standard SMTP, SMS, and text pager)
- SNMP servers (via SNMP traps)
- Any external tool installed on the ePolicy Orchestrator server
- Issues
- Scheduled server tasks
Monitoring and reporting on your network security status

Use customizable dashboards to monitor critical security status "at-a-glance," and report that status to stakeholders and decision makers using preconfigured, customizable queries and reports.

Chapter 19  Monitoring with Dashboards
Chapter 20  Querying the database and reporting on system status
Chapter 21  Detecting Rogue Systems
Chapter 22  Managing Issues and Tickets
Monitoring with Dashboards

Keeping constant watch on your environment is a difficult task. Dashboards help you do this. Dashboards are collections of monitors. A monitor can be anything from a chart-based query, to a small web application like McAfee Labs Security Threats.

A monitor's behavior and appearance is configured individually.

Users must have the appropriate permissions to use, create, edit, and delete dashboards.

Are you using dashboards for the first time?

When using dashboards for the first time:

1. The ePolicy Orchestrator server has a default dashboard you will see if you have never loaded a dashboard before.

2. Create any needed dashboards and their monitors.

3. The next time ePolicy Orchestrator is started, it will load the last dashboard you used.

Contents

- Working with dashboards
- Working with dashboard monitors
- Default dashboards and their monitors

Working with dashboards

Dashboards can be created, modified, duplicated, exported and more so you can monitor your environment at a glance.

Use these tasks when working with dashboards.
Tasks

- **Creating dashboards on page 230**
  To create a different view on your environment, create a new dashboard.
  
- **Adding monitors to dashboards on page 230**
  Dashboards display information through a collection of monitors to give you a customizable, at-a-glance view of your environment.

- **Removing monitors from dashboards on page 231**
  Remove monitors from dashboards when no longer needed.

- **Duplicating dashboards on page 231**
  Sometimes the easiest way to create a new dashboard is to copy an existing one that’s close to what you want.

- **Deleting dashboards on page 232**
  Dashboards can be deleted when no longer needed.

- **Importing dashboards on page 232**
  A dashboard exported as an XML file can be imported to the same or a different system.

- **Exporting dashboards on page 232**
  Exporting dashboards saves them for later import on the same or a different system.

- **Changing the system default dashboard on page 233**
  Users see a default dashboard if their most recently viewed dashboard is no longer available. Customize the default dashboard to meet your organization’s needs.

- **Assigning permissions to dashboards on page 233**
  Dashboards are only visible to users with proper permission.

Creating dashboards

To create a different view on your environment, create a new dashboard.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu | Reporting | Dashboards**, then click **Dashboard Actions | New**.

2. Type a **Dashboard Name** and select a **Dashboard Visibility** option. Click **OK**.

A new blank dashboard is displayed. You can add monitors to the new dashboard as needed.

Adding monitors to dashboards

Dashboards display information through a collection of monitors to give you a customizable, at-a-glance view of your environment.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu | Reporting | Dashboards** and select a dashboard.

2. Click **Add Monitor**.

   The **Monitor Gallery** appears at the top of the screen.

3. Select a monitor category from the **View** drop-down list.

   The available monitors in that category appear in the gallery.
4 Drag a monitor onto the dashboard. As you move the cursor around the dashboard, the nearest available drop location is highlighted. Drop the monitor into your desired location.

The New Monitor dialog appears.

5 Configure the monitor as needed (each monitor has its own set of configuration options), then click OK.

6 After you have added monitors to this dashboard, click Save Changes to save the newly configured dashboard.

7 When you have completed your changes, click Close.

If you add a Custom URL Viewer monitor that contains Adobe Flash content or ActiveX controls to a dashboard, it is possible the content might obscure ePolicy Orchestrator menus, making portions of the menu inaccessible.

Removing monitors from dashboards
Remove monitors from dashboards when no longer needed.

Before you begin
You must have write permission for the dashboard you are modifying and any monitors you want to modify. If you remove a monitor, you can add it back to a dashboard only if you have read permissions to the monitor.

Task
For option definitions, click ? in the interface.

1 Click Menu | Reporting | Dashboards, then select a dashboard from the Dashboard drop-down list.

2 Choose a monitor to remove and click the arrow in its top-left corner. Select Remove Monitor.

The monitor is removed from the dashboard.

3 When you are finished modifying the dashboard, click Save Changes. To revert the dashboard to its prior state, click Discard Changes.

Duplicating dashboards
Sometimes the easiest way to create a new dashboard is to copy an existing one that's close to what you want.

Task
For option definitions, click ? in the interface.

1 Click Menu | Reporting | Dashboards. Select a dashboard from the Dashboard drop-down list.

2 Click Dashboard Actions | Duplicate.

3 ePolicy Orchestrator names the duplicate by appending " (copy)" to the existing name. If you want to modify this name, do so now and click OK.

The duplicated dashboard will now open.

The duplicate is an exact copy of the original dashboard including all permissions. Only the name is changed.
Deleting dashboards
Dashboards can be deleted when no longer needed.

**Before you begin**
You must have write permission for a dashboard to delete it.

**Task**
For option definitions, click ? in the interface.
1. Click Menu | Reporting | Dashboards, then select the dashboard you wish to delete from the Dashboard drop-down list.
2. Click Dashboard Actions | Delete.
3. Click OK to delete the dashboard.

The dashboard is deleted and you see the system default dashboard. Users who had this dashboard as their last viewed dashboard see the system default dashboard when they next log on.

Importing dashboards
A dashboard exported as an XML file can be imported to the same or a different system.

**Before you begin**
You must have access to a previously exported dashboard contained in an XML file.

**Task**
For option definitions, click ? in the interface.
1. Click Menu | Reporting | Dashboards.
2. Click Dashboard Actions | Import.
   The Import Dashboard dialog box appears.
3. Click Browse and select the XML file containing an exported dashboard. Click Open.
4. Click Save.
   The Import Dashboard confirmation dialog box appears. The name of the dashboard in the file is displayed, as well as how it will be named in the system. By default, this is the name of the dashboard as exported with (imported) appended.
5. Click OK. If you do not wish to import the dashboard, click Close.

The imported dashboard is displayed. Regardless of their permissions at the time they were exported, imported dashboards are given private permissions. You must explicitly set their permissions after import.

Exporting dashboards
Exporting dashboards saves them for later import on the same or a different system.
**Task**
For option definitions, click ? in the interface.

1. Click Menu | Reporting | Dashboards, then select a dashboard from the Dashboard drop-down list.
2. Click Dashboard Actions | Export.
   
   Your browser attempts to download an XML file according to your browser settings.
3. Save the exported XML file to an appropriate location.

**Changing the system default dashboard**
Users see a default dashboard if their most recently viewed dashboard is no longer available. Customize the default dashboard to meet your organization's needs.

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

1. Click Menu | Configuration | Server Settings.
2. Click Dashboards | Edit.
3. Click next to Default dashboard for specific permission sets.
4. From the drop-down lists, choose a permission set and the dashboard to be the default for that permission set.
5. Click and to add additional or remove existing permission set/dashboard mappings.
   
   If a user is assigned multiple permission sets, their default dashboard is the first one added to the mapping list.
6. To select a default dashboard for all other permission sets not explicitly mapped above, choose one from the Default dashboard for all other permission sets drop-down list.
7. Click Save.

**Assigning permissions to dashboards**
Dashboards are only visible to users with proper permission.

Dashboards are assigned permissions identically to queries or reports. They can either be entirely private, entirely public, or shared with one or more permission sets.

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

1. Click Menu | Reporting | Dashboards, then select a dashboard from the Dashboard drop-down list.
2. Click Dashboard Actions | Edit.
3 Select a permission:
   • Do not share this dashboard
   • Share this dashboard with everyone
   • Share this dashboard with the following permission sets
     With this option, you must also choose one or more permission sets.
4 Click OK.

It is possible to create a dashboard with more expansive permissions than one or more queries contained on the dashboard. If you do this, users that have access to the underlying data will see the query when opening the dashboard. Users that do not have access to the underlying data will receive a message telling them they do not have permission for that query. If the query is private to the dashboard creator, only the dashboard creator can modify the query or remove it from the dashboard.

Working with dashboard monitors
You can customize and manipulate dashboard monitors.
Use these tasks when working with dashboard monitors.

Tasks
• Configuring dashboard monitors on page 234
  Monitor behavior is configured on a monitor-by-monitor basis.
• Moving and resizing dashboard monitors on page 235
  Monitors can be moved and resized to efficiently use screen space.

Configuring dashboard monitors
Monitor behavior is configured on a monitor-by-monitor basis.

Before you begin
You must have write permissions for the dashboard you are modifying.

Every monitor type supports different configuration options. For example, a query monitor allows the query, database, and refresh interval to be changed.

Task
For option definitions, click ? in the interface.

1 Click Menu | Reporting | Dashboards. Select a dashboard from the Dashboard drop-down list.
2 Choose a monitor to configure and click the arrow in its top-left corner. Select Edit Monitor. The monitor's configuration dialog appears.
3 When you have completed modifying the monitor's settings, click OK. If you decide to not make changes, click Cancel.
4 If you decide to keep the resulting changes to the dashboard, click Save, otherwise click Discard.
Moving and resizing dashboard monitors

Monitors can be moved and resized to efficiently use screen space.

**Before you begin**

You must have write permissions for the dashboard you are modifying.

You can change the size of many dashboard monitors. If the monitor has small diagonal lines in its bottom-right corner, you can resize it. Monitors are moved and resized through drag-and-drop within the current dashboard.

- **To move a dashboard monitor:**
  a. Drag the monitor by its title bar toward its desired location.
     As you move the cursor, the background outline of the monitor shifts to the closest available location for the monitor.
  b. When the background outline has shifted to the location you want, drop the monitor.
     If you attempt to drop the monitor in an invalid location, it returns to its prior location.

- **To resize a dashboard monitor:**
  a. Drag the resize icon in the bottom-right corner of the monitor toward an appropriate location.
     As you move the cursor, the background outline of the monitor changes shape to reflect the supported size closest to the current cursor location. Monitors might enforce a minimum or maximum size.
  b. When the background outline has changed shape to a size you want, drop the monitor.
     If you attempt to resize the monitor to a shape not supported in the monitor's current location, it returns to its prior size.

- When you have finished modifying the dashboard, click **Save Changes**. To revert to the prior configuration, click **Discard Changes**.

Default dashboards and their monitors

This release of ePolicy Orchestrator ships with several default dashboards, each of which has its own default monitors.

All dashboards, other than the default (typically McAfee ePO Summary) are owned by the Global Administrator who installed ePolicy Orchestrator. The Global Administrator who performed the installation must change the permissions on additional dashboards before other McAfee ePO users can view them.

Audit dashboard

The Audit dashboard provides an overview of access-related activities occurring on your McAfee ePO server. The monitors included in this dashboard are:

- **Failed Login Attempts in Last 30 Days** — Displays a list, grouped by user, of all failed logon attempts in the last 30 days.

- **Successful Login Attempts in Last 30 Days** — Displays a list, grouped by user, of all successful logon attempts in the last 30 days.

- **Policy Assignment Change History by User** — Displays a report, grouped by user, of all policy assignments in the last 30 days, as recorded in the Audit log.
Configuration Changes by User — Displays a report, grouped by user, of all actions considered sensitive in the last 30 days, as recorded in the Audit log.

Server Configuration by User — Displays a report, grouped by user, of all server configuration actions in the last 30 days, as recorded in the Audit log.

Quick System Search — You can search for systems by system name, IP address, MAC address, user name, or agent GUID.

McAfee ePO Summary dashboard
The McAfee ePO Summary dashboard is a set of monitors providing high-level information and links to more information from McAfee. The monitors included in this dashboard are:

McAfee Labs Threat Advisory — Displays the protection available, any new threats reported, latest DAT and engine available and, if they are in My Repository, a link to the McAfee Labs Security Threats page and the time last checked.

Systems per Top-Level Group — Displays a bar chart of your managed systems, organized by top-level System Tree group.

Quick System Search — You can search for systems by system name, IP address, MAC address, user name, or agent GUID.

McAfee Links — Displays links to McAfee technical support, escalation tools, virus information library, and more.

McAfee Agent and VirusScan Enterprise (for Windows) Compliance Summary — Displays a Boolean pie chart of managed systems in your environment, which are compliant or noncompliant, by version of VirusScan Enterprise (for Windows), McAfee Agent, and DAT files.

Malware Detection History — Displays a line chart of the number of internal virus detections over the past quarter.

Executive dashboard
The Executive dashboard provides a set of monitors providing some high-level reports on security threats and compliance, with links to more specific product- and McAfee-specific information. The monitors included in this dashboard are:

McAfee Labs Threat Advisory — Displays the protection available, any new threats reported, latest DAT and engine available and, if they are in My Repository, a link to the McAfee Labs Security Threats page and the time last checked.

Malware Detection History — Displays a line chart of the number of internal virus detections over the past quarter.

Product Deployment in the Last 24 Hours — Displays a Boolean pie chart of all product deployments in the last 24 hours. Successful deployments are shown in green.

Product Updates in the Last 24 Hours — Displays a Boolean pie chart off all product updates in the last 24 hours. Successful updates are shown in green.

Product Deployment dashboard
The Product Deployment dashboard provides an overview of product deployment and update activities in your network. The monitors included in this dashboard are:
• **Product Deployment in the Last 24 Hours** — Displays a Boolean pie chart of all product deployments in the last 24 hours. Successful deployments are shown in green.

• **Product Updates in the Last 24 Hours** — Displays a Boolean pie chart of all product updates in the last 24 hours. Successful updates are shown in green.

• **Failed Product Deployment in the Last 24 Hours** — Displays a single group bar chart, grouped by product code, of all the failed product deployments in the last 24 hours.

• **Quick System Search** — You can search for systems by system name, IP address, MAC address, user name, or agent GUID.

• **Failed Product Updates in the Last 24 Hours** — Displays a single group bar chart, grouped by product code, of all failed product updates in the last 24 hours.

• **Agent Uninstalls Attempted in the Last 7 days** — Displays a single bar chart, grouped by day, of all agent uninstall client events in the last seven days.

**RSD Summary dashboard**

The **Rogue System Detection (RSD) Summary** dashboard provides a summary of the state of detected systems on your network. The monitors included in this dashboard are:

• **Rogue Systems, by Domain** — Rogue system interfaces detected by Rogue System Sensors in the last week, grouped by domain.

• **Active Sensor Responses** — Displays a Boolean pie chart of active Rogue System Sensors that have or haven't communicated with the McAfee ePO server in the last 24 hours.

• **Subnet Coverage** — Subnets that are or aren't covered by Rogue System Sensors.

• **Rogue Systems, By OS** — Rogue system interfaces detected by Rogue System Sensors over the last week, grouped by operating system.

• **Passive Sensor Response** — Passive Rogue System Sensors that have or haven't communicated with the McAfee ePO server in the last 24 hours.

• **Rogue Systems, By OUI** — Rogue system interfaces detected by Rogue System Sensors over the last week, grouped by OUI (Organizationally Unique Identifier) in the last week.
Querying the database and reporting on system status

ePolicy Orchestrator ships with its own querying and reporting capabilities. These are highly customizable, flexible and easy to use.

Included are the **Query Builder** and **Report Builder** which create and run queries and reports that result in user-configured data in user-configured charts and tables. The data for these queries and reports can be obtained from any registered internal or external database in your ePolicy Orchestrator system.

In addition to the querying and reporting systems, you can use the following logs to gather information about activities that occur on your McAfee ePO server and throughout your network:

- Audit log
- Server Task log
- Threat Event log

To get you started, McAfee includes a set of default queries that provide the same information as the default reports of previous versions.

**Are you setting up queries and reports for the first time?**

When setting up queries and reports for the first time:

1. Understand the functionality of queries, reports, and the **Query Builder**.
2. Review the default queries and reports, and edit any to your needs.
3. Create queries and reports for any needs that aren’t met by the default queries.

**Contents**
- Query and report permissions
- About queries
- Working with queries
- Multi-server rollup querying
- About reports
- Working with reports
- Using database servers
- Working with database servers
Query and report permissions

You can choose a number of ways to restrict access to queries and reports. To run a query or report, you need permissions to not only that query or report, but the feature sets associated with their result types. A query’s results pages will only provide access to permitted actions given your permission sets.

Groups and permission sets control access to queries and reports. All queries and reports must belong to a group, and access to that query or report is controlled by the permission level of the group. Query and report groups have one of the following permission levels:

- **Private** — the group is only available to the user that created it.
- **Public** — the group is shared globally.
- **By permission set** — the group is only available to users assigned the selected permission sets.

Permission sets have four levels of access to queries or reports. These permissions include:

- **No permissions** — The Query or Report tab is not available to users with no permissions.
- **Use public queries** — Grants permission to use any queries or reports that have been placed in a Public group.
- **Use public queries; create and edit personal queries** — Grants permission to use any queries or reports that have been placed in a Public group, as well as the ability to use the Query Builder to create and edit queries or reports in Private groups.
- **Edit public queries; create and edit personal queries; make personal queries public** — Grants permission to use and edit any queries or reports placed in Public groups, create and edit queries or reports in Private groups, as well as the ability to move queries or reports from Private groups to Public or Shared groups.

About queries

Queries are essentially questions you ask ePolicy Orchestrator and answers are returned in various forms of charts and tables. A query can be used individually to get an answer right now. Any query’s results can be exported to a variety of formats, any of which can be downloaded or sent as an attachment to an email message. Most queries can also be used as dashboard monitors, enabling near real-time system monitoring. Queries can also be combined into reports, giving a more broad and systematic look at your ePolicy Orchestrator software system.
Query results are actionable

Query results are now actionable. Query results displayed in tables (and drill-down tables) have a variety of actions available for selected items in the table. For example, you can deploy agents to systems in a table of query results. Actions are available at the bottom of the results page.

Queries as dashboard monitors

Most queries can be used as a dashboard monitor (except those using a table to display the initial results). Dashboard monitors are refreshed automatically on a user-configured interval (five minutes by default).

Exported results

Query results can be exported to four different formats. Exported results are historical data and are not refreshed like other monitors when used as dashboard monitors. Like query results and query-based monitors displayed in the console, you can drill down into the HTML exports for more detailed information.

Unlike query results in the console, data in exported reports is not actionable.

Reports are available in several formats:

- CSV — Use the data in a spreadsheet application (for example, Microsoft Excel).
- XML — Transform the data for other purposes.
- HTML — View the exported results as a web page.
- PDF — Print the results.
Combining queries in reports
Reports can contain any number of queries, images, static text, and other items. They can be run on-demand or on a regular schedule, and produce PDF output for viewing outside ePolicy Orchestrator.

Sharing queries between servers
Any query can be imported and exported, allowing you to share queries between servers. In a multi-server environment, any query needs to be created only once.

Retrieving data from different sources
Queries can retrieve data from any registered server, including databases external to ePolicy Orchestrator.

Query Builder
ePolicy Orchestrator provides an easy, four-step wizard that is used to create and edit custom queries. With the wizard you can configure which data is retrieved and displayed, and how it is displayed.

Result types
The first selections you make in the Query Builder wizard are the Schema and result type from a feature group. This selection identifies from where and what type of data the query retrieves, and determines the available selections in the rest of the wizard.

Chart types
ePolicy Orchestrator provides a number of charts and tables to display the data it retrieves. These and their drill-down tables are highly configurable.

<table>
<thead>
<tr>
<th>Type</th>
<th>Chart or Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bar</td>
<td>• Bar Chart</td>
</tr>
<tr>
<td></td>
<td>• Grouped Bar Chart</td>
</tr>
<tr>
<td></td>
<td>• Stacked Bar Chart</td>
</tr>
<tr>
<td>Pie</td>
<td>• Boolean Pie Chart</td>
</tr>
<tr>
<td></td>
<td>• Pie Chart</td>
</tr>
<tr>
<td>Bubble</td>
<td>• Bubble Chart</td>
</tr>
<tr>
<td>Summary</td>
<td>• Multi-group Summary Table</td>
</tr>
<tr>
<td></td>
<td>• Single Group Summary Table</td>
</tr>
<tr>
<td>Line</td>
<td>• Multi-line Chart</td>
</tr>
<tr>
<td></td>
<td>• Single Line Chart</td>
</tr>
<tr>
<td>List</td>
<td>• Table</td>
</tr>
</tbody>
</table>

Tables do not include drill-down tables.

Chart types include:

Table 20-1 Chart Type Groups
Table columns
Specify columns for the table. If you select Table as the primary display of the data, this configures that table. If you select a type of chart as the primary display of data, this configures the drill-down table.

Query results displayed in a table are actionable. For example, if the table is populated with systems, you can deploy or wake up agents on those systems directly from the table.

Filters
Specify criteria by selecting properties and operators to limit the data retrieved by the query.

Working with queries
Queries can be created, run, exported, duplicated, and more depending on your needs.

Tasks
• Creating custom queries on page 243
  You create new queries with the Query Builder. Queries can access system properties, product properties, many of the log files, repositories, and more.
• Running an existing query on page 244
  You can run saved queries on-demand.
• Running a query on a schedule on page 245
  A server task is used to run a query on a regular basis.
• Creating a query group on page 245
  Query groups allow you to save queries or reports without allowing other users access to them.
• Moving a query to a different group on page 246
  You can change the permissions on a query by moving it to a different group.
• Duplicating queries on page 246
  Sometimes, the fastest way to create a query is to modify one that already exists.
• Deleting queries on page 246
  Queries can be deleted when they are no longer needed.
• Exporting a query on page 247
  Queries can be exported to ensure different servers are retrieving data in identical ways.
• Importing a query on page 247
  Importing a query exported from another ePolicy Orchestrator server provides a uniform way of retrieving data from all your servers.
• Exporting query results to other formats on page 248
  Query results can be exported to a variety of formats including HTML, PDF, CSV, and XML.

Creating custom queries
You create new queries with the Query Builder. Queries can access system properties, product properties, many of the log files, repositories, and more.
**Task**

For option definitions, click ? in the interface.

1. Click *Menu | Reporting | Queries & Reports*, then click *Actions | New*.

2. On the *Result Type* page, select the *Feature Group* and *Result Type* for this query, then click *Next*.

   This choice determines the options available on subsequent pages.

3. Select the type of chart or table to display the primary results of the query, then click *Next*.

   If you select *Boolean Pie Chart*, you must configure the criteria to include in
   the query before proceeding.

4. Select the columns to be included in the query, then click *Next*.

   If you selected *Table* on the Chart page, the columns you select here are
   the columns of that table. Otherwise, these are the columns that make
   up the query details table.

5. Select properties to narrow the search results, then click *Run*. The *Unsaved Query* page displays the
   results of the query, which is actionable, so you can take any available actions on items in any
   tables or drill-down tables.

   Selected properties appear in the content pane with operators that can
   specify criteria used to narrow the data that is returned for that property.

   • If the query didn't appear to return the expected results, click *Edit Query* to go back to the *Query
     Builder* and edit the details of this query.

   • If you don't need to save the query, click *Close*.

   • If this is a query you want to use again, click *Save* and continue to the next step.

6. The *Save Query* page appears. Type a name for the query, add any notes, and select one of the following:

   • *New Group* — Type the new group name and select either:

     • *Private group (My Groups)*

     • *Public group (Shared Groups)*

   • *Existing Group* — Select the group from the list of *Shared Groups*.

7. Click *Save*.

**Running an existing query**

You can run saved queries on-demand.
Task
For option definitions, click ? in the interface.

1 Click Menu | Reporting | Queries & Reports, then select a query from the Queries list.

2 Click Actions | Run. The query results appear. Drill down into the report and take actions on items as necessary.
   Available actions depend on the permissions of the user.

3 Click Close when finished.

Running a query on a schedule
A server task is used to run a query on a regular basis.
For option definitions, click ? in the interface.

Task
1 Click Menu | Automation | Server Tasks, then click Actions | New Task.

2 On the Description page, name and describe the task, then click Next.

3 From the Actions drop-down menu, select Run Query.

4 In the Query field, browse to the query you want to run.

5 Select the language in which to display the results.

6 From the Sub-Actions list, select an action to take based on the results. Available actions depend on
   the permissions of the user, and the products managed by your ePolicy Orchestrator server.
   You are not limited to selecting one action for the query results. Click the + button to add additional actions to take on the query results. Be careful
   to place the actions in the order you want them to be taken on the query results.

7 Click Next.

8 Schedule the task as desired, then click Next.

9 Verify the configuration of the task, then click Save.

The task is added to the list on the Server Tasks page. If the task is enabled (which it is by default), it
runs at the next scheduled time. If the task is disabled, it only runs by clicking Run next to the task on
the Server Tasks page.

Creating a query group
Query groups allow you to save queries or reports without allowing other users access to them.
Creating a group allows you to categorize queries and reports by functionality as well as controlling
access. The list of groups you see within the ePolicy Orchestrator software is the combination of
groups you have created and groups you have permission to see.

You can also create private query groups while saving a custom query.
**Task**

For option definitions, click ? in the interface.

1. Click **Menu | Reporting | Queries & Reports**, then click **Group Actions | New Group**.
2. In the **New Group** page, type a group name.
3. From **Group Visibility**, select one of the following:
   - **Private group** — Adds the new group under **My Groups**.
   - **Public group** — Adds the new group under **Shared Groups**. Queries and reports in the group can be seen by any user with access to public queries and reports.
   - **Shared by permission set** — Adds the new group under **Shared Groups**. Only users assigned the selected permission sets will be able to access reports or queries in this group.

```
   Global Administrators have full access to all **By permission set** and **Public** queries.
```
4. Click **Save**.

**Moving a query to a different group**

You can change the permissions on a query by moving it to a different group.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu | Reporting | Queries & Reports**. In the **Queries** list, select the query you want to move.
2. Click **Actions** and select one of the following:
   - **Move to Different Group** — Select the desired group from the **Select target group** menu.
   - **Duplicate** — Specify a new name and select the desired group from the **Group to receive copy** menu.
3. Click **OK**.

**Duplicating queries**

Sometimes, the fastest way to create a query is to modify one that already exists.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu | Reporting | Queries & Reports**. From the list, select a query to duplicate and click **Actions | Duplicate**.
2. Type a name for the duplicate and select a group to receive a copy of the query, then click **OK**.

**Deleting queries**

Queries can be deleted when they are no longer needed.
Task
For option definitions, click ? in the interface.

1. Click **Menu | Reporting | Queries & Reports**.

2. From the list, select a query to delete and click **Actions | Delete**. When the confirmation dialog box appears, click **Yes**.

The query no longer appears. If any reports or server tasks used the query, they now appear as invalid until you remove the reference to the deleted query.

**Exporting a query**
Queries can be exported to ensure different servers are retrieving data in identical ways.

Only one query can be exported at a time. If you try to export multiple queries simultaneously, ePolicy Orchestrator instead runs the queries and exports the resulting data based on parameters you provide.

Task
For option definitions, click ? in the interface.

1. Open the Queries page by selecting **Menu | Reporting | Queries & Reports**, then select the **Query** tab.

2. Select the group that contains the query you want to export from the **Groups** list, then select the query you want to export.

3. Click **Actions | Export Definitions**.

   The McAfee ePO server sends an XML file to your browser. What happens next depends on your browser settings. By default, most browsers ask you to save the file.

   The exported XML file contains a complete description of all settings required to replicate the exported query.

**Importing a query**
Importing a query exported from another ePolicy Orchestrator server provides a uniform way of retrieving data from all your servers.

Task
For option definitions, click ? in the interface.

1. Open the **Queries** page by selecting **Menu | Reporting | Queries & Reports**, then select the **Query** tab.

2. Click **Actions | Import Definitions**.

   3. Click **Browse** to navigate to and select the XML file containing the dashboard you want to import.

   4. Select a new or existing group for the query. If a new group, give the name of the group and select whether it is private or public. If an existing group, select the group the imported query will join.

   5. Click **Save**.

      A confirmation screen appears displaying the information about the query as it exists in the XML file and how it will be named after import. If there is no valid query in the selected file, an error message is displayed.

   6. Click **OK** to finalize the import.

The newly imported query acquires the permissions of the group where it was imported.
Exporting query results to other formats

Query results can be exported to a variety of formats including HTML, PDF, CSV, and XML.

Exporting query results differs from creating a report in a couple ways. First, there is no additional information added to the output as you can do within a report; only the resulting data is included. Also, more formats are supported. It is expected that exported query results could be used in further processing, so machine-friendly formats such as XML and CSV are supported. Reports are designed to be human readable, and as such are only output as PDF files.

Unlike query results in the console, exported data is not actionable.

Task

For option definitions, click ? in the interface.

1 Click Menu | Reporting | Queries & Reports then select one or more queries.

   You can also, run the query from the Queries page and click Options | Export Data from the query results page to access the Export page.

2 Click Actions | Export Data.

   The Export page appears.

3 Select what to export. For chart-based queries, select either Chart data only or Chart data and drill-down tables.

4 Select whether the data files are exported individually or in a single archive (zip) file.

5 Select the format of the exported file.
   - CSV — Use this format to use the data in a spreadsheet application (for example, Microsoft Excel).
   - XML — Use this format to transform the data for other purposes.
   - HTML — Use this report format to view the exported results as a web page.
   - PDF — Use this report format when you need to print the results.

6 If exporting to a PDF file, configure the following:
   - Select the Page size and Page orientation.
   - (Optional) Show filter criteria.
   - (Optional) Include a cover page with these text and include the needed text.

7 Select whether the files are emailed as attachments to selected recipients, or they are saved to a location on the server to which a link is provided. You can open or save the file to another location by right-clicking it.

   When typing multiple email addresses for recipients, you must separate entries with a comma or semicolon.

8 Click Export.

   The files are created and either emailed as attachments to the recipients, or you are taken to a page where you can access the files from links.
Multi-server rollup querying

ePolicy Orchestrator includes the ability to run queries that report on summary data from multiple databases.

Use these result types in the Query Builder wizard for this type of querying:

- Rolled-Up Threat Events
- Rolled-Up Client Events
- Rolled-Up Compliance History
- Rolled-Up Managed Systems
- Rolled-Up Applied Policies

Action commands cannot be generated from rollup result types.

How it works

To roll up data for use by rollup queries, you must register each server (including the local server) that you want to include in the query.

Once the servers are registered, you must configure Roll Up Data server tasks on the reporting server (the server that performs the multi-server reporting). Roll Up Data server tasks retrieve the information from all databases involved in the reporting, and populate the EPORollup_ tables on the reporting server. The rollup queries target these database tables on the reporting server.

As a prerequisite to running a Rolled-Up Compliance History query, you must take two preparatory actions on each server whose data you want to include:

- Creating a query to define compliance
- Generating a compliance event

Creating a Rollup Data server task

Rollup Data server tasks draw data from multiple servers simultaneously.

Before you begin

You must first register each ePolicy Orchestrator reporting server you want to include in rollup reporting. Registering each servers is required to collect summary data from those servers to populate the EPORollup_ tables of the rollup reporting server.

The reporting server must also be registered if its summary data is to be included in rollup reporting.

Task

For option definitions, click ? in the interface.

1. Click **Menu** | **Automation** | **Server Tasks**, then click **Actions** | **New Task**.

2. On the **Description** page, type a name and description for the task, and select whether to enable it, then click **Next**.

3. Click **Actions** and select **Roll Up Data**.
4 From the Roll up data from: drop-down menu, select All registered servers or Select registered servers.

5 If you chose Select registered servers in the prior step, click Select and choose the servers from which you want data in the Select Registered Servers dialog box. Click OK.

6 Select the data type to be rolled up. To select multiple data types, click the + at the end of the table heading.

   ![Info](image)

   The data types Threat Events, Client Events, and Applied Policies can be further configured to include the additional properties Purge, Filter and Rollup Method. To do so, click Configure in the row that describes the additional properties available.

7 Click Next. The Schedule page appears.

8 Schedule the task, then click Next. The Summary page appears.

   ![Info](image)

   If you are reporting on rolled-up compliance history data, ensure that the time unit of the Rolled-Up Compliance History query matches the schedule type of the Generate Compliance Event server tasks on the registered servers.

9 Review the settings, then click Save.

**Creating a query to define compliance**

Compliance queries are required on McAfee ePO servers whose data is used in rollup queries.

**Task**

For option definitions, click ? in the interface.

1 Click Menu | Reporting | Queries & Reports, then click Actions | New.

2 On the Result Type page, select System Management as Feature Group, and select Managed Systems as Result Types, then click Next.

3 Select Boolean Pie Chart from the Display Result As list, then click Configure Criteria.

4 Select the properties to include in the query, then set the operators and values for each property. Click OK. When the Chart page appears, click Next.

   ![Info](image)

   These properties define what is compliant for systems managed by this McAfee ePO server.

5 Select the columns to be included in the query, then click Next.

6 Select any filters to be applied to the query, click Run, then click Save.

**Generating compliance events**

Compliance events are used in rollup queries to aggregate data in a single report.
**Task**

For option definitions, click ? in the interface.

1. Click **Menu | Automation | Server Tasks**, then click **Actions | New Task**.
2. On the Description page, type a name for the new task, then click **Next**.
3. From the **Actions** drop-down menu, select **Run Query**.
4. Click browse (…) next to the Query field and select a query. The Select a query from the list dialog box appears with the My Groups tab active.
5. Select the compliance-defining query. This could be a default query, such as McAfee Agent Compliance Summary in the Shared Groups section, or a user-created query, such as one described in Creating a query to define compliance.
6. From the **Sub-Actions** drop-down menu, select **Generate Compliance Event** and specify the percentage or number of target systems, then click **Next**.

   **Events can be generated by the generate compliance event task if noncompliance rises above a set percentage or set number of systems.**

7. Schedule the task for the time interval needed for Compliance History reporting. For example, if compliance must be collected on a weekly basis, schedule the task to run weekly. Click **Next**.
8. Review the details, then click **Save**.

---

**About reports**

Reports combine queries and other elements into PDF documents, providing detailed information for analysis.

You run reports to find out the state of your environment — vulnerabilities, usage, events, etc. — so you can make the changes necessary to keep your environment secure.

Queries provide similar information, but can only be used when you are directly interacting with an ePolicy Orchestrator server. Reports allow you to package together one or more queries into a single PDF document, enabling focused, offline analysis.

Reports are configurable documents that display data from one or more databases. The most recently run result for every report is stored within the system and is readily available for viewing.

You can restrict access to reports through the use of groups and permission sets in exactly the same manner you restrict access to queries. Reports and queries can use the same groups, and because reports primarily consist of queries, this allows for consistent access control.

**Structure of a report**

Reports contain a number of elements held within a basic format.

While reports are highly customizable, they have a basic structure that contains all of the varying elements.
**Page size and orientation**
ePolicy Orchestrator currently supports six combinations of page size and orientation. These include:

**Page sizes:**
- US Letter (8.5" x 11")
- US Legal (8.5" x 14")
- A4 (210mm x 297mm)

**Orientation:**
- Landscape
- Portrait

**Headers and footers**
Headers and footers also have the option of using a system default, or can be customized in a number of ways, including logos. Elements currently supported for headers and footers are:

- Logo
- Date/Time
- Page Number
- User Name
- Custom text

**Page elements**
Page elements provide the content of the report. They can be combined in any order, and may be duplicated as needed. Page elements provided with ePolicy Orchestrator are:

- Images
- Static text
- Page breaks
- Query Tables
- Query Charts

---

**Working with reports**
These tasks create, edit, and manage reports.

Reports can provide a large amount of useful data, but there are many tasks to complete to create a collection of reports that is useful to you.
Tasks

- **Creating a new report on page 253**
  You can create new reports and store them in ePolicy Orchestrator.

- **Editing an existing report on page 253**
  You can modify an existing report’s contents or the order of presentation.

- **Viewing report output on page 258**
  You can view the last run version of every report.

- **Grouping reports together on page 258**
  Every report must be assigned to a group.

- **Running reports on page 259**
  Reports must be run before examining their results.

- **Configuring Internet Explorer 8 to automatically accept McAfee ePO downloads on page 259**
  As a security measure, Microsoft Internet Explorer might block ePolicy Orchestrator downloads from occurring automatically. This behavior can be changed with an Internet Explorer configuration change.

- **Running a report with a server task on page 260**
  Reports can be run automatically using server tasks.

- **Exporting reports on page 260**
  Using the same report definition on multiple servers provides consistency in data gathering and presentation.

- **Importing reports on page 261**
  Reports can contain highly structured information, so exporting and importing them from one server to another allows your data retrieval and reporting to be consistently performed from any ePolicy Orchestrator server.

- **Deleting reports on page 261**
  You can delete reports that are no longer being used.

Creating a new report

You can create new reports and store them in ePolicy Orchestrator.

**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, Description and Group**. Name the report as desired, optionally give it a description, and select an appropriate group for it. Click **OK**.
4. You can now add, remove, rearrange elements, customize the header and footer, and change the page layout. At any point, you can check your progress by clicking **Run** to run the report.
5. When you are finished, click **Save**.

Editing an existing report

You can modify an existing report’s contents or the order of presentation.

If you are creating a new report, you will arrive at this screen after clicking **New Report**.
Task
For option definitions, click ? in the interface.

1 Click Menu | Reporting | Queries & Reports, then select the Report tab.
2 Select a report from the list by selecting the checkbox next to its name.
3 Click Edit.
   The Report Layout page appears.

Any of the following tasks can now be performed on the report.

Tasks
- Adding elements to a report on page 254
  You can add new elements to an existing report.
- Configuring image report elements on page 254
  You can upload new images and modify the images used within a report.
- Configuring text report elements on page 255
  You can insert static text within a report to explain its contents.
- Configuring query table report elements on page 255
  Some queries are better displayed as a table when inside a report.
- Configuring query chart report elements on page 256
  Some queries are better displayed as a chart when inside a report.
- Customizing report headers and footers on page 256
  Headers and footers provide information about the report.
- Removing elements from a report on page 257
  You can remove elements from a report if no longer needed.
- Reordering elements within a report on page 258
  You can change the order in which elements appear within a report.

Adding elements to a report
You can add new elements to an existing report.

Before you begin
You must have a report open in the Report Layout page to perform this task.

Task
For option definitions, click ? in the interface.

1 Select an element from the Toolbox and drag it over the Report Layout.
2 When the element is over your desired location, drop it.
   Report elements other than Page Break require configuration. The configuration page for the element appears.
3 After configuring the element, click OK.

Configuring image report elements
You can upload new images and modify the images used within a report.

Before you begin
You must have a report open in the Report Layout page.
**Task**
For option definitions, click ? in the interface.

1 To configure an image already in a report, click the arrow at the top left corner of the image. Click Configure.
   
   This will display the Configure Image page. If you are adding a new image to the report, the Configure Image page appears immediately after you drop the Image element onto the report.

2 If you want to use an existing image, select it from the gallery.

3 If you want to use a new image, click Browse and select the image from your computer. Click OK.

4 If you want to specify a specific image width, enter it in the Image Width field.
   
   By default, the image will be displayed in its existing width without resizing unless that width is wider than the available width on the page. In that case, it will be resized to the available width keeping aspect ratio intact.

5 Select if you want the image aligned left, center, or right.

6 Click OK.

**Configuring text report elements**
You can insert static text within a report to explain its contents.

**Before you begin**
You must have a report open in the Report Layout page.

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

1 To configure text already in a report, click the arrow at the top left corner of the text element. Click Configure.
   
   This displays the Configure Text page. If you are adding new text to the report, the Configure Text page appears immediately after you drop the Text element onto the report.

2 Edit the existing text in the Text edit box, or add new text.

3 Change the font size as appropriate.
   
   The default is 12pt type.

4 Select the text alignment: left, center, or right.

5 Click OK.

The text you entered appears in the text element within the report layout.

**Configuring query table report elements**
Some queries are better displayed as a table when inside a report.

**Before you begin**
You must have a report open in the Report Layout page.
**Task**

For option definitions, click ? in the interface.

1. To configure a table already in a report, click the arrow at the top left corner of the table. Click **Configure**.
   
   This displays the **Configure Query Table** page. If you are adding a new query table to the report, the **Configure Query Table** page appears immediately after you drop the **Query Table** element onto the report.

2. Select a query from the **Query** drop-down list.

3. Select the database from the **Database** drop-down list to run the query against.

4. Choose the font size used to display the table data.
   
   The default is 8pt type.

5. Click **OK**.

**Configuring query chart report elements**

Some queries are better displayed as a chart when inside a report.

**Before you begin**

You must have a report open in the **Report Layout** page.

**Task**

For option definitions, click ? in the interface.

1. To configure a chart already in a report, click the arrow at the top left corner of the chart. Click **Configure**.

   This will display the **Configure Query Chart** page. If you are adding a new query chart to the report, the **Configure Query Chart** page appears immediately after you drop the **Query Table** element onto the report.

2. Select a query from the **Query** drop-down list.

3. Select whether to display only the chart, only the legend, or a combination of the two.

4. If you have chosen to display both the chart and legend, select how the chart and legend are placed relative to each other.

5. Select the font size used to display the legend.
   
   The default is 8pt type.

6. Select the chart image height in pixels.
   
   The default is one-third the page height.

7. Click **OK**.

**Customizing report headers and footers**

Headers and footers provide information about the report.

There are six fixed locations within the header and footer that can contain different data fields. Three are in the header, three in the footer.
The header contains a left-aligned logo and two right-aligned fields, one above the other. These fields can contain one of four values:

- Nothing
- Date/Time
- Page Number
- User name of the user running the report

The footer contains three fields. One left-aligned, one centered, and one right-aligned. These three fields can also contain the same values listed above as well as custom text.

**Task**

For option definitions, click ? in the interface.

1. Click Menu | Reporting | Queries. Select the Report tab.
2. Select a report and click Actions | Edit.
3. Click Header and Footer.

4. By default, reports use the system setting for headers and footers. If you do not want this, deselect Use Default Server Setting.

   To change the system settings for headers and footers, click Menu | Configuration | Server Settings, then select Printing and Exporting and click Edit.

5. To change the logo, click Edit Logo.
   a. If you want the logo to be text, select Text and enter the text in the edit box.
   b. To upload a new logo, select Image then browse to and select the image on your computer and click OK.
   c. To use a previously-uploaded logo, select it.
   d. Click Save.

6. Change the header and footer fields to match the desired data, then click OK.
7. Click Save to save changes to the report.

**Removing elements from a report**

You can remove elements from a report if no longer needed.

**Task**

For option definitions, click ? in the interface.

1. Click Menu | Reporting | Queries & Reports, then select the Report tab.
2. Select a report and click Actions | Edit.
3. Click the arrow in the top left corner of the element you want to delete, then click Remove.
   The element is removed from the report.
4. To save changes to the report, click Save.
Reordering elements within a report
You can change the order in which elements appear within a report.

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

1. Click **Menu | Reporting | Queries & Reports**, then select the **Report** tab.
2. Select a report from the list and click **Actions | Edit**
3. To move an element, click the title bar of the element and drag it to a new position. The element positioning under the dragged element will shift as you move the cursor around the report. Red bars appear on either side of the report if the cursor is over an illegal position.
4. When the element is positioned where you want it, drop the element.
5. Click **Save** to save the changes to the report.

Viewing report output
You can view the last run version of every report.
Every time a report is run, the results are stored on the server and displayed in the report list.

Whenever a report is run, the prior results are erased and cannot be retrieved. If you are interested in comparing different runs of the same report, it is recommended you archive the output elsewhere.

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

1. Click **Menu | Reporting | Queries & Reports**, then select the **Report** tab.
2. In the report list, you will see a **Last Run Result** column. Each entry in this column is a link to retrieve the PDF that resulted from the last successful run of that report. Click a link from this column to retrieve a report. This will attempt to open a PDF within your browser, and your browser will behave as you have configured it for that file type.

Grouping reports together
Every report must be assigned to a group.
Reports are assigned to a group when initially created, but this assignment can be changed later. The most common reasons for grouping reports together are to collect similar reports together, or to manage permissions to certain reports.

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

1. Click **Menu | Reporting | Queries & Reports**, then select the **Report** tab.
2. Select a report and click **Actions | Edit**.
3. Click **Name, Description and Group**.
4. Select a group from the **Report Group** drop-down list and click **OK**.

5. Click **Save** to save any changes to the report.

When you select the chosen group from the **Groups** list in the left pane of the report window, the report now appears in the report list.

### Running reports

Reports must be run before examining their results.

Reports can be run in three different locations within ePolicy Orchestrator:

- The report listing
- Within a server task
- The Report Layout page while creating a new, or editing an existing report.

This topic explains running reports from within the report listing.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu** | **Reporting** | **Queries & Reports**, then select the **Report** tab.

2. Select a report from the report list, then click **Actions** | **Run**.

   When the report is complete, the resulting PDF is sent to your browser. It is displayed or downloaded according to your browser settings.

Some reports take a while to complete. It is possible to have more than one report running simultaneously, but you cannot initiate more than one report at a time through the interface. When the report is complete, the **Last Run Result** column in the report list is updated with a link to the PDF containing those results.

### Configuring Internet Explorer 8 to automatically accept McAfee ePO downloads

As a security measure, Microsoft Internet Explorer might block ePolicy Orchestrator downloads from occurring automatically. This behavior can be changed with an Internet Explorer configuration change.

Certain operations in ePolicy Orchestrator, such as running a report or exporting information into an XML file, can cause Internet Explorer 8 to notify you that a download has been blocked.

Internet Explorer displays this notification in a yellow bar immediately below the tab bar reading **To help protect your security, Internet Explorer blocked this site from downloading files to your computer. Click here for options...** If you click the message, you are given the option to download the blocked file this one time. However, the message reappears the next time ePolicy Orchestrator attempts to send you a file. To make this message go away permanently, do the following:

**Task**

1. In Internet Explorer 8, select **Tools** | **Internet Options**.

2. Select the **Security** tab and click **Local Intranet**.

   If you have made your ePolicy Orchestrator server a trusted site, click **Trusted Sites** instead of **Local Intranet**.

3. Click **Custom Level**....
Scroll down to the **Automatic prompting for file downloads** option and set it to **Enable**. Click **OK** and click **Yes** to confirm your choice.

Click **OK** to close the **Internet Options** dialog.

Attempting the original operation again downloads the requested file without the yellow caution bar appearing.

### Running a report with a server task

Reports can be run automatically using server tasks.

If you want a report to be run without manual intervention, a server task is the best approach. This task creates a new server task allowing for automatic, scheduled runs of a given report.

**Task**

For option definitions, click ? in the interface.

1. Click **Menu** | **Automation** | **Server Tasks**, then click **Actions** | **New Task**.

2. Give the task an appropriate **Name**, optional **Notes**, and whether the task has a **Schedule status**. Click **Next**.

   If you want the task to be run automatically, set **Schedule status** to **Enabled**.

3. In the **Actions** drop-down list, choose **Run Report**. Select the report to run and the target language. Click **Next**.

4. Choose the **Schedule type** (the frequency), **Start date**, **End date**, and **Schedule** time to run the report. Click **Next**.

   The schedule information will only be used if you enable **Schedule status**.

5. Click **Save** to save the server task.

The new task now appears in the **Server Tasks** list.

### Exporting reports

Using the same report definition on multiple servers provides consistency in data gathering and presentation.

All reports exported simultaneously are contained within the same XML file. Also, report definitions contain complete definitions of all items making up that report. Creating a report and exporting it can be a convenient way to export many diverse items simultaneously.

**Task**

For option definitions, click ? in the interface.

1. Enter the Reports page by selecting **Menu** | **Reporting** | **Queries & Reports**, then select the **Report** tab.

2. Select the group that contains the report(s) you want to export from the **Groups** list.

3. Select the report(s) you want to export, then click **Actions** | **Export**.

   The McAfee ePO server sends an XML file to your browser. What happens depends on your browser settings. By default, most browsers will ask you to save the file.

The exported report contains the definitions of all items contained within the report. This includes external database definitions, queries, graphics, and others.
Importing reports
Reports can contain highly structured information, so exporting and importing them from one server to another allows your data retrieval and reporting to be consistently performed from any ePolicy Orchestrator server.

Task
For option definitions, click ? in the interface.

1 Open the Queries page by selecting Menu | Reporting | Queries & Reports, then select the Report tab.
2 From the Report page, click Actions | Import.
3 Click Browse to navigate to and select the XML file containing the report you want to import.
4 Select a new or existing group for the report. If a new group, give the name of the group and select whether it is private or public. If an existing group, select the group the imported report will join.
5 Click OK.

A confirmation screen will appear displaying the information about the report(s) contained in the specified XML and the group the report will be imported into. If there is no valid report in the selected file, an error message will be displayed.
6 Click Import to finalize the import.

Newly imported reports acquire the permissions of the group they were imported into.

Deleting reports
You can delete reports that are no longer being used.

Before you begin
To delete a report, you must have edit permissions for that report.

Task
For option definitions, click ? in the interface.

1 Click Menu | Reporting | Queries & Reports, then select the Report tab.
2 Select one or more reports to delete from the list of reports.
3 Click Actions | Delete. If you are confident in your actions, click Yes.

The reports are deleted. Any server tasks that refer to deleted reports are no longer valid.

Using database servers
ePolicy Orchestrator can retrieve data from not only its own databases, but those provided by some extensions as well.

You might need to register several different server types to accomplish tasks within ePolicy Orchestrator. These can include authentication servers, Active Directory catalogs, ePolicy Orchestrator servers, and database servers that work with specific extensions you have installed.
Database types
An extension can register a database type, otherwise known as a schema or structure, with ePolicy Orchestrator. If it does, that extension can provide data to queries, reports, dashboard monitors, and server tasks. To use this data, you must first register the server with ePolicy Orchestrator.

Database server
An database server is a combination of a server and a database type installed on that server. A server can host more than one database type, and a database type can be installed on multiple servers. Each specific combination of the two must be registered separately and is referred to as a database server.

After you register a database server, you can retrieve data from the database in queries, reports, dashboard monitors, and server tasks. If more than one database using the same database type is registered, you are required to select one of them as the default for that database type.

---

**Working with database servers**

Database servers can be registered, modified, viewed, and deleted.

**Tasks**

- **Modifying a database registration on page 262**
  
  If connection information or login credentials for a database server changes, you must modify the registration to reflect the current state.

- **Removing a registered database on page 262**
  
  You can remove databases from the system when they are no longer needed.

**Modifying a database registration**

If connection information or login credentials for a database server changes, you must modify the registration to reflect the current state.

**Task**

For option definitions, click ? in the interface.

1. Open the Registered Servers page by selecting Menu | Configuration | Registered Servers.
2. Select a database to edit, then click Actions | Edit
3. Change the name or notes for the server, and click Next.
4. Modify the information as appropriate. If you need to verify the database connection, click Test Connection.
5. Click Save to save your changes.

**Removing a registered database**

You can remove databases from the system when they are no longer needed.
Task
For option definitions, click ? in the interface.

1. Open the Registered Servers page: select Menu | Configuration | Registered Servers.
2. Select a database to delete, and click Actions | Delete.
3. When the confirmation dialog appears, click Yes to delete the database.

The database has been deleted. Any queries, reports, or other items within ePolicy Orchestrator that used the deleted database will be marked invalid until updated to use a different database.
Detecting Rogue Systems

Unprotected systems are often the weak spot of any security strategy, creating entry points through which viruses and other potentially harmful programs can access your network. Even in a managed network environment, some systems might not have an active McAfee Agent on them. These can be systems that frequently log on and off the network, including test servers, laptops, or wireless devices.

Rogue System Detection provides real-time discovery of rogue systems through the use of a Rogue System Sensor installed throughout your network. The sensor listens to network broadcast messages and DHCP responses to detect systems connected to the network.

When a sensor detects a system on the network, it sends a message to the ePolicy Orchestrator server. The server then checks whether the system has an active agent installed and managed. If the system is unknown to the McAfee ePO server, Rogue System Detection provides information to ePolicy Orchestrator to allow you to take remediation steps, which include alerting network and anti-virus administrators or automatically deploying an agent to the system.

In addition to Rogue System Detection, other McAfee products, like McAfee Network Access Control, add detected systems control to ePolicy Orchestrator.

Contents

- What are rogue systems
- How the Rogue System Sensor works
- How detected systems are matched and merged
- Working with detected systems
- Working with sensors
- Working with subnets
- Rogue System Detection command-line options
- Default Rogue System Detection queries

What are rogue systems

Rogue systems are systems that access your network, but are not managed by your McAfee ePO server. Unprotected systems are often the weak spot of any security strategy, creating entry points through which viruses and other potentially harmful programs can access your network. Even in a managed network environment, some systems might not have an active McAfee Agent on them. These can be systems that frequently log on and off the network, including test servers, laptops, or wireless devices.

A rogue system is any device on your network with a network interface card (NIC). On systems with multiple NICs, each resulting interface is identified as a separate system. When these interfaces are detected, they appear as multiple rogue interfaces.
You can specify how the system interfaces are matched in the same manner you use to specify how detected systems are matched. Identifying these systems and their interfaces, and managing them with Rogue System Detection and ePolicy Orchestrator helps provide the network security your organization needs.

**Rogue System Detection states**

Rogue System Detection categorizes systems, sensors, and subnets on your network with different states to make monitoring and managing your network easier. These states determine the following:

- Overall system status
- Rogue System Sensor status
- Subnet status

The Detected Systems page displays information on each of these states via corresponding status monitors. This page also displays the 25 subnets with the most rogue system interfaces in the Top 25 Subnets list and the adjacent Rogue System Interfaces by Subnet table.

**Overall system status**

Overall system status is presented in the Overall System Status monitor as a percentage of compliant systems. Systems states are separated into these categories:

- Exceptions
- Inactive
- Managed
- Rogue

The percentage of compliant systems is the ratio of systems in the Managed and Exceptions categories to those in the Rogue and Inactive categories.
Exceptions

Exceptions are systems that don’t need a McAfee Agent, such as routers, printers, or systems from which you no longer want to receive detection information. Identify these systems and mark them as exceptions to prevent them from being categorized as rogue systems. Mark a system as an exception only when it does not represent a vulnerability in your environment.

Inactive

Inactive systems are listed in the McAfee ePO database, but have not been detected by a detection source in a specified time, which exceeds the period specified in the Rogue category. Most likely these are systems that are shut down or disconnected from the network, for example, a laptop or retired system. The default time period for marking systems as inactive is 45 days.

Managed

Managed systems have an active McAfee Agent that has communicated with the McAfee ePO server in a specified time. To ensure security, the majority of detected systems on your network should be managed.

Rogue

Rogue systems are systems that are not managed by your McAfee ePO server. There are three rogue states:

- Alien agent — These systems have a McAfee Agent that is not in the local McAfee ePO database, or any database associated with additional McAfee ePO servers you have registered with the local server.
- Inactive agent — These systems have a McAfee Agent in the McAfee ePO database that has not communicated in a specified time.
- Rogue — These systems don’t have a McAfee Agent.

Systems in any of these three rogue states are categorized as Rogue systems.

Rogue System Sensor status

Rogue System Sensor status is the measure of how many sensors installed on your network are actively reporting to the McAfee ePO server, and is displayed in terms of health. Health is determined by the ratio of active sensors to missing sensors on your network. Sensor states are categorized into these groups:

- Active
- Missing
- Passive
Active
Active sensors report information about their broadcast segment to the McAfee ePO server at regular intervals, over a fixed time. Both the reporting period and the active period are user-configured. A sensor becomes passive when the active period lapses, at which time the next passive sensor to report in is made active.

Missing
Missing sensors have not communicated with the McAfee ePO server in a user-configured time. These sensors could be on a system that has been turned off or removed from the network.

Passive
Passive sensors check in with the McAfee ePO server, but do not report information about detected systems. They wait for instructions from the McAfee ePO server to replace other sensors that become passive.

Subnet status
Subnet status is the measure of how many detected subnets on your network are covered. Coverage is determined by the ratio of covered subnets to uncovered subnets on your network. Subnet states are categorized into these groups:
- Contains Rogues
- Covered
- Uncovered

Subnets must be known by the McAfee ePO server or be seen by a sensor to fall into one of these categories. Once a subnet has been detected, you can mark it Ignored to prevent receiving further reporting about its status.

Contains Rogues
Subnets that contain rogue systems are listed in the Contains Rogues category to make it easier to take action on them.

Covered
Covered subnets have sensors installed on them that are actively reporting information about detected systems to the McAfee ePO server. The Covered subnets category also includes the systems listed in the Contains Rogues category. For example, the Covered subnets category contains subnets A, B, and C. Subnet B contains rogues, while A and C do not. All three are listed in the Covered category; only subnet B is listed in the Contains Rogues category.

Uncovered
Uncovered subnets don’t have any active sensors on them. Subnets that are uncovered are not reporting information about detected systems to the McAfee ePO server. However, there might be managed systems on this subnet that are being reported on through other means, such as agent-server communication.

Top 25 Subnets
The Top 25 Subnets list provides the subnet list, by name or IP, for the 25 subnets that contain the most rogue system interfaces on your network. When a top 25 subnet is selected, the rogue system interfaces it contains are displayed in the adjacent Rogue System Interfaces by Subnet table.
**Rogue Sensor Blacklist**

The Rogue Sensor Blacklist is the list of managed systems where you do not want sensors installed. These can include systems that would be adversely affected if a sensor were installed on them, or systems you have otherwise determined should not host sensors. For example, mission critical servers where peak performance of core services is essential, such as database servers or servers in the DMZ (demilitarized zone). Also, systems that might spend significant time outside your network, such as laptops.

The Rogue Sensor Blacklist is different than the Exceptions list, in that systems on the Exceptions list are those that either can’t have an agent on them, or that you don’t want categorized as Rogue, such as printers or routers.

**Rogue System Detection policy settings**

Rogue System Detection policy settings allow you to configure and manage the instances of the Rogue System Sensor installed throughout your network. Settings can be applied to individual systems, groups of systems, and IP ranges.

You can configure policy settings for all sensors deployed by the server. This is similar to managing policies for any deployed product, such as VirusScan Enterprise. The Rogue System Detection policy pages are installed on the McAfee ePO server at installation.

Configure the sensor policy settings in the Rogue System Detection policy pages the same way you would for any managed security product. Policy settings that you assign to higher levels of the System Tree are inherited by lower-level groups or individual systems. For more information about policies and how they work, see *Managing your Network with Policies and Client Tasks*.

---

**Considerations for policy settings**

Policy settings configure the features and performance of the Rogue System Sensor. These settings are separated into four groups:

- Communication settings
- Detection settings
- General settings
- Interface settings

**Communication settings**

Communication settings determine:

- Communication time for inactive sensors.
- Reporting time for active sensors.
- Sensor’s detected system cache lifetime.

The communication time for inactive sensors determines how often passive sensors check in with the server.
The Reporting time for active sensors determines how often active sensors report to the McAfee ePO server. Setting this value too low can have the same effect as setting the value for the sensor’s detected system cache lifetime.

The sensor’s detected system cache lifetime is the amount of time a detected system remains in the sensor’s cache. This value controls how often the sensor reports that a system is newly detected. The lower the value, the more often the sensor reports a system detection to the server. Setting this value too low can overwhelm your server with system detections. Setting this value too high prevents you from having current information on system detections.

McAfee recommends that you set the sensor’s detected system cache lifetime and the reporting time for active sensors settings to the same value.

Detection settings
Detection settings determine whether:

- Device details detection is enabled.
- DHCP monitoring is enabled.
- Reporting on self-configured subnets is enabled.

If you use DHCP servers on your network, you can install sensors on them to monitor your network. This allows you to use a single sensor to report on all subnets and systems that connect to it. DHCP monitoring allows you to cover your network with fewer sensors to deploy and manage, and reduces the potential for missed subnets and systems.

Device details detection allows you to specify the type of information the Rogue System Sensor scans systems for.

- Operating System (OS) details — This option allows the sensor to determine detailed information about a device's operating system. If you enable OS details scanning, you can also choose to scan the systems you have marked as exceptions.

- You can also specify which systems and networks are scanned using OS detection by choosing to scan all networks or only specific networks. You can limit OS detection to specific subnets by included or excluding specific IP addresses.

The Rogue System Sensor uses NetBIOS calls and OS fingerprinting to provide more detailed information about the devices on your network. You can enable active probing on your entire network, or include or exclude specific subnets.

This Device details detection feature provides accurate matching of detected system interfaces and should be disabled only if you have specific reasons to do so.

General settings
General settings determine:
• Sensor-to-server communication port.
• Server IP address or DNS name.
• Whether the Rogue System Sensor is enabled.

The server IP address default value is the address of the McAfee ePO server that you are using to install sensors. Rogue System Detection reports system detections to the specified server. When this server detects a system that has an agent deployed by an McAfee ePO server with a different IP address, that system is detected as a rogue because the agent is considered an alien agent.

The sensor-to-server communication port server setting can be changed only during installation. Whichever port you have specified during installation must also be specified in the General tab of Rogue System Detection policies.

Interface settings

Interface settings determine whether sensors:
• Do not listen on interfaces whose IP addresses are included in specific networks.
• Only listen on an interface if its IP address is included on a network found during installation.
• Only listen on interfaces whose IP addresses are included in specific networks.

Specifying these settings allows you to choose the networks that the sensor reports on.

Rogue System Detection permission sets

Permission sets for Rogue System Detection determine what information a user group can view, modify, or create for Rogue System Detection. One or more permission sets can be assigned. By default, permission sets for global administrators are automatically assigned to include full access to all products and features.

The permission sets and their available privileges for Rogue System Detection are listed in the following table.

<table>
<thead>
<tr>
<th>Permission set</th>
<th>Rights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rogue System Detection</td>
<td>• Create and edit Rogue System information; manage sensors.</td>
</tr>
<tr>
<td></td>
<td>• Create and edit Rogue System information; manage sensors; deploy McAfee Agents and add to System Tree.</td>
</tr>
<tr>
<td></td>
<td>• No permissions.</td>
</tr>
<tr>
<td></td>
<td>• View Rogue System information.</td>
</tr>
<tr>
<td>Rogue System Sensor</td>
<td>• No permissions.</td>
</tr>
<tr>
<td></td>
<td>• View and change settings.</td>
</tr>
<tr>
<td></td>
<td>• View settings.</td>
</tr>
</tbody>
</table>
How the Rogue System Sensor works

The Rogue System Sensor is the distributed portion of the Rogue System Detection architecture. Sensors detect systems, routers, printers, and other devices connected to your network. They gather information about the devices they detect, and forward the information to the McAfee ePO server.

The sensor is a Win32 native executable application that runs on any NT-based Windows operating system, including:

- Windows XP
- Windows Server 2003
- Windows 2008
- Windows Vista
- Windows 7

It can be installed on systems throughout your network. A sensor reports on all systems in the broadcast segment where it is installed. A sensor installed on a DHCP server reports on all systems or subnets using DHCP. To maintain coverage in networks or broadcast segments that don’t use DHCP servers, you must install at least one sensor in each broadcast segment, usually the same as a subnet. DHCP deployment can be used with segment-specific deployment of the Rogue System Sensor for the most comprehensive coverage.

Passive listening to layer-2 traffic

To detect systems on the network, the sensor uses WinPCap, a packet capture library. It captures layer-2 broadcast packets sent by systems that are connected to the same network broadcast segment. It also listens passively to all layer-2 traffic for Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP), IP traffic, and DHCP responses.

To obtain additional information, the sensor also performs NetBIOS calls and OS fingerprinting on systems that were already detected. It does this by listening to the broadcast traffic of all devices in its broadcast segment, and by using NetBIOS calls, actively probing the network to gather additional information about the devices connected to it, such as the operating system of a detected system.

The sensor does not determine whether the system is a rogue system. It detects systems connected to the network and reports these detections back to the McAfee ePO server, which determines whether the system is rogue based on user-configured settings.

Intelligent filtering of network traffic

The sensor filters network traffic "intelligently" — it ignores unnecessary messages and captures only what it needs, which is Ethernet and IP broadcast traffic. By filtering out unicast traffic, which might contain non-local IP addresses, the sensor focuses only on devices that are part of the local network.

To optimize performance and minimize network traffic, the sensor limits its communication to the server by relaying only new system detections, and by ignoring any re-detected systems for a user-configured time. For example, the sensor detects itself among the list of detected systems. If the sensor sent a message every time it detected a packet from itself, the result would be a network overloaded with sensor detection messages.
The sensor further filters on systems that were already detected:

- The sensor reports any system the first time it is detected on the network.
- For each detected system, the sensor adds the MAC address to the packet filter, so that it is not detected again, until the user-configured time elapses.
- The sensor implements aging on the MAC filter. After a specified time, MAC addresses for systems that have already been detected are removed from the filter, causing those systems to be re-detected and reported to the server. This process ensures that you receive accurate and current information about detected systems.

**Data gathering and communications to the server**

Once the sensor detects a system on the local network, it gathers information about that system by actively scanning using NetBIOS calls and OS fingerprinting.

The gathered information includes:

- DNS name
- Operating system version
- NetBIOS information (domain membership, system name, and the list of currently logged-on users)

All NetBIOS-related information that is gathered is subject to standard limitations of authorization, and other limitations documented in the Microsoft management API.

The sensor packages the gathered information into an XML message, then sends the message via secure HTTPS to the ePolicy Orchestrator server for processing. The server then uses the ePolicy Orchestrator data to determine whether the system is a rogue system.

**Bandwidth use and sensor configuration**

To save bandwidth in large deployments, you can configure how often the sensor sends detection messages to the server. You can configure the sensor to cache detection events for a given time period, such as one hour, then to send a single message containing all the events from that time period. For more information, see Configuring Rogue System Detection policy settings.

**Systems that host sensors**

Install sensors on systems that are likely to remain on and connected to the network at all times, such as servers. If you don’t have a server running in a given broadcast segment, install sensors on several workstations to ensure that at least one sensor is connected to the network at all times.

To guarantee that your Rogue System Detection coverage is complete, you must install at least one sensor in each broadcast segment of your network. Installing more than one sensor in a broadcast segment does not create issues around duplicate messages because the server filters any duplicates. However, additional active sensors in each subnet results in traffic sent from each sensor to the server. While maintaining as many as five or ten sensors in a broadcast segment should not cause any bandwidth issues, you should not maintain more sensors in a broadcast segment than is necessary to guarantee coverage.
DHCP servers

If you use DHCP servers in your network, you can install sensors on them. Sensors installed on DHCP servers report on all connected subnets by listening for DHCP responses. Using sensors on DHCP servers reduces the number of sensors you need to install and manage on your network to ensure coverage, but it does not eliminate the need to install sensors to network segments that use static IP address.

Installing sensors on DHCP servers can improve coverage of your network. However, it is still necessary to install sensors in broadcast segments that use static IP address, or that have a mixed environment. A sensor installed on a DHCP server does not report on systems covered by that server if the system uses a static IP address.

How detected systems are matched and merged

When a system connects to your network, Rogue System Detection automatically checks the McAfee ePO database to determine whether the incoming system is new or corresponds to a previously detected system. If the system has been previously detected, Rogue System Detection automatically matches it to the existing record in the McAfee ePO database. When a detected system is not matched automatically, you can manually merge the system with an existing detected system.

Matching detected systems

Automatic matching of detected systems is necessary to prevent previously detected systems from being identified as new systems on your network. By default, systems are first matched against an agent’s unique ID. If this unique ID does not exist, the McAfee ePO database uses attributes specified in the Rogue System Matching server settings. You can specify which attributes the database uses for matching, based on which attributes are unique in your environment.

If a system on your network has multiple NICs, each system interface can result in separate detections. Use the Detected System Matching Server Setting to match multiple interfaces to an existing detected system in order to eliminate duplicate systems.

Merging detected systems

When the McAfee ePO server cannot automatically match detected systems, you can merge them manually using Merge systems. For example, the McAfee ePO server might not be able to match a detected system interface that was generated by a system with multiple NICs, based on the matching attributes you have specified.

Working with detected systems

Use these tasks to manage detected systems in Rogue System Detection.
Tasks

- **Configuring Rogue System Detection policy settings** on page 275
  Use this task to configure Rogue System Detection policy settings. Policy settings determine how the sensor obtains and reports information about systems detected on your network.

- **Adding systems to the Exceptions list** on page 276
  Use this task to add detected systems to the Exceptions list.

- **Adding systems to the Rogue Sensor Blacklist** on page 277
  Use this task to add detected systems to the Rogue Sensor Blacklist.

- **Adding detected systems to the System Tree** on page 277
  Use this task to add detected systems to the System Tree from the Detected Systems pages.

- **Editing system comments** on page 277
  Use this task to edit system comments. System comments can be useful for noting important "human readable" information to a detected system entry.

- **Exporting the Exceptions list** on page 278
  Use this task to export the list of MAC addresses of the detected systems on your network that are marked as Exceptions.

- **Importing systems to the Exceptions list** on page 278
  Use this task to import systems to your network’s Exceptions list.

- **Merging detected systems** on page 278
  Use this task to merge detected systems.

- **Pinging a detected system** on page 279
  Use this task to ping a detected system to confirm that it can be reached over the network.

- **Querying detected system Agents** on page 279
  Use this task to query Agents installed on detected systems. Not all detected systems have a McAfee Agent installed. The results of this task indicate whether an Agent is installed and provides links to details about the system and the agent, if available.

- **Removing systems from the Detected Systems list** on page 279
  Use this task to remove systems from the Detected Systems list. You might want to remove a system from this list when you know it is no longer in service. Once a system has been removed, it does not appear in the Detected Systems list until the next time the system is detected.

- **Removing systems from the Exceptions list** on page 280
  Use this task to remove detected systems from the Exceptions list. You might want to remove systems from this list if you would like to start receiving detection information about it, or you know that the system is no longer connected to your network.

- **Removing systems from the Rogue Sensor Blacklist** on page 280
  Use this task to remove detected systems from the Rogue Sensor Blacklist. Rogue System Detection prevents sensors from being installed on systems included in the blacklist. If you want to install a sensor on a system that has been blacklisted, you must remove the system from the list.

- **Viewing detected systems and their details** on page 280
  Use this task to view detected systems and their details. You can view detected system details from any page that displays detected systems.

**Configuring Rogue System Detection policy settings**

Use this task to configure Rogue System Detection policy settings. Policy settings determine how the sensor obtains and reports information about systems detected on your network.

For option definitions, click ? in the interface.
## Task

1. Click **Menu | Policy | Policy Catalog**, then from the Product drop-down list select **Rogue System Detection x.x.x** and from the Category drop-down list, select **General**. All created policies for Rogue System Detection appear.

2. Edit an existing policy, or create a new policy.
   - To edit an existing policy, locate the desired policy and click **Edit Settings** in its row.
   - To create a new policy, click **Actions | New Policy**, from the **Create a policy based on this existing policy** drop-down menu, then select an existing policy on which to base the new policy. Name the new policy and click **OK**.

3. Configure the desired settings, then click **Save**.

### Adding systems to the Exceptions list

Use this task to add detected systems to the Exceptions list.

For options definitions, click ? in the interface.

<table>
<thead>
<tr>
<th>This task can be performed from:</th>
<th>Getting there</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Detected Systems page</strong></td>
<td>1. Click **Menu</td>
</tr>
<tr>
<td></td>
<td>2. From <strong>Detected System Interfaces by Subnet</strong> pane, click any system.</td>
</tr>
<tr>
<td></td>
<td>3. Click **Actions</td>
</tr>
</tbody>
</table>
|                                  | 4. Select one of the following to configure the **Detected Systems | Exceptions** display, and click **OK**:
|                                  |   • **No Category** — Displayed without a category entry. |
|                                  |   • **New Category** — Displayed with the new category name you type. |
|                                  |   • **Select Category** — Displayed with the category selected from the list. |
|                                  |   - **To configure categories, see Editing Detected System Exception Categories.** |
| **Detected Systems Details page** | 1. Click **Menu | Systems | Detected Systems**. |
|                                  | 2. From **Overall System Status** monitor pane, click any detected system category |
|                                  | 3. From the **Detected Systems Details** page, click any system. |
|                                  | 4. Click **Actions | Detected Systems | Add to Exceptions**. The Add to Exceptions dialog box appears. |
|                                  | 5. Select one of the following to configure the **Detected Systems | Exceptions** display, and click **OK**:
|                                  |   • **No Category** — Displayed without a category entry. |
|                                  |   • **New Category** — Displayed with the new category name you type. |
|                                  |   • **Select Category** — Displayed with the category selected from the list. |
|                                  |   - **To configure categories, see Editing Detected System Exception Categories.** |
Adding systems to the Rogue Sensor Blacklist

Use this task to add detected systems to the Rogue Sensor Blacklist.

For option definitions, click ? in the interface.

Task

1. Click Menu | Systems | System Tree | Systems and select the detected systems you want to add to the Rogue Sensor Blacklist.
2. Click Actions, then select Rogue Sensor | Add to Sensor Blacklist.
3. Click Yes to confirm the change.
4. To confirm that the system is moved to the Rogue Sensor Blacklist, click Menu | Systems | Detected Systems, then from the Rogue System Sensor Status monitor, click View Blacklist.

Adding detected systems to the System Tree

Use this task to add detected systems to the System Tree from the Detected Systems pages

<table>
<thead>
<tr>
<th>This task can be performed from:</th>
<th>Getting there</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detected Systems page</td>
<td>Click Menu</td>
</tr>
<tr>
<td>Detected Systems Status page</td>
<td>Click Menu</td>
</tr>
</tbody>
</table>

Task

For option definitions, click ? in the interface.

1. Select the detected systems you want to add to the System Tree.
2. Click Actions | Detected Systems | Add to System Tree. The Add to System Tree page opens.
3. Click Browse to open the Select System Tree Group dialog box, which allows you to navigate to the location where you want to add the selected systems.
4. Specify whether to
   - Tag and Sort Systems — Applies tags and sorts system immediately after adding the systems to the System Tree.
   - Duplicate System Names — Allows duplicate entries to be added to the System Tree.

Editing system comments

Use this task to edit system comments. System comments can be useful for noting important "human readable" information to a detected system entry.

<table>
<thead>
<tr>
<th>This task can be performed from:</th>
<th>Getting there</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detected Systems Details page.</td>
<td>Click Menu</td>
</tr>
<tr>
<td>Detected Systems page.</td>
<td>Click Menu</td>
</tr>
</tbody>
</table>

For option definitions, click ? in the interface.
Task
1 Select the system whose comment you want to edit, then click Actions | Detected Systems | Edit Comment.

2 Type your comments in the Enter New Comment field of the popup, then click OK.

Exporting the Exceptions list
Use this task to export the list of MAC addresses of the detected systems on your network that are marked as Exceptions.
For option definitions, click ? in the interface.

Task
1 Click Menu | Systems | Detected Systems, click Import/Export Exceptions from the Overall System Status monitor, then click the Export Exceptions tab.

2 Click on the link and save the file.

Files are exported in the Comma Separated Value format. The file name for your Exceptions list is predefined as RSDExportedExceptions.csv. You can change the name of the file when you download it to your local system.

Importing systems to the Exceptions list
Use this task to import systems to your network’s Exceptions list.
For option definitions, click ? in the interface.

Task
1 Click Menu | Systems | Detected Systems, click Import/Export Exceptions from the Overall System Status monitor, then click the Import Exceptions tab.

2 Choose the method you want to use to import, specify the systems or file, then click Import Exceptions.

When importing systems, only MAC addresses are recognized. MAC addresses can be separated by whitespace, commas, or semicolons. The MAC address can include colons, but they are not required.

Merging detected systems
Use this task to merge detected systems.
For option definitions, click ? in the interface.

Task
1 Click Menu | Systems | Detected Systems, then from Overall System Status monitor, select Rogue. The rogue systems appear in the display.

2 Select the systems you want to merge.

3 Click Actions, then select Detected Systems | Merge Systems. The Merge Systems page appears.

4 Click Merge.

5 When the merge warning message appears, click OK.
Pinging a detected system

Use this task to ping a detected system to confirm that it can be reached over the network.

<table>
<thead>
<tr>
<th>This task can be performed from:</th>
<th>Getting there</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detected Systems Status page</td>
<td>Click Menu</td>
</tr>
<tr>
<td>System Tree page</td>
<td>Click Menu</td>
</tr>
</tbody>
</table>

For option definitions, click ? in the interface.

Task

1. Select the system you want to ping.

   You can only ping one system at a time.

2. Click Actions | Detected Systems or Directory Management, then click Ping. The result is displayed on the Actions bar in the notification panel at the bottom right corner of the McAfee ePO console window.

Querying detected system Agents

Use this task to query Agents installed on detected systems. Not all detected systems have a McAfee Agent installed. The results of this task indicate whether an Agent is installed and provides links to details about the system and the agent, if available.

<table>
<thead>
<tr>
<th>This task can be performed from:</th>
<th>Getting there</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detected Systems page</td>
<td>Click Menu</td>
</tr>
<tr>
<td>Detected Systems Status page</td>
<td>Click Menu</td>
</tr>
</tbody>
</table>

Task

For option definitions, click ? in the interface.

1. Select the systems whose Agents you want to query.

2. Click Actions | Detected Systems | Query Agent or Actions | Query Agent. The Query McAfee Agent Results page opens.

Removing systems from the Detected Systems list

Use this task to remove systems from the Detected Systems list. You might want to remove a system from this list when you know it is no longer in service. Once a system has been removed, it does not appear in the Detected Systems list until the next time the system is detected.

For option definitions, click ? in the interface.

Task

1. Click Menu | Systems | Detected Systems.

2. In the Overall System Status monitor, click any detected system category then click the system you want to remove.

3. Click Actions | Detected Systems | Delete, then click OK when prompted.
Removing systems from the Exceptions list

Use this task to remove detected systems from the Exceptions list. You might want to remove systems from this list if you would like to start receiving detection information about it, or you know that the system is no longer connected to your network.

For option definitions, click ? in the interface.

Task

1. Click Menu | Systems | Detected Systems.
2. In the Overall System Status monitor, click the Exceptions category, then select the system you want to remove.
3. Click Actions, select Detected Systems | Remove from Exceptions, then click OK when prompted.

Removing systems from the Rogue Sensor Blacklist

Use this task to remove detected systems from the Rogue Sensor Blacklist. Rogue System Detection prevents sensors from being installed on systems included in the blacklist. If you want to install a sensor on a system that has been blacklisted, you must remove the system from the list.

For option definitions, click ? in the interface.

Task

1. Click Menu | Systems | Detected Systems.
2. In the Rogue System Sensor Status monitor, click View Blacklist.
3. Select the system you want to remove from the Rogue System Blacklist page.
4. Click Actions, select Rogue Sensor | Remove from Blacklist, then click OK when prompted.

Viewing detected systems and their details

Use this task to view detected systems and their details. You can view detected system details from any page that displays detected systems.

Task

For option definitions, click ? in the interface.

1. Click Menu | Systems | Detected Systems.
2. In the Overall System Status monitor, click any category to view the list of detected systems it contains, such as Managed. The Detected Systems page appears.
3. Click any detected system to view its details.

The System Details page is different than the Detected Systems Details page. The Detected Systems Details page displays some information that is unique to Rogue System Detection.

Working with sensors

Use these tasks when working with sensors, for example, to change install or remove a sensor.
Tasks

- **Installing sensors on page 281**
  Use any of these tasks to deploy sensors to your network.

- **Editing sensor descriptions on page 283**
  Use this task to edit sensor descriptions.

- **Removing sensors on page 283**
  Use this task to remove sensors from specific systems on your network. This task creates a deployment task that removes the sensor from the selected systems, then performs an immediate agent wake-up call on them.

**Installing sensors**

Use any of these tasks to deploy sensors to your network.

Tasks

- **Installing sensors on specific systems on page 281**
  Use this task to install sensors to specific systems on your network. This task creates a deployment task that installs the sensor to the selected systems, then performs an immediate agent wake-up call on them.

- **Using queries and server tasks to install sensors on page 282**
  Use this task to create a query that can run as a server task action that installs sensors on managed systems.

- **Using client task to install sensors on page 282**
  Use this task to create a client task that installs sensors to systems on your network.

**Installing sensors on specific systems**

Use this task to install sensors to specific systems on your network. This task creates a deployment task that installs the sensor to the selected systems, then performs an immediate agent wake-up call on them.

<table>
<thead>
<tr>
<th>This task can be performed from:</th>
<th>Getting there</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed Systems for Subnet xxx.xxx.xxx.xxx page</td>
<td>Click **Menu</td>
</tr>
<tr>
<td>Systems Details page</td>
<td>Click **Menu</td>
</tr>
<tr>
<td>Systems page</td>
<td>Click **Menu</td>
</tr>
</tbody>
</table>

For option definitions, click ? in the interface.

**Task**

1. Select the systems where you want to install sensors, then click **Actions | Rogue Sensor | Install Rogue Sensor**.
   - In the Managed Systems for Subnet xxx.xx.xx.xx.x page, select the systems where you want to install sensors.
   - In the Systems Details page, you can install the sensor only from the system you are viewing.
   - In the Systems page, select the desired group in the System Tree, and select the systems where you want to install sensors.

2. In the Action pane, click **OK**.
Using queries and server tasks to install sensors

Use this task to create a query that can run as a server task action that installs sensors on managed systems.

For option definitions, click ? in the interface.

**Task**

1. Click Menu | Reporting | Queries & Reports, then click Actions | New. The Query Builder wizard opens.

2. On the Result Type page, select System Management as Feature Group and Managed Systems as Result Types, then click Next.

3. From the Display Results As column on the Chart page, expand the List display and select Table, then click Next.

4. From the Available Columns pane on the Columns page, click the types of information you want your query to return, then click Next.

5. On the Filter page, click the properties you want to filter with and specify the values for each, then click Run.

6. Click Save and specify the name of your query and any notes, then click Save again.

   McAfee recommends using a product-specific prefix when naming your queries, to keep them organized and make them easier to find. For example, RSD: QueryName.

7. Click Menu | Automation | Server Tasks, then click Actions | New Task. The Client Task Builder wizard opens.

8. On the Description page, name and describe the task and specify the Schedule status, then click Next.

9. On the Action page, select Run Query from the drop-down list.

10. From the Query list, select the query you created. Then from the Language drop-down list, select the language you want for the displayed results.

11. Select Install Rogue Sensor as the subaction to take on the results of the query, then click Next.

12. On the Schedule page, specify the schedule for the task, then click Next.

13. Review the summary of the task, then click Save.

Using client task to install sensors

Use this task to create a client task that installs sensors to systems on your network.

For option definitions, click ? in the interface.

**Task**

1. Click Menu | Policy | Client Task Catalog, select Rogue System Detection x.x.x | Sensor Deployment as Client Task Types, then click Actions | New Task. The New Task dialog box appears.

2. Ensure that Sensor Deployment is selected, then click OK.

3. Type a name for the task you are creating and add any notes.

4. Select Install, then click Save.

   Select Run at every policy enforcement if needed.
5 Click Menu | Systems | System Tree | Systems, then select the system on which you want to install sensors and click Actions | Agent | Modify Tasks on a single system.

   To install sensors on a group of systems, refer to Configuring the Deployment task for groups of managed systems.

6 Click Actions | New Client Task Assignment. The Client Task Assignment Builder wizard appears.

7 On the Select Task page, select Product as Rogue System Detection and Task Type as Sensor Deployment, then select the task you created for installing sensors.

8 Next to Tags, select the desired platforms to which you are deploying the packages, then click Next:
   - Send this task to all computers
   - Send this task to only computers that have the following criteria — Use one of the edit links to configure the criteria.

9 On the Schedule page, select whether the schedule is enabled, and specify the schedule details, then click Next.

10 Review the summary, then click Save.

### Editing sensor descriptions

Use this task to edit sensor descriptions.

<table>
<thead>
<tr>
<th>This task can be performed from:</th>
<th>Getting there</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rogue System Sensor Details page</td>
<td>Click Menu</td>
</tr>
<tr>
<td>Rogue System Sensor page</td>
<td>Click Menu</td>
</tr>
</tbody>
</table>

For option definitions, click ? in the interface.

#### Task

1 Select the system whose description you want to edit, click Actions | Rogue Sensor | Edit Description.

2 In the Edit Description pane, type the description, then click OK.

### Removing sensors

Use this task to remove sensors from specific systems on your network. This task creates a deployment task that removes the sensor from the selected systems, then performs an immediate agent wake-up call on them.

<table>
<thead>
<tr>
<th>This task can be performed from:</th>
<th>Getting there</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed Systems for Subnet xxx.xxx.xxx.xxx page</td>
<td>Click Menu</td>
</tr>
<tr>
<td>Systems Details page</td>
<td>Click Menu</td>
</tr>
<tr>
<td>Systems page</td>
<td>Click Menu</td>
</tr>
</tbody>
</table>

For option definitions, click ? in the interface.
Task
1 From the Systems page or Systems Details page, select the systems where you want to remove sensors, then click **Actions** | **Rogue Sensor** | **Remove Rogue Sensor**.
   - In the Managed Systems for Subnet xxx.xx.xx.x page, select the systems where you want to remove sensors.
   - In the Systems Details page, select the desired group in the System Tree, then select the systems where you want to remove sensors.
2 In the **Action** pane, click **OK**.

Working with subnets
Use these tasks when working with subnets in Rogue System Detection, for example, adding, including, and deleting subnets.

Tasks
- **Adding subnets on page 284**
  Use this task to add subnets to Rogue System Detection.
- **Deleting subnets on page 285**
  Use this task to delete subnets from Rogue System Detection.
- **Ignoring subnets on page 285**
  Use this task to ignore subnets that you do not want to receive information about.
- **Including subnets on page 285**
  Use this task to include subnets that have previously been ignored by Rogue System Detection. This task can be performed by querying ignored subnets using the steps below, or you can include subnets from the Ignored Subnets page. Click the **Ignored** link in the **Subnet Status** monitor on the Detected Systems page to see the list of ignored subnets, where you can optionally choose to include one or more ignored subnets.
- **Renaming subnets on page 286**
  Use this task to rename subnets.
- **Viewing detected subnets and their details on page 286**
  Use this task to view detected subnets and their details. You can view detected subnets details from any page that displays detected subnets.

Adding subnets
Use this task to add subnets to Rogue System Detection.

For option definitions, click ? in the interface.

Task
1 Click **Menu** | **Systems** | **Detected Systems**, then in the Subnet Status monitor, click **Add Subnet**. The Add Subnets page appears.
2 Choose the method you want to use to add subnets, specify the subnets you want to add, then click **Import**.
Deleting subnets
Use this task to delete subnets from Rogue System Detection.

<table>
<thead>
<tr>
<th>This task can be performed from:</th>
<th>Getting there</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detected Subnets Details page</td>
<td>Click Menu</td>
</tr>
<tr>
<td>Detected Subnets page</td>
<td>Click Menu</td>
</tr>
</tbody>
</table>

For option definitions, click ? in the interface.

Task
1 Select the subnets you want to delete, click Actions, then select Detected Systems | Delete.
2 In the Delete confirmation pane, click Yes.

Ignoring subnets
Use this task to ignore subnets that you do not want to receive information about.

<table>
<thead>
<tr>
<th>This task can be performed from:</th>
<th>Getting there</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detected Subnets Details page</td>
<td>Click Menu</td>
</tr>
<tr>
<td>Detected Subnets page</td>
<td>Click Menu</td>
</tr>
<tr>
<td>Detected Systems page</td>
<td>Click Menu</td>
</tr>
</tbody>
</table>

Ignoring a subnet deletes all detected interfaces associated with that subnet. All further detections on that subnet are also ignored. To view the list of ignored subnets click the Ignore link in the Subnet Status monitor. This link only appears when there are subnets being ignored.

For option definitions, click ? in the interface.

Task
1 Select the subnets you want to ignore, click Actions, then select Detected Systems | Ignore.
2 In the Ignore dialog box, click OK. When ignoring a subnet on the Detected Systems page in the Top 25 Subnets list, a dialog box opens. Click OK.

Including subnets
Use this task to include subnets that have previously been ignored by Rogue System Detection. This task can be performed by querying ignored subnets using the steps below, or you can include subnets from the Ignored Subnets page. Click the Ignored link in the Subnet Status monitor on the Detected Systems page to see the list of ignored subnets, where you can optionally choose to include one or more ignored subnets.

For option definitions, click ? in the interface.
Task
1 Click Menu | Reporting | Queries & Reports, and query for any ignored subnets. For more information on working with queries, see Reporting on System Status.

2 On the Unsaved Queries page, click Include.

3 In the Include dialog box, click OK.

Renaming subnets
Use this task to rename subnets.

<table>
<thead>
<tr>
<th>This task can be performed from:</th>
<th>Getting there</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detected Subnets Details page</td>
<td>Click Menu</td>
</tr>
<tr>
<td>Detected Subnets page</td>
<td>Click Menu</td>
</tr>
</tbody>
</table>

For option definitions, click ? in the interface.

Task
1 Select the subnet you want to rename, then click Actions and select Detected Systems | Rename.

2 In the Rename dialog box, type the new name for the subnet, then click OK.

Viewing detected subnets and their details
Use this task to view detected subnets and their details. You can view detected subnets details from any page that displays detected subnets.

For option definitions, click ? in the interface.

Task
1 Click Menu | Systems | Detected Systems.

2 In the Subnet Status monitor, click any category to view the list of detected subnets it contains, such as Covered. The Detected Subnets page appears and displays the subnets in that category.

3 Click any detected subnet to view its details. The Detected Subnet Details page appears.

Rogue System Detection command-line options
You can run command-line options from the client system. You can start the sensor manually from the command-line instead of starting it as a Windows service. You might want to do this if you are testing functionality, or to check the sensor version. The following table lists the run-time command-line options for the sensor.

<table>
<thead>
<tr>
<th>Switch</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>--console</td>
<td>Forces the sensor to run as a normal command-line executable; otherwise it must be run as an NT service.</td>
</tr>
<tr>
<td>--help</td>
<td>Prints the Help screen and lists available command-line options.</td>
</tr>
<tr>
<td>--install</td>
<td>Registers the sensor with the Windows Service Control Manager.</td>
</tr>
</tbody>
</table>
## Switch Description

<table>
<thead>
<tr>
<th>Switch</th>
<th>Description</th>
</tr>
</thead>
</table>
| **--port**    | Overrides the Server Port configuration setting in the registry that you specified during installation. This parameter takes effect only when running in command-line mode, which also requires the **--console** command-line switch.  
Sample syntax: `sensor.exe --port "8081" --console` |
| **--server**  | Overrides the Server Name configuration setting in the registry that you specified during installation.  
This parameter takes effect only when running in command-line mode, which also requires the **--console** command-line switch.  
Sample syntax: `sensor.exe --server "MyServerName" --console` |
| **--uninstall** | Unregisters the sensor with the Windows Service Control Manager. |
| **--version** | Prints the version of the sensor and exits. |

### Default Rogue System Detection queries

Rogue System Detection provides default queries that you can use to retrieve specific information from your network. These queries can be modified or duplicated in the same manner as other queries in ePolicy Orchestrator. You can also create custom queries, display query results in dashboard monitors, and add those dashboard monitors to the Dashboards section in ePolicy Orchestrator.

For more information on using dashboards, see [Assessing Your Environment With Dashboards](#).

#### Rogue System Detection query definitions

<table>
<thead>
<tr>
<th>Query</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Sensor Response (Last 24 Hours)</td>
<td>Returns the details of active sensors installed on your network in the last 24 hours, in pie chart format.</td>
</tr>
<tr>
<td>Passive Sensor Response (Last 24 Hours)</td>
<td>Returns the details of passive sensors installed on your network in the last 24 hours, in pie chart format.</td>
</tr>
<tr>
<td>Rogue Systems, By Domain (Last 7 Days)</td>
<td>Returns the details of systems detected on your network as rogue systems in the last seven days, grouped by domain, in table format.</td>
</tr>
<tr>
<td>Rogue Systems, By OS (Last 7 Days)</td>
<td>Returns the details of systems detected on your network as rogue systems in the last seven days, grouped by operating system, in pie chart format.</td>
</tr>
<tr>
<td>Rogue Systems, By OUI (Last 7 Days)</td>
<td>Returns the details of systems detected on your network as rogue systems in the last seven days, grouped by organizationally unique identifier, in pie chart format.</td>
</tr>
<tr>
<td>Subnet Coverage</td>
<td>Returns the details of detected subnets on your network, in pie chart format.</td>
</tr>
</tbody>
</table>
Managing Issues and Tickets

The Issues feature of ePolicy Orchestrator software allows you to create, modify, assign, and track issues. Issues are action items that can be prioritized, assigned, and tracked.

**Issues**

Users can create basic issues manually or the McAfee ePO server can automatically create issues in response to product events. For example, users with the proper permissions can configure ePolicy Orchestrator to automatically create a Benchmark Rule Compliance issue if a noncompliant system is discovered during an audit.

**Tickets**

A ticket is the external equivalent of an issue that exists in a ticketing server. Once a ticket is added to an issue, the issue is referred to as a "ticketed issue." A ticketed issue can have only one associated ticket.

**Integrating issues with third-party ticketing servers**

Integration of a ticketing server forces the creation of tickets associated with issues that were created in products. ePolicy Orchestrator supports these ticketing servers:

- Hewlett-Packard Openview Service Desk versions 4.5 and 5.1 — an integrated help desk and trouble ticketing solution.
- BMC Remedy Action Request System versions 6.3 and 7.0 — a consolidated platform for automating and managing trouble tickets.

**Contents**

- Issues and how they work
- Working with issues
- Purging closed issues
- Tickets and how they work
- Integration with ticketing servers
- Working with tickets
- Working with ticketing servers
- Upgrading a registered ticketing server
Issues and how they work

The way issues are managed is defined by users with proper permissions and the installed managed product extensions.

An issue's state, priority, severity, resolution, assignee, and due date are all user-defined, and can be changed at any time. You can also specify default issue responses from the Automatic Responses page. These defaults are automatically applied when an issue is created, based on a user-configured response. Responses also allow multiple events to be aggregated into a single issue so that the McAfee ePO server is not overwhelmed with large numbers of issues.

Issues can be deleted manually, and closed issues can be manually purged based on their age and automatically purged through a user-configured server task.

Working with issues

You can create, assign, view details of, edit, delete, and purge issues.

Tasks

- Creating basic issues manually on page 290
  Basic issues can be created manually. Non-basic issues must be created automatically.
- Configuring responses to automatically create issues on page 291
  You can use responses to automatically create issues when certain events occur.
- Managing issues on page 294
  You can add comments, assign, delete, edit, and view details of issues.

Creating basic issues manually

Basic issues can be created manually. Non-basic issues must be created automatically.

Task

For option definitions, click ? in the interface.

1. Click Menu | Automation | Issues, then click Actions | New Issue.

2. In the New Issue dialog box, select Basic from the Create issue of type drop-down list, then click OK.

3. Configure the new issue.

<table>
<thead>
<tr>
<th>Use this...</th>
<th>To do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a meaningful name for the issue.</td>
</tr>
<tr>
<td>Description</td>
<td>Type a meaningful description of the issue.</td>
</tr>
<tr>
<td>State</td>
<td>Assign a state to the issue:</td>
</tr>
<tr>
<td></td>
<td>• Unknown</td>
</tr>
<tr>
<td></td>
<td>• New</td>
</tr>
<tr>
<td></td>
<td>• Assign</td>
</tr>
<tr>
<td></td>
<td>• Resolved</td>
</tr>
<tr>
<td></td>
<td>• Closed</td>
</tr>
</tbody>
</table>
Use this... | To do this...
---|---
**Priority** | Assign a priority to the issue:
- Unknown
- Lowest
- Low
- Medium
- High
- Highest

**Severity** | Assign a severity to the issue:
- Unknown
- Lowest
- Low
- Medium
- High
- Highest

**Resolution** | Assign a resolution to the issue. The issue resolution can be assigned once the issue is processed:
- None
- Fixed
- Waived
- Will not fix

**Assignee** | Type the user name of the person assigned to the issue, or choose them by clicking ...

**Due Date** | Select whether the issue has a due date and, if so, assign a date and time that the issue is due. Due dates in the past are not allowed.

4 Click Save.

**Configuring responses to automatically create issues**
You can use responses to automatically create issues when certain events occur.

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

1 Click **Menu | Automation | Automatic Responses**, then click **Actions** and select **New Response**. The **Description** page of the **Response Builder** appears.

---

<table>
<thead>
<tr>
<th>Use this...</th>
<th>To do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Type a meaningful name for the response.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Type a description of the response.</td>
</tr>
<tr>
<td><strong>Language</strong></td>
<td>Select the language in which the response will appear.</td>
</tr>
</tbody>
</table>
Use this... | To do this...
---|---
Event<br>• Event group — Select an event group, such as ePO Notification Events.<br>• Event type — Select an event type that is part of the event group, such as Server.<br>Status | Enable or disable the response.

2 Click Next.

3 Select properties to narrow the events that trigger the response, then click Next.

4 Next to Aggregation, select one:<br>• Trigger this response for every event — generates a response for every event.<br>• Trigger this response if multiple events occur within — generates a response for multiple events that occur during a specified time period and, if needed, after a certain number of events have occurred or a certain property accumulates a specified number of distinct values.

5 Next to Grouping, select one:<br>• Do not group aggregated events — events of the same type are not aggregated.<br>• Group aggregated events by — a property of the event. For example, if you narrow your events by audit, you can aggregate events that are noncompliant with the audit.

6 Next to Throttling, select the maximum time period that you want this response to occur.

7 Click Next.

8 Select Create issue from the drop-down list, then select the type of issue to create. This choice determines the options that appear on this page.
9 Type a name and description for the issue. Optionally, select one or more variables for the name and description. This feature provides an number of variables providing information to help fix the issue.

10 If applicable, type or select the appropriate option.

<table>
<thead>
<tr>
<th>Use this...</th>
<th>To do this...</th>
</tr>
</thead>
</table>
| State       | Assign a state to the issue:  
• Unknown   
• New       
• Assigned  
• Resolved  
• Closed    |
| Priority    | Assign a priority to the issue:  
• Unknown    
• Lowest    
• Low        
• Medium   
• High    
• Highest |
Use this... | To do this...
--- | ---
Severity | Assign a severity to the issue:
• Unknown
• Lowest
• Low
• Medium
• High
• Highest
Resolution | Assign a resolution to the issue. The issue resolution can be assigned once the issue is processed:
• None
• Fixed
• Waived
• Will not fix
Assignee | Type the user name of the person assigned to the issue or choose them by clicking ...

11 Click Next.

12 Review the details for the response, then click Save.

Managing issues
You can add comments, assign, delete, edit, and view details of issues.

Task
For option definitions, click ? in the interface.

1 Click Menu | Automation | Issues,

2 Perform the tasks that you want.

<table>
<thead>
<tr>
<th>Task</th>
<th>Do this...</th>
</tr>
</thead>
</table>
| Adding comments to issues | 1 Select the checkbox next to each issue you want to comment, then click Action | Add comment.  
2 In the Add comment panel, type the comment you want to add to the selected issues.  
3 Click OK to add the comment. |
| Adding tickets to issues | Select the checkbox next to each issue you want to add ticket, then click Action | Add ticket. |
| Assigning issues | Select the checkbox next to each issue you want to assign, then click Assign to user. |
| Display required columns on Issues page | Click Actions | Choose Columns. Select columns of data to be displayed on the Issues page. |
### Purging closed issues

These tasks purge closed issues from the database. Purging closed issues deletes them permanently. Purging a closed ticketing issue deletes the issue, but the associated ticket remains in the ticketing server database.

**Tasks**
- Purging closed issues manually on page 295
  - Periodically purging closed issues from the database keeps it from getting too full.
- Purging closed issues on a schedule on page 295
  - You can schedule a task to periodically purge the database of closed issues. This keeps the database smaller.

### Purging closed issues manually

Periodically purging closed issues from the database keeps it from getting too full.

**Task**

For option definitions, click ? in the interface.

1. Click Menu | Automation | Issues, then click Actions | Purge.
2. In the Purge dialog box, type a number, then select a time unit.
3. Click OK to purge closed issues older than the specified date.

   **Tip:** This function affects all closed issues; not just those in the current view.

### Purging closed issues on a schedule

You can schedule a task to periodically purge the database of closed issues. This keeps the database smaller.

<table>
<thead>
<tr>
<th>Task</th>
<th>Do this...</th>
</tr>
</thead>
</table>
| Deleting issues     | 1. Select the checkbox next to each issue you want to delete, then click Delete.  
                       2. Click OK in the Action to delete the selected issues.          |
| Editing issues      | 1. Select the checkbox next to an issue, then click Edit.              
                       2. Edit the issue as needed.                                 
                       3. Click Save.                                                |
| Exporting the list  | Click Actions | Export Table. Opens the Export page. From the Export page you can specify the format of files to be exported, as well as how they are packaged (For example, in a zip file), and what to do with the files (For example, Email them as an attachment). |
| of issues           |                                                           |
| Viewing issue       | Click an issue.                                                          
                       The Issue Details page appears. This page shows all of the settings for the issue as well as the Issues Activity Log. |
| details             |                                                           |
**Task**
For option definitions, click ? in the interface.

1. Click **Menu | Automation | Server Tasks**, then click **Actions | New Task**.
2. Type a name and description for the server task.
3. Enable or disable the schedule for the server task.
   The server task does not run until it is enabled.
4. Click **Next**.
   The **Actions** page appears.
5. From the drop-down list, select **Purge Closed Issues**.
6. Type a number, then select a time unit.
7. Click **Next**.
8. Schedule the server task, then click **Next**.
9. Review the details of the server task, then click **Save**.

The closed issues are purged at the time of the scheduled task.

---

**Tickets and how they work**

A ticket is the external equivalent of an issue that exists in a ticketing server. Once a ticket is added to an issue, the issue is referred to as a "ticketed issue."

**Ways to add tickets to issues**

A ticket can be added to an issue manually or automatically. A ticketed issue can have only one associated ticket.

When a ticket is added to an issue, the state of the resulting ticketed issue is changed to Ticketed, regardless of the issue's status prior to being ticketed. When the ticket is created in the ticketing server, that ticket's ID is added to the ticketed issue. The ticket ID creates the ticket-to-issue association.

After the steps for integrating a ticketing server are completed, all subsequent issues are ticketed automatically. McAfee recommends always adding an assignee to an issue before the ticket is created. If an assignee is added manually to a ticketed issue, you must add tickets manually to any issues that existed prior to the integration.

**Assignment of ticketed issues to users**

Adding an assignee manually to a ticketed issue is considered editing an issue, which breaks the issue-to-ticket association. Do this by specifying an assignee in the response, which creates issues. In this way, an assignee is added to the issue automatically when it is created.

For details, see *How tickets and ticketed issues are closed*.

**How tickets and ticketed issues are closed**

Ticketed issues are closed automatically by the system when the server task, which synchronizes ticketed issues, runs. This server task identifies tickets that changed to the Closed state since the last time the task ran. The status of a ticketed issue associated with a closed ticket is then changed to
Closed. Also, that ticket's comments replace the comments in the ticketed issue if the integration of the ticketing server was configured to overwrite ticketed issue comments. 

For details see Benefits of adding comments to ticketed issues.

Benefits of adding comments to ticketed issues

When a comment is added to a ticketed issue, it is added to the associated ticket immediately or the next time the Issue Synchronization server task runs. Ticketed issue comments are added only to tickets that are not in the Closed state.

If the ticketing server allows issue comments to be overwritten by ticket comments, when a ticket's state becomes Closed, comments for that ticket replace all comments in the associated ticketed issue. This process is performed when the server task, which synchronizes ticketed issues, identifies a ticket whose state changed to Closed since the last time the task was run. This task is performed only once for each closed ticket. Allowing issue comments to be overwritten by ticket comments can allow users with access to the system (but not to the ticketing server) the ability to see what happened to the ticket.

How tickets are reopened

A ticket is reopened when it is added to a previously added ticketed issue, whose ID can be matched to a ticket in the ticketing server. If the ID cannot be matched, a new ticket is created. Reopening a ticket does not reopen the associated ticket issue.

The configuration mapping for the ticketing server must also be configured to allow tickets to be reopened. See Required fields for mapping.

Ticketed issue synchronization

The Issues feature includes the Issue Synchronization server task, which synchronizes ticketed issues with their associated tickets in the ticketing server. This server task is disabled by default; it will not run until enabled.

When this server task runs, the system attempts to:

- Change the status of ticketed issues from Ticketed to Closed if the state of their associated tickets is closed.
- Create tickets for issues or add comments to tickets that the system was unable to create or add previously. For example, if a communication error occurred when the tickets or the comments were first added.
- Replace the comments of a ticketed issue with the comments of its associated ticket if the ticket's state is Closed, and the integration of the ticketing server was configured to overwrite ticketed issue comments.
- Change the state of each ticketed issue to Assigned if the ticketed issue does not have an assignee specified, or New if the registered server for the ticketing server is deleted.

Integration with ticketing servers

Integration of a ticketing server forces the creation of tickets associated with issues that were created in products.

The ePolicy Orchestrator software supports these ticketing servers:
• Hewlett-Packard Openview Service Desk versions 4.5 and 5.1 — an integrated help desk and trouble ticketing solution.
• BMC Remedy Action Request System versions 6.3 and 7.0 — a consolidated platform for automating and managing trouble tickets.

The person who performs this integration should be familiar with the ticketing server and its fields and forms. Integrating a ticketing server consists of these basic steps:

1. Configure ePolicy Orchestrator to integrate with the ticketing server.
   - The system running the ticketing extension must be able to resolve the address of the Hewlett-Packard Openview Service Desk system. This might involve adding the IP address of the Service Desk system to the hosts file on the system running the ticketing extension, or setting up a domain trust between the two systems. See Configuring the DNS for Service Desk 4.5.

2. Integrate a ticketing server with ePolicy Orchestrator. Only one registered ticketing server can be integrated with ePolicy Orchestrator.

3. Configure the field mappings between issues and tickets.

Considerations when deleting a registered ticketing server

There might be times when you want to delete the registered server for your ticketing server. For example, if you upgrade your ticketing server.

When the registered server is deleted, the system changes the state of each ticketed issue to Assigned, or to New if the ticketed issue does not have a specified assignee, the next time the Issue synchronization server task is run. This is why it is important to disable scheduling for that server task if you are upgrading the ticketing server. For more details, see Upgrading a registered ticketing server.

When the registered ticketing server is deleted, the ticket ID that associated the ticket to the ticketed issue remains with that ticketed issue. This allows the ticket to be reopened if the issue-to-ticket association is broken. For example, if the server task runs before the upgraded server is registered. See How tickets are reopened.

Required fields for mapping

Mapping is the process by which information in issues is mapped to information in tickets. Each piece of information is called a field, and the fields in issues need to be mapped to corresponding fields in tickets.

To determine which ticket fields must be mapped, review the fields required to create a ticket on the ticketing form in the ticketing server. For information about which fields are required, see the documentation for your ticketing server.

For the system to know when to close ticketed issues, the field with the ticket's state must be mapped.

Sample mappings

When you register your ticketing server, you must also configure the field mappings for issues and tickets. The field mappings in the following examples are provided for reference only. Your mappings will vary based on the fields required in your ticketing server and the values those fields accept.

Mapping is a two-way process. These examples demonstrate how to map an issue to a ticket and to map the ticket's status back to the issue's status. For example, if the ticket is marked as closed, the issue status will be updated to show that it is closed.
Sample mapping for Hewlett-Packard Openview Service Desk
This is a reference-only sample mapping for Hewlett-Packard Openview Service Desk versions 4.5 and 5.1.

Source values, mapped values, and field IDs are case-sensitive.

Map Issue to Ticket

- **Ticket form**: Default_Problem

- **Ticket field**: Description
  - **Operation**: Identity
  - **Source field**: Name

- **Ticket field**: Status
  - **Operation**: Substitution
  - **Source field**: State
  - **Values**: Default Value: 10

<table>
<thead>
<tr>
<th>Source Value</th>
<th>Mapped Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEW</td>
<td>10</td>
</tr>
<tr>
<td>RESOLVED</td>
<td>20</td>
</tr>
<tr>
<td>UNKNOWN</td>
<td>20</td>
</tr>
<tr>
<td>ASSIGNED</td>
<td>20</td>
</tr>
</tbody>
</table>

- **Ticket field**: Information
  - **Operation**: Identity
  - **Source field**: Description

- **Ticket field**: HistoryLines
  - **Operation**: Identity
  - **Source field**: Activity Log

- **Ticket field**: Type the name or ID for any open text field.
  - **Operation**: Identity
  - **Source field**: URL

Map Ticket back to Issue Status field

Because this section only maps the ticket’s status, you are not prompted to add the ID of the issue’s status field. This field is implied.

- **Operation**: Substitution

- **Source field**: Status

- **Values**: Default Value: TICKETED

<table>
<thead>
<tr>
<th>Source Value</th>
<th>Mapped Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>40</td>
<td>CLOSED</td>
</tr>
</tbody>
</table>
• Overwrite issue comments with ticket comments: selected
• Ticket Comment field: HistoryLines
• Tickets can be re-opened: selected

Sample mapping for BMC Remedy Action Request System
This is a reference-only sample mapping for BMC Remedy Action Request System versions 6.3 and 7.0.

Source values, mapped values, and field IDs are case-sensitive.

Map Issue to Ticket
• Ticket form: Help Desk
• Ticket field: 8
  • Operation: Identity
  • Source field: Name
• Ticket field: 7
  • Operation: Substitution
  • Source field: State
  • Values: Default Value: 0

<table>
<thead>
<tr>
<th>Source Value</th>
<th>Mapped Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NEW</td>
<td>0</td>
</tr>
<tr>
<td>RESOLVED</td>
<td>2</td>
</tr>
<tr>
<td>ASSIGNED</td>
<td>1</td>
</tr>
</tbody>
</table>

• Ticket field: 2
  • Operation: Custom Mapping
  • Source field: Type the user name for the ticketing server. This is the same user name provided for Authentication on the Description page of the Registered Server Builder.

• Ticket field: 200000004
  • Operation: Custom Mapping
  • Source field: External

In this example, "External" specifies that the ticket was created by a product external to the ticketing server. You can type the name of the product instead, to indicate which product created the ticket.
Ticket field: 240000008

Ticketing systems can have multiple comment or diary fields. Make sure to choose the one you want used for this integration. If a comment field is not mapped, ticketed issue comments cannot be added to tickets.

Operation: Identity
Source field: Activity Log
Ticket field: Type the name or ID for any open text field.
Operation: Identity
Source field: URL

Map Ticket back to Issue Status field

Because this section only maps the ticket's status, you are not prompted to add the ID of the issue's status field. This field is implied.

Operation: Substitution
Source field: 7
Values: Default Value: 0

<table>
<thead>
<tr>
<th>Source Value</th>
<th>Mapped Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>CLOSED</td>
</tr>
</tbody>
</table>

Overwrite issue comments with ticket comments: selected
Ticket Comment field: 240000008
Tickets can be re-opened: selected

Working with tickets

You can add tickets to issues and synchronize ticketed issues with the Issue Synchronization server task.

Tasks

- *Adding tickets to issues on page 301*
  You can add a ticket to a single issue, or to multiple issues at once.
- *Synchronizing ticketed issues on page 302*
  The Issue synchronization server task updates ticketed issues and their associated tickets in the ticketing server.
- *Synchronizing ticketed issues on a schedule on page 302*
  The Issue synchronization server task updates ticketed issues and their associated tickets in the ticketing server. Use this task to configure the Issue synchronization server task to run on a schedule.

Adding tickets to issues

You can add a ticket to a single issue, or to multiple issues at once.

A ticket can be added in a similar way when viewing the details of an issue. When a ticket is added, a new ticket is created automatically in the ticketing server. Issues with existing tickets are ignored.
Task
For option definitions, click ? in the interface.

1. Click Menu | Automation | Issues, select the checkbox next to each issue, then click Actions | Add ticket.

2. In the Add Ticket panel, click OK to add a ticket to each selected issue.

Synchronizing ticketed issues
The Issue synchronization server task updates ticketed issues and their associated tickets in the ticketing server.

Task
For option definitions, click ? in the interface.

1. Click Menu | Automation | Server Tasks.

2. Click Run next to the Issue synchronization task.

3. Review the results of the server task.
   For more details, see the section in this guide about the server task log.

Synchronizing ticketed issues on a schedule
The Issue synchronization server task updates ticketed issues and their associated tickets in the ticketing server. Use this task to configure the Issue synchronization server task to run on a schedule.

- The schedule for the Issue synchronization server task is disabled by default.

Task
For option definitions, click ? in the interface.

1. Click Menu | Automation | Server Tasks, then click Edit in the Actions column for the Issue synchronization task.

2. Select Enable next to Schedule status.
   If you disable the schedule, the server task will not run on a schedule, but you can still run it manually.

3. Click Next.

4. In the Actions tab, click Next.

5. Schedule the server task as needed, then click Next.

6. Review the details of the server task, then click Save.

Working with ticketing servers
These tasks integrate your ticketing server with ePolicy Orchestrator.
Tasks

- **Installing extensions for ticketing server on page 303**
  You must integrate your ticketing system with ePolicy Orchestrator before you can issue tickets. The files that you copy to ePolicy Orchestrator depend on your ticketing system.

- **Registering and mapping a ticketing server on page 305**
  Use these tasks to register and map a ticketing server. You must complete these tasks before tickets can be added to issues. Only one registered ticketing server can exist at a time.

- **Configuring the field mappings on page 306**
  You must configure the field mappings for a ticketing server before you can associate tickets to issues.

Installing extensions for ticketing server

You must integrate your ticketing system with ePolicy Orchestrator before you can issue tickets. The files that you copy to ePolicy Orchestrator depend on your ticketing system.

Task

1. Go to **Start** | **Control Panel** | **Administrative Tools**, then double-click **Services**.

2. In the **Name** column, double-click **McAfee Policy Auditor Application Server**.

3. Select the **General** tab.

4. Under **Service status**, click **Stop**.
   The server is now stopped.

5. Copy the required files for your ticketing server, then repeat steps 1-3.

6. Under **Service status**, click **Start**.
   The server is now running.

Tasks

- **Stopping and starting the server on page 303**
  You must stop an ePolicy Orchestrator server before you can copy the files required by the ticketing server. After the files are copied, start the server.

- **Copying the Hewlett-Packard Openview Service Desk files on page 304**
  Before you can use the Hewlett-Packard Openview Service Desk (Service Desk) 5.1 or 4.5 extension, you must copy certain files. For information about these files, see your Service Desk documentation.

- **Copying the BMC Remedy Action Request System files on page 304**
  Before you can use BMC Remedy Action Request System (Remedy) extension, you must copy certain files. For information about these files, see your Remedy documentation. The Remedy extension includes support for the Remedy 6.3 and 7.0 servers.

- **Installing the ticketing server extensions on page 305**
  You must install the ticketing server extensions before you can integrate them into the ePolicy Orchestrator ticketing system.

Stopping and starting the server

You must stop an ePolicy Orchestrator server before you can copy the files required by the ticketing server. After the files are copied, start the server.
Task
1 In Windows, click Start | Control Panel | Administrative Tools, then double-click Services.
2 In the Name column, locate then double-click McAfee Policy Auditor Application Server.
3 Select the General tab.
4 Under Service status, click Stop.
   The server is now stopped.
5 Copy the required files for your ticketing server, then repeat steps 1-3.
6 Under Service status, click Start.
   The server is now running.

Copying the Hewlett-Packard Openview Service Desk files
Before you can use the Hewlett-Packard Openview Service Desk (Service Desk) 5.1 or 4.5 extension, you must copy certain files. For information about these files, see your Service Desk documentation.

• Copy the required files to the Server\common\lib folder of your ePolicy Orchestrator software installation.
  For example, C:\Program Files\McAfee\ePolicy Orchestrator\Server\common\bin.

Copying the BMC Remedy Action Request System files
Before you can use BMC Remedy Action Request System (Remedy) extension, you must copy certain files. For information about these files, see your Remedy documentation. The Remedy extension includes support for the Remedy 6.3 and 7.0 servers.

You can use the Remedy 5.1 or 7.0 API files for the Remedy extension. McAfee does not support an integration with the Remedy 5.1 server, but the 5.1 API files will work for integrations with the Remedy 6.3 or 7.0 servers. The Remedy 6.3 API files are not supported.
Task

1 Copy the following required files to the \Server\bin folder of your ePolicy Orchestrator software installation. For example, C:\Program Files\McAfee\ePolicy Orchestrator\Server\bin.

<table>
<thead>
<tr>
<th>Remedy API Version</th>
<th>Required Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remedy 5.1</td>
<td>arapi51.dll</td>
</tr>
<tr>
<td></td>
<td>arjni51.dll</td>
</tr>
<tr>
<td></td>
<td>arrpc51.dll</td>
</tr>
<tr>
<td></td>
<td>arutil51.dll</td>
</tr>
<tr>
<td>Remedy 7.0</td>
<td>arapi70.dll</td>
</tr>
<tr>
<td></td>
<td>arutiljn70.dll</td>
</tr>
<tr>
<td></td>
<td>icudt32.dll</td>
</tr>
<tr>
<td></td>
<td>icuin32.dll</td>
</tr>
<tr>
<td></td>
<td>icuuc32.dll</td>
</tr>
<tr>
<td></td>
<td>arutil70.dll</td>
</tr>
</tbody>
</table>

2 Copy the following required files to the Server\common\lib folder of your ePolicy Orchestrator installation. For example, C:\Program Files\McAfee\ePolicy Orchestrator\Server\common\lib.

<table>
<thead>
<tr>
<th>Remedy API Version</th>
<th>Required Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remedy 5.1</td>
<td>arapi51.jar</td>
</tr>
<tr>
<td></td>
<td>arutil51.jar</td>
</tr>
<tr>
<td>Remedy 7.0</td>
<td>arapi70.jar</td>
</tr>
<tr>
<td></td>
<td>arutil70.jar</td>
</tr>
</tbody>
</table>

Installing the ticketing server extensions

You must install the ticketing server extensions before you can integrate them into the ePolicy Orchestrator ticketing system.

Task

For option definitions, click ? in the interface.

1 Click Menu | Software | Extensions, then click Install Extension.

2 Browse to the InstallDir\ePolicy Orchestrator\Installer\Core\Extensions folder and select the desired extension (zip) file. Extensions for BMC Remedy 6.3 and 7.0, and Hewlett-Packard Openview Service Desk versions 4.5 and 5.1 are included with ePolicy Orchestrator.

3 Click OK.

Registering and mapping a ticketing server

Use these tasks to register and map a ticketing server. You must complete these tasks before tickets can be added to issues. Only one registered ticketing server can exist at a time.
Tasks

- **Configuring the DNS for Hewlett-Packard Openview Service Desk 4.5 on page 306**
  Before you can integrate with Service Desk 4.5, you must configure the server information.

- **Registering a ticketing server on page 306**
  You must register a ticketing server before tickets can be associated with issues.

**Configuring the DNS for Hewlett-Packard Openview Service Desk 4.5**
Before you can integrate with Service Desk 4.5, you must configure the server information.

The system running the ticketing extension must be able to resolve the address of the Service Desk system.

**Task**

1. On the McAfee ePO server that is integrated with the ticketing system, use a text order to open the hosts file.
   The hosts file should be located in the `c:\windows\system32\drivers\etc\` folder.

2. Edit the hosts file to include the IP address of the system running Service Desk 4.5, followed by a space, followed by the DNS suffix (the name of the system on which Service Desk 4.5 is running). For example, `168.212.226.204 SRVDSK45.qaad.com`.

3. Save and close the hosts file.

4. Restart the McAfee ePO server.

**Registering a ticketing server**
You must register a ticketing server before tickets can be associated with issues.

**Task**

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

1. Click `Menu | Configuration | Registered Servers`, then click `New Server`.

2. Select the server type for your ticketing server.
   This choice determines the options available on subsequent pages of the builder.

3. Type a name and description, then click `Next`.

4. Type the host for the server.

5. Type the port, user name, and password for the server.

6. If Service Desk 4.5 or 5.1 was selected, select a `Workflow`.

**Configuring the field mappings**
You must configure the field mappings for a ticketing server before you can associate tickets to issues.

**Tasks**

- **Mapping issues to tickets on page 307**
  Configuring the field mapping from the issue to the ticket keeps your data synchronized when using a ticketing server.

- **Mapping tickets back to issue status on page 307**
  You need to configure field mapping from the ticket back to the issue’s status, or state, field to fully integrate the ticketing server.
Mapping issues to tickets
Configuring the field mapping from the issue to the ticket keeps your data synchronized when using a ticketing server.

Source values, mapped values, and field IDs are case-sensitive.

Task
For option definitions, click ? in the interface.

1 Next to Configure mapping, click Configure.

2 Select the options from the Mapping Options pane as needed.
   Selected options appear in the Mapping Definitions pane with operators to specify how an issue should be mapped to a ticket, and how a ticket should be mapped back to an issue. Both mappings must be completed.

3 Under Map Issue to Ticket, type the name of a Ticket form.

4 Type a Ticket field ID.

5 Select an Operation.

6 Do one of the following:
   - If Substitution is selected, select an issue field in the Source field drop-down list, then click Edit next to Values. The Edit Substitution Mapping dialog box appears.
     1 Type a Default Value that should be substituted if a source value, which is not mapped, is returned.
     2 Type a Source Value for the issue, then type the Mapped Value that should be substituted for this value in the ticket.
     3 Click + to map another value.
     4 When finished, click OK.
   - If Numeric Range is selected, select an issue field to map in the Source field drop-down list, then click Edit next to Values. The Edit Numeric Range Mapping dialog box appears.
     1 Type a Default Value that should be substituted if a source range that is not mapped is returned.
     2 Type the Source Range for the issue, then type the Mapped Value that should be substituted for this range in the ticket.
     3 Click + to map another value.
     4 When finished, click OK.
   - If Custom Mapping is selected, type the Value that should be added to the ticket.

7 Click + to map another ticket field.

Mapping tickets back to issue status
You need to configure field mapping from the ticket back to the issue's status, or state, field to fully integrate the ticketing server.

Because this section only maps the ticket's state/status, you are not prompted to add the ID of the issue's status (state) field. This field is implied.

Source values, mapped values, and field IDs are case-sensitive.
Task
For option definitions, click ? in the interface.

1 Under Map Ticket back to Issue Status field, select an Operation.

2 In the Source field, type the ID of the ticket field that contains the state/status of the ticket.

3 If Numeric Range or Substitution is selected for the Operation, click Edit next to Values.
   • If Numeric Range is selected, type a range of Ticket Values for the ticket, then type the Label that is substituted for this range in the issue.
   • If Substitution is selected, type a Source Value for the ticket, then type the Mapped Value that is substituted for this value in the issue.

4 Select Overwrite issue comments with ticket comments if you want issue comments to take precedence, then type the ID of the Ticket comment field that overwrites the data in the issue's comment field.

5 Select Tickets can be re-opened if you want that ability.

6 When finished, click Test Mapping.
   If the test is successful, a ticket ID appears in a dialog box. This is the ID for a test ticket which was created in your ticketing server.

7 Do one of the following:
   • If the test was successful, locate the ticket in your ticketing server, and verify that all the values for the basic issue type are mapped correctly, including the test's comments. Then click OK.

   *The test mapping function verifies the mapping for the basic issue type, regardless of the issue type configured. Therefore, testing the mapping for issue types from other product extensions (extended issue types) can be successful per the basic mapping test, but you might see unexpected results in the tickets. For these issue types, verify that tickets added to issues after your ticketing server is fully integrated are created correctly.*

   • If the test was unsuccessful, review your mappings and the status of the ticketing server.

8 When finished testing the mapping, click Save.
   *You can save the configuration and register the server even if the mapping test fails.*

9 When finished, click Save.

Upgrading a registered ticketing server
If you upgrade your ticketing server, you might need to modify the integration of the existing ticketing server for it to continue working.

If the server task, which synchronizes ticketed issues, runs after the existing registered ticketing server is modified or deleted, but before the upgraded ticketing server is integrated, the issue-to-ticket association is broken. If this occurs, complete this task, then manually add tickets to all previously ticketed issues. This causes the reopen function to run. For more details, see the section in this guide about how tickets are reopened.
**Task**

1. Do the following to disable the server task, which synchronizes ticketed issues.
   a. Click *Menu* | *Automation* | *Server Tasks*, then click the issue synchronization server task. The Description page of the Server Task Builder appears.
   b. Select **Disable** next to **Schedule status**.
   c. Click **Save**.

2. Ensure that no instances of the server task are running. If an instance is running, wait for it to complete or cancel it before continuing.

3. Do one of the following:
   - Edit the existing registered ticketing server based on the configuration requirements for the upgraded ticketing server.
   - Delete the existing registered ticketing server, then create a new one based on the configuration requirements for the upgraded ticketing server.

   For more details, see the sections in this guide about integrating ticketing servers, installing ticketing server extensions, and registering and configuring a ticketing server.

4. After you have configured the integration with the upgraded ticketing server, enable the server task, which synchronizes ticketed issues.
Appendix: Maintaining ePolicy Orchestrator Databases

Your databases require regular maintenance to promote optimal performance and to protect your data. Use the Microsoft management tool appropriate for your version of SQL:

<table>
<thead>
<tr>
<th>SQL Version</th>
<th>Management Tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL 2005</td>
<td>SQL Server Enterprise Manager</td>
</tr>
<tr>
<td>SQL 2008</td>
<td>SQL Server Management Studio</td>
</tr>
<tr>
<td>SQL Express</td>
<td>SQL Server Management Studio Express</td>
</tr>
</tbody>
</table>

Depending on your deployment of McAfee ePO software, plan on spending a few hours each week on regular database backups and maintenance. The tasks discussed in this section should be performed on a regular basis, either weekly or daily. However, these are not the only maintenance tasks available. See your SQL documentation for details on what else you can do to maintain your database.

Contents
- Perform regular maintenance of SQL Server databases
- Backup and restore ePolicy Orchestrator databases
- Changing SQL Server information

Perform regular maintenance of SQL Server databases

There are two modes available for maintaining your Microsoft SQL Server (SQL Server) databases: Simple Recovery Mode and Full Recovery Mode.

When SQL Server backs up the ePolicy Orchestrator server in simple recovery mode, it marks the backed-up transaction log records as inactive; also known as truncating the log. In this way, new operations written to the transaction log can reuse that space by overwriting the inactive entries. This helps prevent the log size from growing.

In full recovery mode, if the transaction log is not periodically backed up, it continues to grow. The transaction log will grow until it consumes all available disk space. Therefore, it is important to perform regular transaction log backups when using full recovery mode to keep the size of the transaction log in check.

In simple recovery mode, SQL Server truncates the transaction log when a check point occurs, and records are flushed to disk. This frees up space internal to the transaction log file. The transaction log therefore does not grow in size to any meaningful extent, as long as there is enough space available for the current open transactions. This means that in simple recovery mode, there is no need to back up the transaction log, just a regular full backup of the ePolicy Orchestrator database. In the event of a disaster, you can only recover to the last full backup. All changes that occurred since the last full backup are lost.
For most enterprise customers, using simple recovery mode is an acceptable solution as the most typical data lost in the event of a disaster is event information. Using full recovery mode adds the administrative overhead of periodically backing up the transaction log, as well as the ePolicy Orchestrator database.

Primarily for this reason, McAfee recommends using simple recovery mode for the ePolicy Orchestrator database.

If you use full recovery mode, ensure you have a good backup plan for both your ePolicy Orchestrator database and transaction log. A discussion of SQL Server database backup plans is beyond the scope of this guide. For more details, please refer to the Microsoft SQL Server documentation.

**Backup and restore ePolicy Orchestrator databases**

McAfee recommends that you back up ePolicy Orchestrator databases regularly to protect your data and guard against hardware and software failure. If you ever need to reinstall the server, you might need to restore from a backup.

How often you back up depends on how much of your data you are willing to risk. Some possible approaches include:

- Back up your database at least once a week.
- If you have made many changes to your deployment, you might want to back up daily.
- To mitigate bandwidth demands during regular business hours, you might schedule automated nightly backups.
- To further balance the load, you might perform incremental daily or nightly backups, and a full weekly backup each week.

Save the backup copy to a different server than the one hosting your live database. If your database server crashes, you don’t want to lose your backup too.

Performing regular backups provides the ability to restore your database if that should ever become necessary because of software or hardware failure, or because of an upgrade to server or database server hardware.

For information on backing up and restoring your SQL database, see:

- Microsoft documentation for the management tool appropriate for the database you are using.
- McAfee KnowledgeBase article KB52126.

**Changing SQL Server information**

Use this task to edit the SQL Server connection configuration details.

This is useful to make changes to the user account information in ePolicy Orchestrator when you make changes to the SQL Server authentication modes in SQL Server Enterprise Manager or SQL Server Management Studio. Do this if you need to use a privileged SQL user account for added network security.

Changing the database settings to point this McAfee ePO server to an McAfee ePO database that is not an exact match can cause the removal of product extensions and the loss of all associated data. McAfee recommends performing this task only to change the configuration of your existing database.
You can use the web page at https://servername:port/core/config to adjust any database configuration file information that used to be done with the Cfgnaims.exe file.

Things to know about this page:

- **Authentication** — If the database is up, this page uses normal McAfee ePO user authentication and only a global administrator can access it. If the database is down, a connection is required from the system running the SQL server.

- The McAfee ePO server must be restarted for any configuration changes to take effect.

- **As a last resort, you might edit the configuration file** (\<ePO installation directory>\server\conf \orion\db.properties) by hand, put in the plaintext password, start the server, then use the config page to re-edit the db config, which stores the encrypted version of the passphrase.

**Task**

1. Log on to ePolicy Orchestrator with global administrator credentials.

2. Type the following URL in the browser's address field.
   
   https://servername:port/core/config

3. On the **Configure Database Settings** page, change the credentials or SQL Server information, as needed.

4. Click **OK** when done.

5. Restart the system or ePolicy Orchestrator services to apply the changes.
A

about this guide 11
access requirements for System Tree 123
accounts, See user accounts
actions, Rogue System Detection
events and 63
queries and installing sensors 282
Active Directory
applying permission sets 55
configuring Windows authorization 57
containers, mapping to System Tree groups 142
implementation strategies 55
systems only synchronization 127
Active Directory synchronization
borders and 124
deleting systems 126, 127
duplicate entry handling 126
integration with System Tree 126
Synchronize Now action 126
systems and structure 127
tasks 126
to System Tree structure 142
types 127
adding comments to issues 294
administrator accounts, See user accounts
administrators, global, See global administrators
agent
alien, on rogue systems 266
configuring policies to use repositories 174
configuring proxy settings for 83
first call to server 130
grouping 105
grouping by assignment rules 106
GUID and System Tree location 130
inactive, on rogue systems 266
maintenance 149
McAfee Agent, ePolicy Orchestrator components 16
properties, viewing 153
responses and event forwarding 214
wake-up calls 155
agent communication port 36
agent deployment credentials 31
Agent Handlers
about 101
Agent Handlers (continued)
assigning agents 103
assignment priority 107
configuring and managing 103
how they work 101
moving agents between 105
multiple 101
priority
in sitelist file 102
scalability 22
when not to use 22
when to use 22
agent-server communication
about 149
secure communication keys (ASSC) 67
System Tree sorting 129
agent-server secure communication (ASSC)
about 64
using different key pairs for servers 71
using one key pair 70
viewing systems that use a key pair 71
working with keys 68, 69
aggregation, See notifications
Applied Policies
creating queries 170
Apply Tag action 132
ASCI (See agent-to-server communication interval) 150
assigning issues 294
assignment of ticketed issues to users 296
assignment rules
agents and handlers 106
Audit Log
about 112
purging 113
viewing action history 112
working with 112
authentication
configuring for Windows 56
authentication, configuring for Windows 53
authorization
configuring for Windows 56
strategies 55
Index

B
bandwidth
  considerations for event forwarding 32
  considerations for pull tasks 192
  distributed repositories and 78
  replication tasks and 193
  Rogue System Sensor and 273
  sensor-to-server traffic 273
best practices
  agent-to-server communication interval 149
  duplicating policies before assigning 165
  importing Active Directory containers 142
  policy assignment locking 165
  product deployment 200
  System Tree creation 135
BMC Remedy Action Request System
  versions 6.3 and 7.0 297
borders (See System Tree organization) 124
branches
  Change Branch action 206
  Current 195, 209
  deleting DAT and engine packages 208
  Evaluation 206
  manually moving packages between 208
  Previous 207
  types of, and repositories 80
broadcast segments and Rogue System Sensor 272
Broken Inheritance
  creating queries 170
C
catch-all groups 130
certificate authentication
  configuring ePolicy Orchestrator 58
  configuring users 60
  disabling 59
  enabling 59
  introduction to 58
  strategies for use 58
  troubleshooting 60
  uploading server certificates 59
Change Branch action 206
charts (See queries) 242
Check IP Integrity action 129
client tasks
  about 199, 200
  client task catalog 200
  creating and scheduling 204
  deleting 205
  editing settings for 205
  installing RSD sensors 282
  objects 200
  sharing 200
  working with 204
command-line options
  notifications and registered executables 221
  rogue system detection 286
communication port, Rogue System Detection 269
communication to the server 273
compliance
  compliant systems 266
  configuring RSD settings 61
  creating a query for 250
  generating events 250
components
  ePolicy Orchestrator server, about 16
  ePolicy Orchestrator, about 16
  repositories, about 78
configuration
  essential features 27
  general server settings 31
  overview 22
contacts
  responses and 224
conventions and icons used in this guide 11
creating issues 290
creating tickets 296
credentials
  caching deployment 31
  modifying database registrations 262
  changing, on distributed repositories 94
criteria-based tags
  applying 133, 134
  sorting 140
Current branch
  checking in update packages 209
  defined 80
  for updates 195
custom login messages 34
D
dashboard monitors
  configuring 234
  moving and resizing 235
  removing 231
  working with 234
dashboards
  setting defaults 32
  adding monitors 230
  configuring for exported reports 36
  configuring monitors 234
  copying 231
  creating 230
  default 233
  default monitors 235
  deleting 232
  export 232
  granting permissions to 233
  import 232
dashboards (continued)
   introduction 229
   moving and resizing monitors 235
   removing monitors 231
   Rogue System Detection 266
   working with 229
DAT file updating
   checking in manually 209
   checking versions 205
   considerations for creating tasks 203
   daily task 203
   deployment 189
   from source sites 73
   in master repository 80
   scheduling a task 203
DAT files
   deleting from repository 208
   evaluating 206
   repository branches 208
Data Rollup server task 249
database servers
   about using 261
   editing registrations 262
   registering 99
   removing 262
   working with 262
databases
   maintaining 311
   management tools 311
   McAfee ePO, systems listed in 266
   multi-server querying 249
   ports and communication 39
   queries and retrieving data 240
   recovering 311
deleting issues 294
deployment
   checking in packages manually 207
   global updating 191
   installing products 201, 202
   package security 187
   product and update, first time 189
   products and updates 189
   supported packages 187
   tasks 200
   tasks, for managed systems 200
detected systems
   configuring policy settings 275
   Exceptions list, adding to 276
   Exceptions list, importing to 278
   homepage 266
   how Rogue System Sensor work 272
   merging 278
   merging and matching 274
   removing from lists 279, 280
   Rogue Sensor Blacklist, adding to 277
detected systems (continued)
   status monitors 266
   viewing 280
   working with 274
Detected Systems list, removing systems from 279
detections
   configuring RSD policies 275
   settings for rogue systems 269
   subnet status and rogue systems 268
devices, detected by Rogue System Sensor 272
DHCP servers
   Rogue System Sensor and 269, 273
   system and subnet reporting 272
Directory (See System Tree) 142
distributed repositories
   about 78, 79
   adding to ePO 87
   changing credentials on 94
   creating and configuring 86
   deleting 90
   deleting SuperAgent repositories 86
   editing existing 90
   enabling folder sharing 90
   ePolicy Orchestrator components 16
   folder, creating 87
   how agents select 193
   limited bandwidth and 78
   replicating packages to SuperAgent repositories 86
   replicating to 196, 197
   SuperAgent, tasks 84
types 79
   unmanaged 79
   unmanaged, copying content to 91
documentation
   audience for this guide 11
   product-specific, finding 12
   typographical conventions and icons 11
domain synchronization 124
duplicate entries in the System Tree 144

E
   editing database server registrations 262
   editing issues 294
   email servers
      configuring responses 216
   enforcement (See policy enforcement) 178
   engine updating
      checking in manually 209
      deployment packages 189
      from source sites 73
      in master repository 80
      scheduling a task 203
   engines
      deleting from repository 208
      repository branches 208
Index

F
fallback sites
about 78
categorizing sites 73
deleting 75
deleting existing 75
switching to source 75
features, ePolicy Orchestrator
components 16
filters
Event Filtering settings 39
for server task log 115
query results 242
setting for response rules 223
FTP repositories
about 79
creating and configuring 86
editing 90
enabling folder sharing 90

G
geographic borders, advantages of 124
global administrators
about 43
changing passwords on user accounts 44
creating groups 121
creating user accounts 44
deleting permission sets 51
deleting user accounts 45
permissions 43
source sites, configuring 73
global unique identifier (GUID) 130
global updates
contents 33
global updating
enabling 191
process description 190
requirements 190
grouping, See notifications
groups
catch-all 130
configuring criteria for sorting 140
controlling access 47
creating manually 136
criteria-based 130
defined 121
importing NT domains 144
moving systems manually 147
operating systems and 125
pasting policy assignments to 179
policies, inheritance of 121
policy enforcement for a product 178
sorting criteria 140
sorting, automated 124
groups (continued)
   updating manually with NT domains 147
   using IP address to define 124
   viewing policy assignment 182

H
handler assignment
   editing priority 104, 107
   managing 104
   viewing summary 104
handler groups
   about 102
   creating 104
   deleting 105
   editing settings 105
handlers
   creating groups 104
   grouping agents 107
   moving agents between 105
   priority 102
Hewlett-Packard Openview Service Desk
   versions 4.5 and 5.1 297
HTTP repositories
   about 79
   creating and configuring 86
   editing 90
   enabling folder sharing 90
I
importing
   basics 110
   client task objects 111
   dashboards 111
   permission sets 51
   policies 111
   policy assignments 111
   queries 111
   reports 261
   repositories 111
   responses 111, 217
   systems 111
   tags 111
   tasks 111
inactive agents 156
inactive systems, rogue system status 266
inheritance
   and policy settings 165
   broken, resetting 183
   defined 121
   viewing for policies 183
installation
   Rogue System Sensor 281
   intelligent filtering and Rogue System Sensor 272
interface
   favorites bar 18
   menu 18
   navigation 18
interface,
   Menu 18
internet explorer
   blocked downloads 259
Internet Explorer
   configuring proxy settings 83
   proxy settings and ePO 84
intervals
   between notifications 33
IP address
   as grouping criteria 124
   checking IP overlap 129
   IPv6 109
   range, as sorting criteria 140
   sorting 129
   sorting criteria 135, 140
   subnet mask, as sorting criteria 140
issue management 290
issue synchronization server taskl 297
issues
   about 289
   adding comments 294
   adding tickets to 301
   assigning 294
   associations with tickets (See ticketed issues) 296
   creating 290
   creating automatically from responses 291
   deleting 294
   editing 294
   managing 290
   viewing details 294
   working with 290
issues, purging
   closed issues 295
   closed issues on a schedule 295
K
keys, See security keys
L
LAN connections and geographical borders 124
language packages (See agent) 124
LDAP servers
   authentication strategies 55
   LDAP servers, registering 97
license key 34
local distributed repositories 91
log files
   server task log 114
   login messages 34
McAfee® ePolicy Orchestrator® 4.6.0 Software Product Guide

Index

M
managed systems
agent-server communication 149
deployment tasks for 201
Detected Systems list 279
Exceptions list 276
global updating and 78
installing products on 202
policy assignment 183
policy management on 163
Rogue Sensor Blacklist 269, 277
rogue system status 266
rollup querying 249
sorting, criteria-based 128
tasks for 201
master repositories
about 78
checking in packages manually 209
communicating with source sites 82
configuring proxy settings 83
ePolicy Orchestrator components 16
key pair for unsigned content 65
pulling from source site 194, 195
replicating to distributed repositories 196, 197
security keys in multi-server environments 66
updating with pull tasks 192
using replication tasks 193
McAfee Agent (see agent) 16
McAfee Default policy
frequently asked questions 185
McAfee Labs
Security Threats page 34
Security Threats, working with 35
Threat Service, default monitor 235
McAfee Links, default monitor 235
McAfee recommendations
configure RSD sensor policies before deploying sensors 269
create a Rollup Data server task 249
deploy agents when importing large domains 144
duplicate policies before assignment 165
evaluate borders for organization 124
install multiple Rogue System Sensors per broadcast segment 273
phased rollout for product deployment 200
schedule replication tasks 193
System Tree planning 123
use global updating 190
use IP addresses for sorting 124
use tag-based sorting criteria 124
McAfee ServicePortal, accessing 12
Menu
navigating in the interface 19
menu-based navigation 18
message
custom login 34
Microsoft Internet Information Services (IIS) 79
Microsoft Windows Resource Kit 139
monitors
adding to dashboards 230
configuring 234
removing from dashboards 231
monitors, Rogue System Detection
overall system status 266
status monitors 266
multiple McAfee ePO servers
policy sharing 185
My Default policy
frequently asked questions 185
N
navigation
menu-based 18
navigation,
Menu 18
menu-based 18
navigation bar 19
NETDOM.EXE utility, creating a text file 139
network bandwidth (See System Tree organization) 124
network traffic
bandwidth 273
Rogue System Sensor and 272
New Group wizard
creating new groups 245
Notification event interval 33
notification rules
defaults 213
importing .MIB files 220
notifications
assigning permissions 216
event forwarding 215
how they work 212
recipients 212
registered executables, working with 221
SNMP servers 98, 218
throttling, aggregation, and grouping 213
NT domains
importing to manually created groups 144
integration with System Tree 126
synchronization 127, 144
updating synchronized groups 147
O
operating systems
filters for response rule 223
grouping 125
legacy systems (Windows 95, Windows 98) 125
Rogue System Detection and 272
Rogue System Sensor and 272
overall system status, Rogue System Detection 266
packages
  checking in manually 207
  configuring deployment task 202
  deploying updates with tasks 194
  moving between branches in repository 208
passwords
  changing on user accounts 44
permission sets
  applying to Active Directory groups 55
  assigning to reports 258
  creating 49
  deleting 51
  duplicating 50
  editing 50
  example 47
  exporting 50
  importing 51
  interaction with users and groups 47
  mapping to Active Directory groups 53
  rogue system detection 271
  System Tree 123
  working with 49, 51
permissions
  assigning for notifications 216
  assigning for responses 217
  for queries 240
  global administrator 43
  to dashboards 233
policies
  hiding for unsupported products 35
  about 163
  assigning and managing 173
  broken inheritance, resetting 183
  categories 163
  changing the owner 175
  controlling on Policy Catalog page 172, 173
  controlling, on Policy Catalog page 172
  frequently asked questions 185
  group inheritance, viewing 183
  how they are applied to systems 165
  importing and exporting 163, 175, 176
  inheritance 165
  ownership 165, 182
  settings, viewing 181
  sharing between McAfee ePO servers 175
  using tags to assign 168
  verifying changes 153
  viewing 163, 180
  working with Policy Catalog 171
policies, Rogue System Detection
  about 269
  compliance settings 61
  configuring 275
  considerations 269
  matching settings 62
policy assignment
  copying and pasting 179, 180
  disabled enforcement, viewing 182
  group, assigning to 176
  locking 165
  Policy Catalog 165
  systems, assigning to 177
  viewing 181–183
policy assignment rules
  about 166
  and multi-slot policies 166
  creating 169
  deleting and editing 170
  editing priority 170
  importing and exporting 170
  priority 166
  rule criteria 166
  system-based 166
  system-based policies 168
  user-based 166
  user-based policies 167
  viewing summary 170
policy catalog
  hiding policies 35
Policy Catalog
  page, viewing 163
  working with 171
policy enforcement
  enabling and disabling 178
  for a product 178
  viewing assignments where disabled 182
  when policies are enforced 163
policy management
  using groups 121
  working with client tasks 204
Policy Management
  creating queries 170
policy sharing
  assign 184
  designating 184
  multiple McAfee ePO servers 184
  registering server 184
  using registered server 184
  using server tasks 184, 185
ports
  agent communication 36
  RSD sensor-to-server port 269
  server settings 39
  server settings and communication 39
Previous branch
  defined 80
  moving DAT and engine packages to 208
queries (continued)
   personal query group 245
   report formats 240
   result type 249
   results as dashboard monitors 240
   results as tables 242
   rollup, from multiple servers 249
   running existing 244
   scheduled 245
   using in a server task 250
   using results to exclude tags on systems 133
   working with 243
queries, Rogue System Detection
   installing sensors 282
Query Builder
   creating custom queries 243
Query Builder wizard
   about 242
   result types 242
Quick System Search, default monitor 235
R
registered executables
   adding 221
   duplicating 221
registered servers
   adding SNMP servers 98
   enabling policy sharing 184
   LDAP servers, adding 97
   registering 95
   supported by ePolicy Orchestrator 95
registering database servers 99
registering servers 95
Remedy
   sample mapping for (See ticketing servers) 300
removing database server registrations 262
Replicate Now task 197
replication
   avoiding for selected packages 89, 198
   disabling of selected packages 89
replication tasks
   copying contents of master repository 196
   deploying updates 194
   full vs. incremental 193
   Replicate Now task from master repository 197
   scheduling repository replication 196
   server task log 199
   updating master repository 193
report elements
   configuring charts 256
   configuring images 254
   configuring tables 255
   configuring text 255
   removing 257
   reordering 258

Q
queries
   about 240
   actions on results 240
   changing groups 246
   chart types 242
   creating a compliance query 250
   custom, creating 243
   deleting 246
   duplicating 246
   exported as reports 240
   exporting 247
   exporting to other formats 248
   filters 242
   importing 247
   permissions 240

purgings closed issues
   manually 295

pull tasks
   considerations for scheduling 192
   deploying updates 194
   Pull Now task, initiating 195
   server task log 199
   updating master repository 192, 194
proxy settings
   configuring ePO for Internet Explorer 84
   configuring for master repository 83
   McAfee Agent 83
   server settings 36
product properties
   agent, viewing from the console 153
   product 157
   system 157
   verifying policy changes 153
pull tasks
   considerations for scheduling 192
   deploying updates 194
   Pull Now task, initiating 195
   server task log 199
   updating master repository 192, 194
purging closed issues
   manually 295
previous branch (continued)
   saving package versions 207
product deployment packages
   checking in 207
   checking in manually 209
   security and package signing 187
   supported packages 187
   updates 187
product installation
   configuring deployment tasks 201, 202
   installing extension files 207
product updates
   checking in packages manually 207
   deploying 189
   package signing and security 187
   process description 189
   source sites and 78
   supported package types 187
properties
   agent, viewing from the console 153
   product 157
   system 157
   verifying policy changes 153
proxy settings
   configuring ePO for Internet Explorer 84
   configuring for master repository 83
   McAfee Agent 83
   server settings 36
pull tasks
   considerations for scheduling 192
   deploying updates 194
   Pull Now task, initiating 195
   server task log 199
   updating master repository 192, 194
purging closed issues
   manually 295
queries
   about 240
   actions on results 240
   changing groups 246
   chart types 242
   creating a compliance query 250
   custom, creating 243
   deleting 246
   duplicating 246
   exported as reports 240
   exporting 247
   exporting to other formats 248
   filters 242
   importing 247
   permissions 240
reports
about 251
adding elements 254
adding to a group 258
configuring chart elements 256
configuring image elements 254
configuring table elements 255
configuring template and location for 36
configuring text elements 255
creating 253
deleting 261
editing existing 253
exported query results 240
exporting 260
formats 240
headers and footers 256
importing 261
removing elements 257
reordering elements 258
running 259
running with a server task 260
scheduling 260
structure and page size 251
viewing output 258
working with 252
repositories
branches 80, 206, 208
creating SuperAgent repository 85
how they work together 82
importing from repository list files 93
master, configuring proxy settings for 83
replication and selection of 193
replication tasks 197
scheduling a pull task 194
scheduling a replication task 196
security keys 64, 66
source site 78, 195
types of 78
unmanaged, copying content to 91
repository list files
about 81
adding distributed repository to 87
exporting to 92, 93
importing from 93
priority of Agent Handlers 102
SiteList.xml, uses for 81
working with 92
Response Builder wizard 224
response rules
creating and editing 222
Description page 222
setting filters for 223
setting thresholds 223
responses
assigning permissions 217
responses (continued)
configuring 216, 220, 224
configuring to automatically create issues 291
contacts for 224
event forwarding 214
frequently asked questions 226
planning 214
registered executables, working with 220
rules that trigger 224
SNMP servers 217, 219
Rogue Sensor Blacklist
about 269
adding systems 277
removing systems from 280
Rogue System Detection
about 265
compliance settings 61
configuring server settings 61
deploying sensors 281
operating system support 272
policy configuration 275
policy settings 269
sensor blacklist 269
sensor settings 63
sensor-to-server communication port 269
status and states 266
working with subnets 284–286
Rogue System Sensor
about 272
active, configuring 63
blacklist 269
data gathering 273
installation 281
installing 282
operating systems and 272
removing 283
Rogue System Detection settings, configuring 63
status and sensor states 267
traffic and intelligent filtering 272
working with 280
rogue systems
about 265
system status 266
Top 25 Subnets list 268
rules
configuring contacts for responses 224
defaults for notifications 213
setting up for notifications, SNMP servers 220
Run Tag Criteria action 132
S
scalability
about 21
horizontal 21
planning 21
scalability (continued)
   using agent handlers 22
   using multiple servers 21
   vertical 21
schedule server task
   for policy sharing 185
scheduling
   applying criteria-based tags 134
   client tasks 204
   Repository Pull task 194
   Repository Replication task 196
   server tasks with Cron syntax 115, 198
security certificate
   certificate authority (CA) 37
   installing 38
security keys
   agent-server secure communication (ASSC) 64, 67
   ASSC, working with 68, 69
   backing up 72
   for content from other repositories 65
   general 64
   managing 65
   master keys in multi-server environments 66
   private and public 65
   restoring 72, 73
   server settings 39
   using one master key 66
selected packages
   avoid replication of 89, 198
   disabling replication of 89
sensor-to-server port 269
server certificate
   removing 59
   replacing 37
server settings
   about 31
   configuration 31
   configuring Rogue System Detection 61
   default categories 39
   general 31
   global updates 33
   global updating 191
   Internet Explorer 83
   notifications 213
   ports and communication 39
   proxy settings 36
   proxy, and master repositories 78
   SSL certificates 37
   types of 39
Server Task Builder wizard 134
server task log (continued)
   Replicate Now task 197
   reviewing status of tasks 114
   working with 114
server tasks
   about 190
   allowing Cron syntax 115, 198
   Data Rollup 249
   for policy sharing 184
   installing Rogue System Sensor 282
   log file, purging 115
   replacing server certificate 37
   Repository Pull, scheduled 194
   Repository Replication 196
   running reports 260
   scheduling a query 245
   scheduling with Cron syntax 115, 198
   server task log 114
   Synchronize Domain/AD 126
server types
   supported by ePolicy Orchestrator 95
servers
   database 261
   configuration overview 22
   ePolicy Orchestrator server, components 16
   importing and exporting policies 163
   importing policies from 176
   LDAP servers, registering 97
   master repository key pair 65
   registering 95
   registering additional McAfee ePO servers 95
   server task log, about 199
   settings and controlling behavior 39
   sharing policies 175
   SNMP, and notifications 218
   SNMP, and responses 217
   supported server types 95
   tasks, scheduling repository replication 196
   transferring systems 148
   types you can register 95
   when to use more than one 21
Service Desk
   sample mappings for (See ticketing servers) 299
ServicePortal, finding product documentation 12
sitelist files 102
sites
   deleting source or fallback 75
   editing existing 75
   fallback 73, 78
   switching source and fallback 75
SNMP servers
   See also responses
   registering 98
software manager
- about 159
- checking in extensions 160
- checking in packages 160
- contents 159
- evaluation software 160
- licensed software 160
- removing extensions 160
- removing packages 160

Sort Now action 128

sorting criteria
- configuring 140
- for groups 140
- groups, automated 124
- IP address 129
- IP address-based 140
- sorting systems into groups 128
- tag-based 124, 130, 140

source sites
- about 78
- configuring 73
- creating 74
- deleting 75
- editing existing 75
- fallback 78
- importing from SiteMgr.xml 93
- product updates and 78
- pulling from 194, 195
- switching to fallback 75
- update packages and 189

SPIPE 149

SQL database
- management tools 311

SQL servers
See also databases
- editing information 312

SSL certificates
- about 37

status monitors
- detected systems 266

subgroups
- and policy management 144
- criteria-based 130

subnets
- active Rogue System Detection sensors, configuring duration 63
- in Rogue System Detection 284–286
- status, Rogue System Detection 268
- Top 25 Subnets list 268

subnets, as grouping criteria 124

SuperAgent repositories
- about 79
- creating 85
- deleting 86
- global updating requirements 190

SuperAgent repositories (continued)
- replicating packages to 86
- tasks 84

SuperAgents
- distributed repositories 79
- wake-up calls 151, 155
- wake-up calls to System Tree groups 155

synchronization
- Active Directory and 127
- defaults 130
- deploying agents automatically 127
- excluding Active Directory containers 127
- NT domains 127
- preventing duplicate entries 127
- scheduling 146
- Synchronize Now action 126
- systems and structures 127
- systems only, with Active Directory 127

synchronization of ticketed issues 297

system status
- monitors 266
- Rogue System Detection 266

System Tree
- access requirements 123
- assigning policies to a group 176
- child groups and inheritance 121
- creation, automated 124
- criteria-based sorting 128
- defined 121
- deleting systems from 121
- grouping agents 107
- groups and manual wake-up calls 155
- My Organization level 121
- parent groups and inheritance 121
- permission sets 123
- populating groups 135

System Tree organization
- borders in your network 124
- creating groups 135
- duplicate entries 144
- importing Active Directory containers 142
- importing systems and groups 137, 139
- mapping groups to Active Directory containers 142
- moving systems to groups manually 147
- network bandwidth 124
- operating systems 125
- planning considerations 123
- text files, importing systems and groups 138
- using subgroups 144

System Tree sorting
- default settings 130
- enabling 39, 141
- IP address 129
- on agent-server communication 129
- ordering subgroups 130
System Tree sorting (continued)
server and system settings 39, 129
sort systems once 129
tag-based criteria 130
System Tree synchronization
Active Directory integration 126
NT domain integration 126
scheduling 146
to Active Directory structure 142
system-based policies
about 168
criteria 168
systems
exporting from the Systems Tree 138
assigning policies to 177
pasting policy assignments to 180
policy enforcement for a product 178
properties 157
sorting into groups 141
viewing policy assignment 183

tag-based sorting criteria 124, 130
tags
applying 133, 134
creating with Tag Builder wizard 132
criteria-based 125, 128
criteria-based sorting 140
defined 125
excluding systems from automatic tagging 133
group sorting criteria 124
manual application of 133
permissions for 125
types 125
without criteria 125
working with 132
Technical Support, finding product information 12
Test Sort action 128
Threat Event Log
about 116
working with 117
throttling, See notifications
ticketed issues
about 296
assignment to users 296
creating 289
how comments are handled 297
how they are closed 296
how they are reopened 297
how they are synchronized 297
synchronizing 302
synchronizing on a schedule 302
ticketing
installing server extensions 303
ticketing servers
about sample mappings 298
BMC Remedy Action Request System
versions 6.3 and 7.0 297
configuring DNS for Service Desk 4.5 306
considerations when deleting 298
Hewlett-Packard Openview Service Desk
versions 4.5 and 5.1 297
installing extensions 303
installing extensions for 303, 305
installing extensions for Remedy 304
installing extensions for Service Desk 304
integration with 297
mapping 306
mapping issues to tickets 307
mapping tickets back to issue status 307
registering 306
registering and mapping 305
required fields for mapping 298
sample mapping for Remedy 300
sample mappings for Service Desk 299
upgrading 308
working with 302
ticketing systems
BMC Remedy Action Request System 289
Hewlett-Packard Openview Service Desk 289
tickets
about 289, 296
adding to issues 301
associations with issues (See ticketed issues) 296
creating 289, 296
how comments are handled 297
how they are closed 296
how they are reopened 297
how they are synchronized 297
server integrations for 297
synchronizing 302
synchronizing on a schedule 302
working with 301
troubleshooting
certificate authentication 60
product deployment 200
verifying properties of agent and products 153

U
UNC share repositories
about 79
creating and configuring 86
editing 90
enabling folder sharing 90
unmanaged repositories 79
unsupported products
  hiding policies for 35
updates
  checking in manually 207
  client tasks 203
  considerations for creating tasks 203
  deploying packages with tasks 194
  deployment packages 189
  package signing and security 187
  packages and dependencies 187
  scheduling an update task 203
  source sites and 78
updating
  automatically, with global updating 191
  DATs and engine 189
  deployment tasks 200
  global, process 190
  master repository with pull tasks 194
  process description 189
  Pull Now task to update master repository 195
  scheduling an update task 203
user accounts
  about 43
  changing passwords 44
  creating 44
  deleting 45
  editing 44
  working with 44
user-based policies
  about 167
  (continued)
  criteria 167
  users
    permission sets and 47
  utilities
    NETDOM.EXE, creating a text file 139
V
  viewing issue details 294
VPN connections and geographical borders 124
W
  wake-up calls
    about 151
    manual 155
    SuperAgents and 151, 155
    tasks 151
    to System Tree groups 155
  WAN connections and geographical borders 124
what's in this guide 12
Windows
  authentication, configuring 53, 56
  Authorization, configuring 57
Windows authentication
  configuring 56
  enabling 56
  strategies 55
Windows authorization
  configuring 56